Wie sicher sind meine Daten?
Datenschutz bei Google, Facebook & Co.

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

Tagung für Führungskräfte der Polizei
Web 2.0/Soziale Netzwerke
Sielbeck 05.07.2010

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD SH
- Funktionalitäten, Daten, Nutzungsformen
- Rechtliche Grundlagen des Datenschutzes
- Datenschutz als globale Herausforderung
- Anforderungen an Internet-Dienste, Transparenz
- Selbstschutz
- Ermittlungen im Web 2.0
- Handlungsbedarf

Unabhängiges Landeszentrum für Datenschutz

- Datenschutzkontrollbehörde für öffentlichen und nicht-öffentlichen Bereich (u.a. Polizei, Staatsanwaltschaften, Telemedienanbieter in Sch.Holst., incl. Bußgeldbehörde)
- Ausbildung, Beratung und Unterstützung von Betroffenen, Politik, Verbänden, verarbeitenden Stellen, Forschung u. Entwicklung
- Erstellung von Gutachten und Stellungnahmen
- Durchführung von Projekten (z.B. zu Identity-Management, Online-Spielen, Cloud Computing)
- Datenschutz-Gütesiegel und -Audit (seit 2001, incl. European Privacy Seal - EuroPriSe, seit 2008)

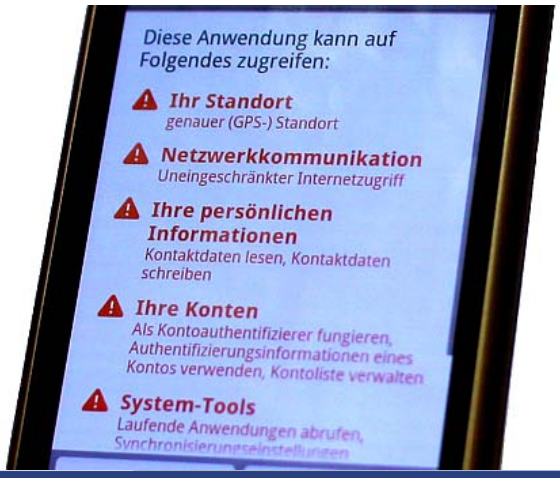
Web 2.0 - Funktionalitäten

- Internetendgerät
  (Info-Abruf, Nutzung von Web 2.0-Diensten)
- E-Mail und sonstige elektronische Kommunikation
- Hoch-, Runterladen und Abspielen von Unterhaltung
  (Musik, Filme, Spiele)
- Konsumzwecke für Verbraucher (eCommerce)
- Personal Digital Assistance
  (u.a. Adressverwaltung, Kalender, Bildverwaltung)
- Berufliche DV-Basis
  (Textverarbeitung, Dokumentenmanagement, Archivierung)
- Telefonie (Voice over IP)
- Navigationsgerät (Mobilgeräte)

Verarbeitete Daten

- Bestandsdaten (Access – Vertragsdaten)
- Verkehrsdaten (Nutzungsdaten bzgl. Netzzugang, Dienste Kommunikation), incl. Standort-Geokoordinaten
- Inhaltsdaten (Content – Dokumente, Bilder, Sprache, Programme)

- ➢ Verhaltensprofile
- ➢ Bewegungsprofile
- ➢ Kommunikations- und Sozialprofile
- ➢ Konsum- und Interessenprofile
- ➢ Evtl. Bonitätsbewertung, Bewerbungsbewertung ...



Wo fallen Daten an?

- TK-Anbieter (Festnetz und mobil)
  - Stammdaten (bei Provider)
  - Verbindungsdaten
  - Zugriff auf Inhaltsdaten

- Dienste-Anbieter
  - Oft personifizierte Accounts
  - Viele Apps verarbeiten Daten nicht im Gerät, sondern auf Servern (z.B. auch bei Spracherkennung => Inhaltsdaten)
  - Einbindung weiterer Dienste (Werbedienste, E-Mail-Dienste, z.B. Bewertungen, „Gefällt mir-Button“ bei Facebook)
  - Cloud-Anbieter

Grundlagen des Datenschutzes I

- Allgemeines Persönlichkeitsrecht (Art. 2 I i.V.m. 1 I GG)
  - Recht auf Privatsphäre (right to be let alone)
  - Recht am eigenen Bild, am gesprochenen Wort
  - Recht auf informationelle Selbstbestimmung
  - Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme
- Telekommunikationsgeheimnis (Art. 10 GG)
- Meinungs-, Informations- und Pressefreiheit (Art. 5 GG)
- Weitere Grundrechte (Eigentum 14 GG, Beruf 12 GG, Ehe u. Familie 6 GG, Religion 4 GG)

Grundlagen des Datenschutzes II

- Recht in Ruhe gelassen zu werden (1969)
- Verbot umfassender Persönlichkeitsprofile (1969)
- Verbot von Personenkennzeichen (1983)
- Verbot der Rundumüberwachung (2004)
- Verbot der Vorratsdatenverarbeitung (anlasslose Kontrolle, „ins Blaue hinein“, 1983)
- Ausnahmecharakter der verdeckten Erhebung (1970)
- Schutz des Kernbereichs persönlicher Lebensgestaltung (2004)
- Individueller Systemschutz (Vertraulichkeit und Integrität eigengenutzter IT-Systeme, 2008)
- Verbot der Totalerfassung als „verfassungsrechtliche Identität der BRD“ (2010)

Grundlagen des Datenschutzes III

- Grundrechte als Abwehrrechte gegenüber dem Staat
- Grundrechte als Bestandteil der objektiven Wertordnung (Drittwirkung im Verhältnis zwischen Privaten)
- Grundrechte als staatliche Gewährleistungsverpflichtung (Recht – z.B. BDSG, Organisation – z.B. Datenschutz-kontrolle, Technik – z.B. Internetinfrastruktur)

Seit Privatisierung der Telekommunikation besondere Verpflichtung der TK-Zugangsdienste bzgl. TK-Geheimnis

Integration des Datenschutzes ins Arbeitsrecht

Integration des Datenschutzes in den Verbraucherschutz

Adressiert auch Diensteanbieter und Programmhersteller

Grundlagen des Datenschutzes IV

- Materielle Zulässigkeit der Datenverarbeitung (BDSG, TMG, TKG, LDSG, KUG, Spezialgesetze, z.B. SGB, KrankhG)
- Datenvermeidung/Datensparsamkeit (Anonymisierung, Aggregierung, Pseudonymisierung, Filetrennung, Verzicht auf IDs, Verschlüsselung)
- Datensicherheit (Integrität, Vertraulichkeit, Verfügbarkeit, Authentizität, Revisionsfähigkeit, Transparenz, Unverknüpfbarkeit)
- Betroffenenrechte (Auskunft, Benachrichtigung, Berichtigung, Löschung, Sperrung, Widerspruch, Schadenersatz)

Datenschutz als globale Herausforderung I

- Nationales Datenschutzrecht knüpft an territorialer Datenverarbeitung an: Erhebung, Speicherung, Verarbeitung (Cookie), Auswertung, Übermittlung, Nutzung
- EU-Datenschutzrichtlinie (gemeinsame DS-Anforderungen und Fiktion eines einheitlichen Standards)
- Anerkennung nationaler Standards durch EU-Kommission
- Safe Harbor für US-Anbieter (Notice, Choice, Onward Transfer, Security, Data Integrity, Access, Enforcement)
- Einzelvertragsregelungen (Binding Corporate Rules, Standardvertragsklauseln)

Datenschutz - globale Herausforderung II

- Begrenzung der Anwendbarkeit: es gibt (noch?) kein Weltrechtsprinzip beim europäischen Datenschutz

➢ Öffentliche Diskreditierung von Diensten, Produkten und Anwendungen

➢ Kulturclash zw. europäischem und anglo-amerikanischem Verständnis

  ➢ USA: Konsument kann sich selbst schützen, Free Speech

  ➢ Europa: Staatlicher Schutz- und Regulierungsauftrag

    Druck z.B. auf Google: Search, Street View, Analytics, Chrome, Dashboard, Mail, Calender ...

Anforderungen an Web-Dienste

- Datenschutzfreundliche Defaults
- Handhabbare u. funktionale Mensch-Maschine-Schnittstellen
- Einwilligungsbasierte Speicherungen (Lokalisierung, Cookies, Werbung)
- Abhärtung des „eigengenutzten Informationssystems“
- Koppelungsverbot
- Logische Trennung der Anwendungen
- Auswertungen nur anonym/pseudonym, getrennt
- Datensicherheit (Update-Service, Apps, Virenprüfung)
- Umfassende Transparenz (trotz beschränkter Displays)

Insbesondere Transparenz

- Information über verantwortliche Stelle und Zweck
- Impressumspflichten
- Privacy Policies
- Benachrichtigung über Erhebung durch Dritte
- Inhalt der Einwilligungen
- Anzeige der Wahlmöglichkeiten
- Information über (Werbe-)Widerspruchsmöglichkeit
- Auskunftsanspruch
- Informationspflichten nach Fernabsatzgesetz (Produkt, Zahlungsweise, Widerrufsrecht, Rückgaberecht)
- Evtl. Breach Notification

Selbstschutz im Web 2.0

- AGBs bzw. Privacy Policies prüfen
- Impressum prüfen, evtl. Web-Infos über Anbieter suchen
- Datensparsame Browser-Einstellungen (z.B. bzgl. Cookies, Werbeblocker)
- Datensparsame Diensteinstellungen
- Nutzung von Anonymisierungsdiensten, Verschlüsselung, Pseudonymen, datenschutzzertifizierten Angeboten
- Bewusste (datensparsame) Eingaben, Uploads
- Nur konsentierte oder spez. begründete Drittangaben
- Eigensuche, eigenes Profil, Betroffenenauskunft
- Widerspruch, Lösch-/Sperrantrag
- Beschwerde bei Datenschutz-Aufsichtsbehörde

Ermittlungen im Web 2.0

- Anlasslose und anlassbezogene Online-Recherchen im allgemein zugänglichen Internet (Einsatz von Suchmaschinen und Analyse-Tools)
- Einsatz „verdeckter Ermittler“ unter Pseudonym
- Bestandsdatenabfrage nach § 111 TKG
- Verkehrsdatenabfrage z.B. nach § 100g StPO (u.a. Quick Freeze, Funkzellenabfrage, IMSI-Catch, stille SMS)
- Inhaltsdatenabfrage nach § 100a StPO
- Derzeit keine Vorratsdatenabfrage
- Computer-Beschlagnahme nach § 94 StPO
- Online-Durchsuchung nach § 20k BKAG

Handlungsbedarf

- Internet-Regelungen im Datenschutzrecht
- Frühestmögliche Integration von Datenschutz (Forschung, Entwicklung, Betrieb) bei Software, Dienste, Oberflächen, Policies
- Entwicklung von Schutzprofilen für Web 2.0-Anwendungen
- Standardisierung von datenschutzkonformen Lösungen (DIN, ISO)
- Weiterentwicklung der Zertifizierung und Markt-Evaluation (Stiftung Datenschutz)
- Etablierung v. Verbraucherschutzinstrumenten (Foren u.Ä.)
- Festlegung Internationaler Privacy-Regelungen

Wie sicher sind meine Daten? Datenschutz bei Google, Facebook & Co.

Dr. Thilo Weichert
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Independent Centre for Privacy Protection Schleswig-Holstein (ICPP)

Holstenstr. 98, 24103 Kiel, Germany

mail@datenschutzzentrum.de

https://www.datenschutzzentrum.de/