

Datenleak – Wie reagiert der Rechtsstaat?

Thilo Weichert, Leiter des ULD
42. Europäische Präsidentenkonferenz
Wiener Advokatengespräche
28. Februar 2014

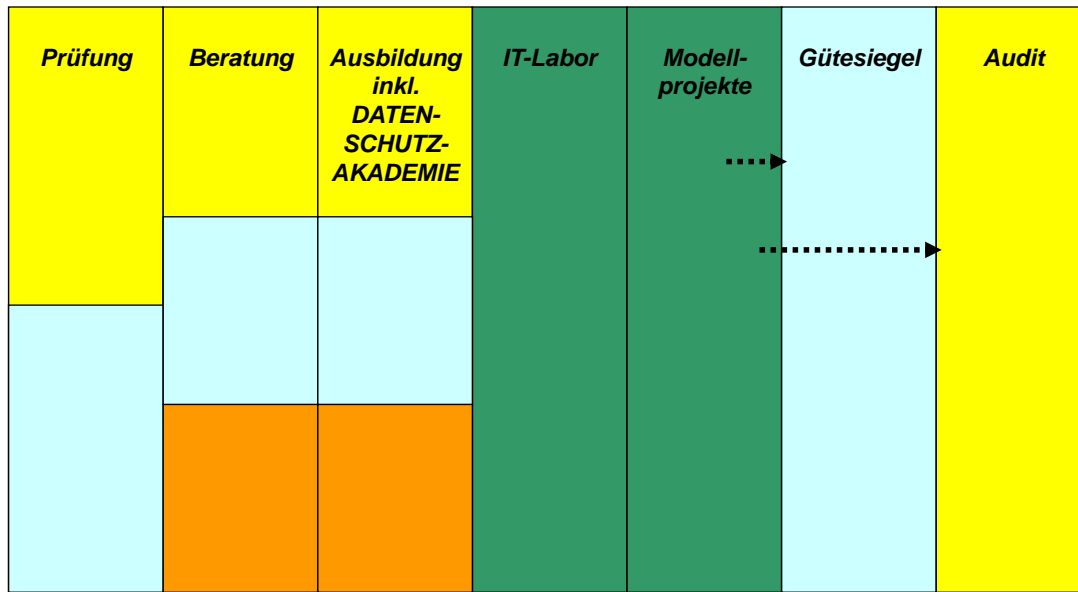


www.datenschutzzentrum.de

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Datenleak?
- Rechtlicher Datenschutzbestand in Europa
- Sonstiger europäischer Grundrechtsstandard
- USA
- Technische Perspektiven
- Gegenstrategien
- Schlussfolgerungen

Datenschutz und Informationsfreiheit



Primäre Adressaten:
 Öffentl. Verwaltungen
 Unternehmen
 Bürger, Kunden, Patienten
 Wirtschaft, Wissenschaft, Verwaltung

Datenleak?

- Edward Snowden = Whistleblowing
- Chelsea Manning/Wikileaks = Transparenz ohne große journalistische Aufbereitung
- Datenzugriff auf Nutzerdaten durch Google, Apple, Facebook & Co. = grundrechtswidrige Geschäftsmodelle
- Hacker-Angriffe auf Portale, Webseiten, Unternehmens- und Privatrechner = Wirtschaftskriminalität
- NSA, GCHQ = staatlicher Datenangriff
- Geheimdienste von Iran, China, Russland, Syrien... = Angriff auf digitale demokratische Grundfreiheiten

Rechtlicher Datenschutzbestand in Europa

- Seit 70er Datenschutzgesetze
- 1980 OECD Datenschutz-Leitlinien zur Verhinderung von Handelshemmnissen
- 1981 Europarat Datenschutzkonvention
- 1983 deutsches BVerfG: Datenschutz erhält Grundrechtsstatus
- 1995 Europäische Datenschutz-Richtlinie
- 2008 deutsches BVerfG: Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme
- 2009 Art. 8 EUGR-Charta: Grundrecht auf Datenschutz

Sonstiger Europäischer Grundrechtsstandard

- Digitale Meinungsfreiheit
- Kommunikationsfreiheit
- Informationsfreiheit
- Zugang zu Verwaltungsinformationen, seit 2013 gem. EGMR auf Art. 10 EMRK mit Grundrechtsstatus
- Digitale Versammlungsfreiheit
- Petitionsrecht
- Digitale Komponente der analogen Freiheit (Religion, Familie, Beruf, Wohnung, Freizügigkeit ...)
- Gleichbehandlung (Diskriminierungsverbot wg. Geschlecht, Abstammung, Herkunft, Glauben ...)

Sonstiger Europäischer Grundrechtsstandard

- Rechtsstaatsprinzip
 - > Verbot mit Erlaubnisvorbehalt bei informationellen Eingriffen
 - > Unabhängige digitale Aufsichtsbehörden (Informations- und Datenschutzbeauftragte)
 - > Anspruch auf gerichtliche Kontrolle
- Zusätzliche Absicherungen:
- Unschuldsvermutung
 - Nemo Tenetur
 - Verbot heimlicher Eingriffe, Offenheit staatlichen Handelns
 - Faires Verfahren, Grundrechtsschutz durch Verfahren

USA

- Keine digitalen Grundrechte (schon gar nicht für Ausländer)
- US-Supreme Court: Reasonable Expectations of Privacy
- Vorrang der Sicherheitsbelange
- Keine (gesetzliche) Bindung von Privaten

1890 - Warren/Brandeis: „Right to Privacy“

1967 - Westin: „Privacy and Freedom“

Seitdem keine rechtsstaatliche Weiterentwicklung trotz verfassungsrechtlicher Grundlagen in Amendments

- > Sicherung der globalen Sicherheitshegemonie
- > Sicherung der globalen wirtschaftlichen Hegemonie

Technische Perspektiven

- Wearable Computing (Smart Glasses, Watches ...)
 - Internet der Dinge (Wohnung, Verkehr, Arbeit, Freizeit)
 - Big Data (komplexe Auswertung)
 - Automatisierte Wirksysteme (Scoring, Rating, Car2Car-Communication, Security-Devices ...)
- > Digitale Diktatur realistisch (möglich)

Gegenstrategien

- UNO-Resolution 26.11.2013: Art. 12 Allgem. Erkl. der Menschenrechte, Art. 17 Int. Pakt für ziv. u. pol. Rechte: „Schutz der Privatheit im digitalen Zeitalter“ = Schutz vor „massenhafter Überwachung, Abhören und Sammeln persönlicher Daten“
- Schutz durch Aufenthalt für Edward Snowden: 12.02.2014 EP-Innenausschuss dagegen
- Internationaler Schutz von Whistleblower
- Sukzessive Kündigung der Kooperationsabkommen mit USA über Roadmaps (Safe Harbor, PNR, SWIFT ...)
- Aussetzung d. Verhandlungen zum Freihandelsabkommen

Gegenstrategien

- Schnelle Verabschiedung der Europäischen Datenschutz-Grundverordnung (Marktortprinzip, europaweiter effektiver Rechtsschutz gegen US-Unternehmen)
- Schengen-Routing
- (Staatliche) Sicherheitsangebote (Ende-zu-Ende-Verschlüsselung, Identitätsmanagementsysteme, E-Government)
- Juristische Aufarbeitung d. NSA/GCHQ-Rechtsverletzungen (nationale strafrechtliche Verfolgung, Klagen vor EuGH, EGMR)
- Diplomatische Sanktionen
- Aktualisierung der nationalen Geheimdienstregelungen

Schlussfolgerungen

- Bisherige Initiativen von Europa greifen zu kurz (Abwiegelungen, No-Spy-Abkommen)
- Massive Unterstützung der Bürgerrechtsbewegungen in den USA
- Kurzfristig: konsequentes Verfolgen eines europäischen Weges (auch im Interesse der heimischen Wirtschaft)
- Mittelfristige Zielsetzung: Internationale digitale Menschenrechts-Charta

Datenleak – Wie reagiert der Rechtsstaat?

Dr. Thilo Weichert

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Holstenstr. 98, D- 24103 Kiel

mail@datenschutzzentrum.de

<https://www.datenschutzzentrum.de>