# Datenschutz in mobilen Anwendungen – speziell auf der Plattform Android

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

droidcon, Berlin 27.05.2010

droidcon 2010 mai 26/27

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein



## Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD SH
- Smartphones – Funktionalitäten, Daten, Nutzungsformen
- Rechtliche Grundlagen des Datenschutzes
- Datenschutz als globale Herausforderung
- Anforderungen an Mobile Geräte und an Entwickler
- Handlungsbedarf

# Unabhängiges Landeszentrum für Datenschutz

- Datenschutzkontrollbehörde für öffentlichen und nicht-öffentlichen Bereich (u.a. Telemedienanbieter in Sch.Holst.)
- 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 PRIME-life)
- Datenschutz-Gütesiegel und –Audit (seit 2001, incl. European Privacy Seal - EuroPriSe, seit 2008)





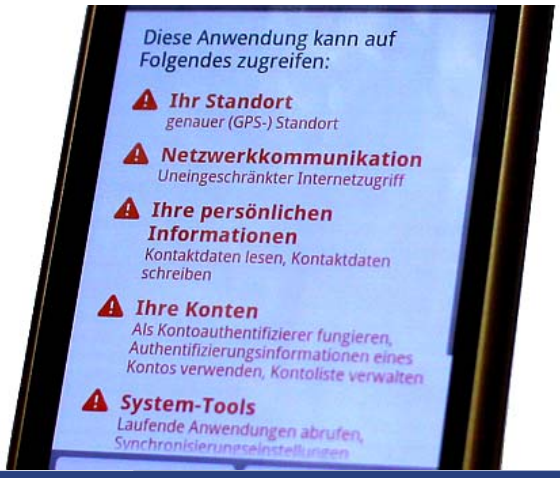
# Funktionalitäten von Smart-Phones

- Telefonie
- E-Mail, SMS, Chat, Instant Messaging und sonstige elektronische Kommunikation
- Internetendgerät
  (Info-Abruf, Nutzung für Web 2.0-Dienste)
- Hoch-, Runterladen und Abspielen von Unterhaltung (Musik, Filme, Spiele)
- Konsumzwecke für Verbraucher (eCommerce)
- Personal Digital Assistant
  (u.a. Adressverwaltung, Kalender, Bildverwaltung)
- Berufliche DV-Basis
  (Textverarbeitung, Dokumentenmanagement, Archivierung)
- Navigationsgerät

# 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 ...








# 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 ...





# Wo fallen Daten an?

- TK-Anbieter (GPRS/UMTS-Provider, aber ggf. auch WLAN-Betreiber)
  - Stammdaten (bei Provider)
  - Verbindungsdaten
  - Zugriff auf Inhaltsdaten
- Google (bei Android)
  - Personifizierter Google-Account für (mindestens) Market erforderlich
  - Wer nutzt sein Android-Handy ohne Google-Account?
- Dienste-Anbieter
  - Bei Nutzung von Internet-Diensten offensichtlich, aber:
  - Auch viele Apps verarbeiten Daten nicht im Gerät, sondern auf Servern (z.B. auch bei Spracherkennung => Inhaltsdaten).
- Smartphone Tracking-Dienste
  - Firmen wie z.B. Flurry bieten Application Use Tracking an.
  - Einwilligung?


search recently forecasted that Android adoption will overtake iPhone adoption
Flurry and Pinch Media now, the companies establish uncontested leadership
tics category, **reaching 4 out of 5 iPhone OS and 2 out 3 Android devices**. With
better positioned to help application developers succeed in new ways.

http://www.flurry.com/about-us/merger/faq.html

# Anforderungen an Mobile Geräte

- 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
- Impressumpflichten
- 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

# Anforderungen an Android

- Bewahrung des Open Souce-Ansatzes (Transparenz!)
- Anwendungsneutralität
- Transparente und handhabbare Datenverwaltung, klare Verantwortlichkeiten
- Verarbeitung von Anwendungsdaten im Gerät, nicht bei Dienstleistern
- Datenvermeidungskonzepte z.B. bei Location Based Services, Tracking u.Ä.
- Löschkonzepte
- Zertifizierung von Betriebssystems-Versionen, -teilen und von Applikationen (BSI-Grundschutz, DS-Gütesiegel)





# Aufforderung an Android-Entwickler

- Wo sind die Privacy-Enhancing Tools?
  - Sichere Verschlüsselung für Dateisystem, Mail, Chat, SMS, Voice
  - Opt-out-Tools für Tracking-Dienste


- Privacy by Design
  - Datenschutz als Default => viele Apps verbesserungsfähig!
  - Simpler erster Schritt: Nutzerdaten nur per SSL übertragen
  - Privatsphäre als Alleinstellungsmerkmal am Mark(e)t nutzen!

# Handlungsbedarf

- Frühestmögliche Integration von
  Datenschutz bei Forschung und Entwicklung
- Forschungsbedarf
  bzgl. Software, Oberflächen, Privacy Policies
- Entwicklung von Schutzprofilen für mobile 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





# Datenschutz in mobilen Anwendungen – speziell auf der Plattform Android

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/