Datenschutz braucht Informatik

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

Kommunikation in Verteilten Systemen

Christian-Albrechts-Universität Kiel

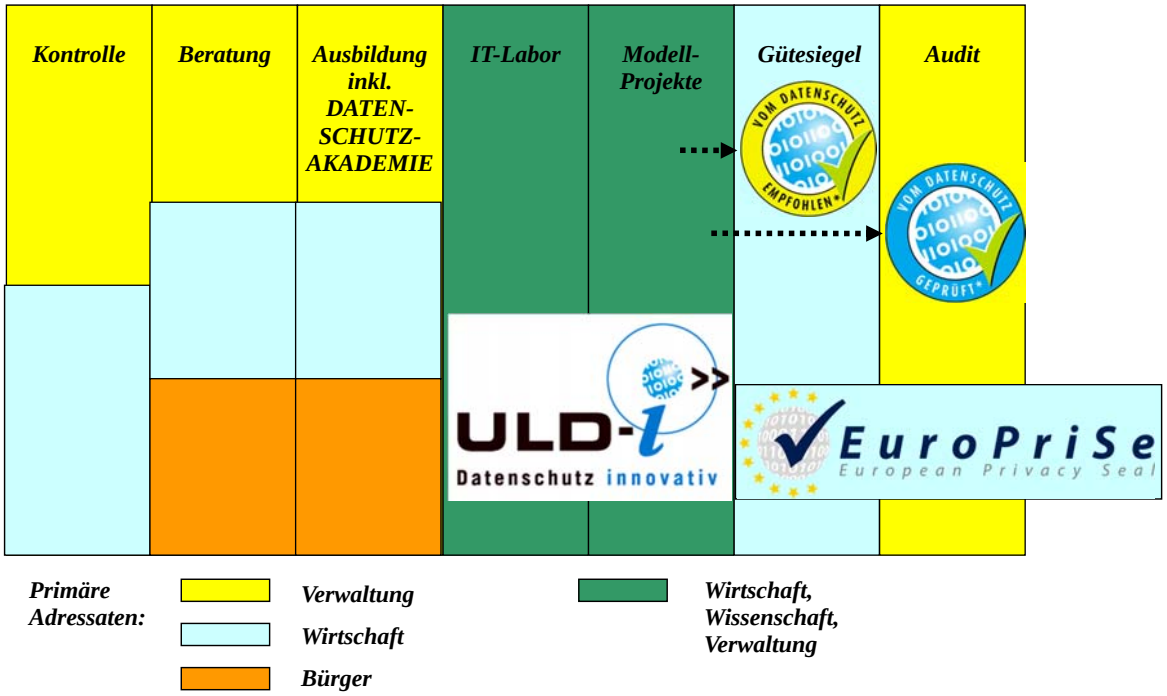
Kiel, 08.03.2011

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Zielsetzung und Entwicklung des Datenschutzes
- Technischer Datenschutz
- Instrumente und Maßnahmen
- Tätigkeitsfelder für InformatikerInnen
- Beispiele: Internet, Smartphone, AAL, Großprojekte

Unabhängiges Landeszentrum für Datenschutz



ULD www.datenschutzzentrum.de

Zielsetzung des Datenschutzes

- Bundesverfassungsgericht (BVerfG) 1983: Recht auf informationelle Selbstbestimmung > Wissen (Transparenz) und Bestimmenkönnen
- BVerfG 2008: Recht auf Gewährleistung der Integrität und Vertraulichkeit eigengenutzter informationstechnischer Systeme (digitale Privatsphäre)
- Technisch-organisatorische Maßnahmen der Datensicherheit
- Verfahrensrechtliche Sicherungen
- Verwandte Schutzrechte (z.B. Telekommunikationsgeheimnis, Schutz der Wohnung, Schutz der Familie, Schutz von Beruf und Eigentum, politische Freiheiten, Informations- und Meinungsfreiheit)

Entwicklung des Datenschutzes

Bis 70er: Ordnungsgemäßheit (Funktionieren) von Datenverarbeitung

70er: Datenschutzgesetze schützen vor Datenmissbrauch

1983 (BVerfG): strenger Gesetzesvorbehalt, Zweckbindung, informationelle Gewaltenteilung, Erforderlichkeitsprinzip

90er: Privacy Enhancing Technologies (PET), Datensparsamkeit, mehrseitige Sicherheit

Seit 1995 (EU-DSRL): Sicherung der Grundrechte zwecks Informationsaustausch im Binnenmarkt

00er: Datenschutz als Verbraucherschutz, als Wettbewerbsfaktor, als IT- (Sicherheits-) Management, als Compliance (2008/2009: Skandale)

ULD www.datenschutzzentrum.de

Verfassungs- und völkerrechtliche Grundlagen

Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

- BVerfG 1969: Verbot von teilweise und vollständigen Persönlichkeitsbildern
- BVerfG 1983: Grundrecht auf informationelle Selbstbestimmung = Recht, selbst zu bestimmen, wer was wann bei welcher Gelegenheit über einen weiß

Art. 8 EMRK: Achtung des Privatlebens (Privat- u. Familienleben, Wohnung, Briefverkehr)

Europäische Datenschutzkonvention 1981

Art. 8, 9 Europ. Grundrechtecharta 2009: Schutz personenbezogener Daten und der Privatsphäre

Europäische Datenschutzrichtlinie 1995

Empfehlungen des OECD und der UNO

BVerfG, U.v. 15.12.1983 (1 BvR 09/83 u.a.)

„Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten vom **allgemeinen Persönlichkeitsrecht** ... umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."

„Einschränkungen dieses **Rechts auf ´informationelle Selbstbestimmung`** sind nur im überwiegenden Allgemeininteresse zulässig."

ULD www.datenschutzzentrum.de

BVerfG , B.v. 23.10.2003 (1 BvR 2027/02)

„Das allgemeine Persönlichkeitsrecht ... entfaltet als Norm des objektiven Rechts seinen Rechtsgehalt **auch im Privatrecht**."

„Ist ersichtlich, dass in einem Vertragsverhältnis ein Partner ein solches Gewicht hat, dass er den **Vertragsinhalt faktisch einseitig bestimmen** kann, ist es Aufgabe des Rechts, auf die Wahrung der Grundrechtspositionen beider Vertragspartner hinzuwirken, um zu verhindern, dass sich für einen Vertragsteil die Selbstbestimmung in eine Fremdbestimmung verkehrt."

Rechtsgrundlagen

- Bundesdatenschutzgesetz (BDSG) seit 1976, letzte Aktualisierung 2009 - schützt u.a. Inhaltsdaten im Internet, inbes. § 29 BDSG
- Telekommunikationsrecht (TKG, TMG): schützt Nutzungsdaten
- Verbraucher- und Vertragsrecht, hier v.a. Regelungen zu Allgemeinen Geschäftsbedingungen (§§ 305 ff. BGB)

ULD www.datenschutzzentrum.de

7 Regeln des Datenschutzes

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit und Datensparsamkeit
5. Transparenz und Betroffenenrechte
6. Datensicherheit
7. Kontrolle

> Umsetzung durch Informationstechnik nötig

Technischer Datenschutz – früh

- Bis 90er Jahre: keine wichtige Rolle
- 10 Technisch-organisatorische Maßnahmen (TOM) Datensicherheit
  - Zugangskontrolle
  - Datenträgerkontrolle
  - Speicherkontrolle
  - Benutzerkontrolle
  - Zugriffskontrolle
  - Übermittlungskontrolle
  - Eingabekontrolle
  - Auftragskontrolle
  - Transportkontrolle
  - Organisationskontrolle
- Danach leichte Modifikationen der Kontroll-Maßnahmen

ULD www.datenschutzzentrum.de

Technischer Datenschutz – modern

- Schutzziele
  - Vertraulichkeit
  - Integrität
    - Authentizität
  - Verfügbarkeit
  - Transparenz (Revisionsfähigkeit)
- Weiterentwicklung
  - Intervenierbarkeit
  - Nichtverkettbarkeit

Instrumente – frühe Einzelregelungen

- TOM nach § 9 BDSG und Anlage
- Vertragliche Anforderungen an Auftragsdatenverarbeitung (§ 11 BDSG)
- Verfahrensverzeichnis
- Protokollierungspflichten Stichprobenkontrollen
- Verschlüsselungspflichten bei mobilen Geräten od. bei sensibler Verarbeitung

ULD www.datenschutzzentrum.de

Instrumente – systematisch

- Datenschutzverordnung Schleswig-Holstein (DSVO)
- Integration von Fachanwendungen/Verfahren in umfassendes Datenschutzmanagement
- Kriterienkatalog Gütesiegel für Produkte und Dienstleistungen
- Schutzprofile (protection profiles), z.B. Behavioural Targeting, Suchmaschinen, medizinische Archivierung, Social Communities
- Technische Datenschutzstandards (DIN, ISO/IEC)
- Datenschutzaudit (für Organisation, Organisationsteile, Verfahren) und laufendes Monitoring

Verwandte Instrumente

- BSI-Grundschutz
  Bundesamt für die Sicherheit in der Informationstechnik
- Common Criteria
  ISO, BSI
- ISO 9001/ISO 27001
  International Standardization Organisation

ULD www.datenschutzzentrum.de

Beispiele für Maßnahmen

- Anonymisierung, Aggregierung, Pseudonymisierung, frühzeitige (echte) Löschung (Datensparsamkeit)
- Verschlüsselung (Vertraulichkeit)
- Identitätsmanagement, Rollen-, Rechte- od. Strukturkonzepte (Nichtverkettbarkeit)
- Biometrie, digitale Signatur (Authentifizierung, Identifizierung)
- Protokollierung, Protokollauswertung (Transparenz)
- Verfahrens-Dokumentation (Transparenz)

Tätigkeitsfelder für Informatiker

- Verfahrens- und Systembetrieb (Unternehmen, Behörden)
- Implementierung (extern, intern)
- Verfahrens- und Systemkontrolle (IT-Sicherheit, Datenschutzbeauftragte, Datenschutzaufsicht)
- Beratung (intern, extern)
- Entwicklung (Institute, Industrie, Hochschulen)
- Forschung (s.o.)

ULD www.datenschutzzentrum.de

Fächerübergreifende Kooperationen

- Informatik
- Recht (Datenschutz, Datensicherheit, Verbraucherschutz…)
- Psychologie (Nutzer, Anwender, Informatiker, Entscheider)
- Pädagogik (s.o.)
- Politik (-Wissenschaft)
- Wirtschaft (E-Commerce, Werbung, Teil des IT-Managements)
- Sicherheit (Polizei, „Intelligence“, private Unternehmen, Teil der IT-Sicherheit)

Internet

Datenschutz-Herausforderungen für Informatik:

- Identitätsmanagement
- Sichere Zustellung (ePost, De-Mail)
- Sichere Identifizierung und Authentifizierung (nPA)
- Cookie-Management
- Umsetzung von Betroffenenrechten (Notice, Choice, z.B. Button-Lösungen)
- Transparente Privacy Policies
- „Digitaler Radiergummi“
- Spamabwehr, Virenschutz

ULD www.datenschutzzentrum.de

Smart-Phones

Spezifische Herausforderungen

- Verhinderung von Bewegungsprofilen
- Realisierung von Rollenkonzepten und Zweckbindung (Beruf, Familie, Freizeit, Soziales)
- Privacy by Design, by Default (Flüchtigkeit der Nutzung)
- Sicherheit der Applications
- Etablierung datenschutzfreundlicher Standards
- Anwendungsfreundliche Mensch-Maschinen-Schnittstellen
- Sicherung der Integrität und Vertraulichkeit des eigengenutzten IT-Systems

Ambient Assisted Living (AAL)

= Elektronische Assistenzsysteme für v.a. hilfsbedürftige Personen

- Wirksame Intervenierbarkeit für Betroffene (Sex-Button)
- Umsetzung des Transparenzgebotes
- Technische Umsetzung gestufter Einwilligungen
- Skalierbarkeit
- Aggregierungs- und Anonymisierungslösungen
- Vertreterlösungen (Delegation)
- Verhinderung von Profilbildungen und des Eindringens in Kernbereich persönlicher Lebensgestaltung

IT-Großprojekte

ELENA – Elektronischer Leistungsnachweis

eGK – Elektronische Gesundheitskarte

Vorratsspeicherung TK-Verbindungsdaten

Datenverbünde im Sicherheitsbereich (z.B. INPOL-neu, NADIS-neu)

> Frühzeitige Einbindung des Datenschutzes
> Einbindung der Beteiligten und Betroffenen
> Systematisches und modulares Vorgehen

> Hohe Funktionalität, Akzeptanz, Compliance

Schlussfolgerungen

Es gibt keinen rein technischen Datenschutz, nötig ist immer Instrumentenmix

Datenschutz ist bisher Stiefkind in der Informatik

Herausforderungen durch (mobile) Vernetzung

Herausforderungen durch Integration von IT- und Bio-Technik (Genetik, Biometrie, Medizintechnik)

Technischer Datenschutz hat Zukunft

ULD www.datenschutzzentrum.de

Datenschutz braucht Informatik

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