«Zertifizierten» Datenschutz

Dr.iur. Bruno Baeriswyl
Datenschutzbeauftragter des Kantons Zürich

CH - 8090 Zürich
Tel.: +41 43 259 39 99
Fax: +41 43 259 51 38
datenschutz@dsb.zh.ch
www.datenschutz.ch

Symposium on Privacy and Security
6. November 2007

Inhalt

- Ausgangslage
- Gesetzliche Bestimmungen
  - Datenschutzgesetz Bund (DSG)
  - Informations- und Datenschutzgesetz Zürich (IDG)
- Zertifizierung
  - Ziel, Inhalt, Verfahren
- Bedeutung
- Kritische Erfolgsfaktoren
- Fazit

Ausgangslage (1)

- Zertifizierungsverfahren
- Gütesiegel
  - Umweltschutz, Fair Trade, Bio-label, E-commerce……

…. und jetzt noch Datenschutz?

Ausgangslage (2)

… schon vorhanden!

Was wird sich ändern?

Grundlagen (1)

- Gesetzliche Bestimmungen
  - Zielsetzungen
  - Rahmenbedingungen

→ Transparenz

DSG (Revision)

Art. 11 Zertifizierungsverfahren

1 Um den Datenschutz und die Datensicherheit zu verbessern, können die Hersteller von Datenbearbeitungssystemen oder -programmen sowie private Personen oder Bundesorgane, die Personendaten bearbeiten, ihre Systeme, Verfahren und ihre Organisation einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen unterziehen.

2 Der Bundesrat erlässt Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens. Er berücksichtigt dabei das internationale Recht und die international anerkannten technischen Normen.

IDG

Art. 13 Qualitätssicherung

1 Das öffentliche Organ kann zur Sicherstellung der Qualität der Informationsbearbeitung seine Verfahren, seine Organisation und seine technischen Einrichtungen durch eine unabhängige und anerkannte Stelle prüfen lassen.

2 Der Regierungsrat regelt das Nähere in einer Verordnung.

Verordnungen

- Bund:
  - Verordnung über die Datenschutzzertifizierungen (28. September 2007)
- ZH:
  - In Vorbereitung

Gesetzliche Bestimmungen

- können = Freiwilligkeit
- Anreiz DSG:
  - Keine Anmeldepflicht von Datensammlungen (Mitteilung der Zertifizierung) (Art. 11a Abs. 5 lit. f DSG)
- **Wirklicher Anreiz?**

Freiwilligkeit

- Mehrwert:
  - Nutzen für Datenbearbeiter
    - Kundennähe
    - Transparenz
    - Sensitivität
    - Wettbewerbsvorteil
    - Vertrauen

  = auch Nutzen für betroffene Personen
- **Aber auch ein «Mehr» an Datenschutz !**

Verbesserung (1)

- Ziel:
  - «Um den Datenschutz und die Datensicherheit zu verbessern….»
- «Mangelhaften» Datenschutz beheben?
  - *Nein !*
- Compliance?
  - *Ja, aber…*
  - *mit «Kontinuierlichem Verbesserungsprozess» (KVP)*

Verbesserung (2)

- Einsatz datenschutzfreundlicher Technologien
  - Anonymisierung von Personendaten, wenn Identität nicht erforderlich
  - Datenvermeidung und Datensparsamkeit
  - (… und nicht Ausweitung der Einwilligungserklärung!)
- Verminderung des «Restrisikos» durch organisatorische Massnahmen
- Laufende Überprüfung der Angemessenheit der Sicherheitsmassnahmen

Bewertung

- Hersteller
  - Datenbearbeitungssysteme und –programme
    - Hardware / Software

    → «Produktezertifizierung»
- Datenbearbeiter
  - Systeme, Verfahren, Organisation

    → «Qualitätsmanagementsysteme»

Zertifizierungsstellen (Dienstleister)

- Anerkannte unabhängige Zertifizierungsstellen
  - Akkreditierung (Akkreditierungs- und Bezeichnungsverordnung vom 17. Juni 1962
  - Festgelegte Organisation, festgelegtes Zertifizierungsverfahren (Mindestanforderungen z.B. betr. Qualifikation des Personals (Anhang 1)
  - CH Akkreditierungsstelle mit Beizug EDÖB
  - Anerkennung ausländischer Zertifizierungsstellen (durch EDÖB)

Massstab

- Internationales Recht und international anerkannte technische Normen
  - ISO 9001:2000
  - ISO 27001:2005
- Organisation und Verfahren
  - Datenschutzmanagementsystem
    - Mindestanforderungen (Richtlinien EDÖB)
- Produkte
  - Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität
  - Datenvermeidung
  - Transparenz und Nachvollziehbarkeit (Personendaten)
    - Mindestanforderungen (Richtlinien EDÖB, 1.1.2010)

Zertifizierung (1)

- Gütesiegel
  - Erfüllung der Anforderungen = Zertifizierung
- Verfahren: Gültigkeit 3 Jahre
- Produkte: Gültigkeit 2 Jahre
- Jährlicher Audit (summarisch) (Verfahren)
- Audit (wesentliche Veränderungen) (Produkte)

Zertifizierung (2)

- Anerkennung ausländischer Zertifizierungen
  - EDÖB in Rücksprache mit Akkreditierungsstelle
- Verzeichnis
  - Zertifizierungen (Befreiung von der Registrierungspflicht)
- Sanktionen
  - Schwere Mängel (Entzug Zertifizierung durch Zertifizierungsstelle)

Aufsicht

- Feststellung von Mängel (Art. 27, 29 DSG)
  - Information der Zertifizierungsstelle
  - Intervention der Zertifizierungsstelle bei Datenbearbeiter
- Empfehlungen (Art. 31 DSG)
  - An Zertifizierungsstelle
  - An Datenbearbeiter

Bedeutung (1)

- Warum eine Zertifizierung?
  - Verbesserung des Datenschutzes
    - Braucht klares Commitment
  - Transparenz der Datenbearbeitungen
    - Der Nutzen für den Kunden
  - Sensibilität der Datenbearbeitungen
    - Schaffen von Vertrauen
  - Ergänzung von bestehenden Zertifizierungen
    - ISO 9001 etc.
  - Kosten / Nutzen
    - Betonung der Bedeutung des Datenschutzes

Bedeutung (2)

- Warum auf eine Zertifizierung verzichten?
  - Anmeldung der Datensammlungen
    - Vorteil oder Nachteil?
  - Compliance mit dem DSG
    - Kein Vorteil durch Zertifizierung
  - Ansatzpunkt für Zertifizierung
    - Qualität, Standards sind kein Thema
  - Image Verbesserung
    - Aus einem schwarzen Schaf wird kein weisses…
  - Kosten / Nutzen
    - Investitionen in tatsächliche Verbesserungen

Kritische Erfolgsfaktoren (1)

- Zertifizierungsstellen
  - Zum Discountpreis ins Massengeschäft
    - » (unabhängige) Überprüfung
- Kein «offizielles» Qualitätszeichen
  - Aussagekraft des Gütesiegels
    - » (unabhängige) Vergabe

Kritische Erfolgsfaktoren (2)

- Verbesserung
  - Bedeutung der Standards
  - Mindestanforderungen
    - » Indikatoren
  - Branchenspezifität
- Entwicklung von neuen Standards
  - BSI Grundschutzhandbuch (www.bsi.de/gshb/index.htm)
  - ISO 29100 / 29101 / 24760

Kritische Erfolgsfaktoren (3)

- Reaktion der betroffenen Personen
  - Bedeutung von «Privacy»
- Best Practices
  - www.datenschutzzentrum.de
  - http://www.european-privacy-seal.eu

Fazit

- Selbstregulierung in einem gesetzlichen Rahmen
- Verbesserung des Datenschutzes
- Wenn eine Zertifizierung, dann aber korrekt!

Besten Dank!

Datenschutzbeauftragter des Kantons Zürich

CH - 8090 Zürich
Tel.: +41 43 259 39 99
Fax: +41 43 259 51 38

datenschutz@dsb.zh.ch
www.datenschutz.ch

Qualität ist uns wichtig –
Unsere Dienstleistungen sind
zertifiziert nach ISO 9001:2000