

Implications for Data Systems: Perspectives on European Privacy Policies and Legislations

Marit Hansen

marit.hansen@datenschutzzentrum.de

**Independent Centre for Privacy Protection
Kiel, Germany**

**Talk at Almaden Institute
April 9, 2003**



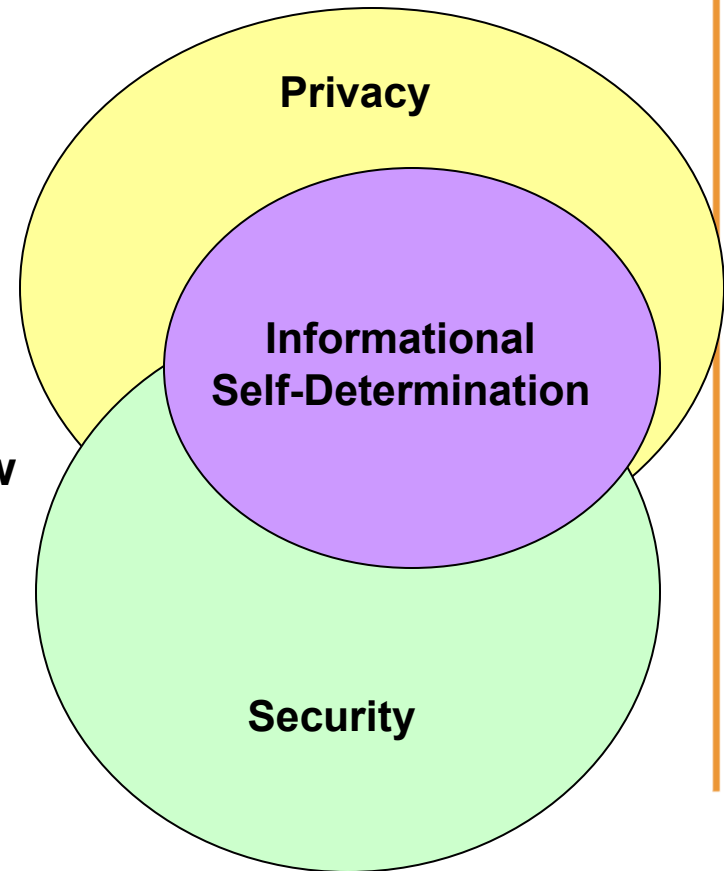
Overview

- **A little bit Terminology on Data Protection**
 - **Privacy, Informational Self-Determination, Security**
- **EU Legal Baseline**
 - **EU Directives, National Legislation, Safe Harbor**
- **EU Policies**
 - **Co-Regulation, Standardization, Funding, Projects**
- **Implications on Data Systems**
 - **Design, Operation, Use, Quality Assurance**
- **Outlook & Conclusion**



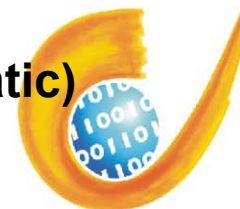
What are we talking about?

- **Privacy**
 - Individual-focused
 - **More than data** is concerned
- **Informational Self-Determination**
 - Focus on the **individual in society**
 - “Everybody should be able to know who knows what about him/her.”
- **Data Security**
 - Focus on **data and processes**
 - Security goals such as
 - Confidentiality
 - Integrity
 - Availability



Europe: Mainly Lawful Regulation

- Protection of information privacy as a fundamental, **human right**
- Tradition of **lawmaking**
- **EU Directive from 1995**
 - Takes a **regulatory and comprehensive approach** to privacy issues
 - Objectives:
 - To **protect individuals** with respect to the processing of personal information; and
 - To ensure the **free movement** of personal information within the EU through the coordination of national laws
 - Broad scope:
 - **All processing** of data (on-/off-line, manual/automatic)
 - **All organizations** holding personal data



General Legal Baseline

- **Right to Informational Self-Determination:**
 - **Directive 1995/46/EC: Data Protection of Individuals**
 - **National law:**
 - **Federal Data Protection Acts**
 - **Additional federal legislation, e.g. Teleservices Data Protection Act, Germany**
 - **in some nations: State Data Protection Acts**
- **Other relevant EU Directives:**
 - **Directive 1997/66/EC: Privacy Protection in the Telecommunications Sector**
 - **Directive 2002/58/EC: Privacy and Electronic Communications**
 - **Directive 1999/93/EC: Electronic Signatures**



Right to Informational Self-Determination

- **Right to Informational Self-Determination:**
 - “Everybody person should be able to know who knows what about him/her.”
 - In Germany derived from the Constitution by Federal Constitutional Court in 1983.
- **What Data? - Personally Identifiable or Identified Data**
 - **What:** data independent from media
 - **Relativism:**
 - For *whom* identifiable?
 - With *which effort* identifiable?
 - *Intention* to identify individuals?
 - **Non-identifiable for an entity:**
No *reasonable* way for the entity to attach the collected data to the identity of a *natural* person



Right to Informational Self-Determination

- **Whose Responsibility:**
 - The **entity** collecting data
 - The consumer himself / herself
- **What Control & Enforcement:**
 - Monitoring (regularly / on specific occasions)
 - **Independent** authorities (governmental / companies)
 - Enforcement (none / fees / usage restrictions)
 - Publicity (blacklisting / press coverage)
- **What Actions:**
 - Obligations of the **entity** collecting data
 - Rights of the **consumer** whose data are collected



EU Directive: Some Principles

- **Notice & Choice**

- Provide consumer with **notice** regarding data collection
- Give consumer **choice** regarding their data
- **Opt-in** instead of opt-out

- **Access**

Provide consumer **access** to allow review

- **Collection and Use Limits**

- **Limit collection/use** to what is necessary
- Kept in identifiable form no longer than necessary for original **purpose**

- **Security**

Provide **adequate security** against improper use

- **Accountability**

- Be **accountable** for legal conformance
- **Auditability** of privacy environment

No Privacy - No Trade
→ **Safe Harbor**





Privacy Commissions

- **Tasks**

- **Guarantee** privacy and data security (as laid down in Privacy Acts)
- Being a **trustworthy advocate** for citizens' privacy rights

- **Approved Methods**

- **Monitoring** use of personal data
- In case of **infringements** of Privacy Acts:
 - Complaint (seldom punishment)
 - Recommendation of improvements
 - Publishing (reports, press)

- **New Methods**

Implementing privacy protection into technologies



Implementing Privacy: No Easy Task ...

- **Art. 8 Directive: The processing of special categories of data**
 - (1) Member States shall prohibit the processing of personal data revealing **racial** or **ethnic** origin, **political** opinions, **religious** or **philosophical** beliefs, **trade-union** membership, and the processing of data concerning **health** or **sex life**.
 - (2) Paragraph 1 shall **not apply** where:
 - a) the data subject has given his explicit consent to the processing of those data, **except** where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or
 - b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
 - c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
 - d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
 - e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.
 - (3) ...



EU Policies

- **Traditional forms of regulation:**
 - **US: self-regulation**, bottom-up, legislating in response to individual privacy problems
 - **Europe: lawful regulation**, command & control, top-down

⇒ **Co-regulation**

- **Standardization:**
 - On national level
 - On European level:
 - CEN (Comité Européen de Normalisation)
 - IPSE (Initiative for Privacy Standardization in Europe)
 - On international level

- **Funding**



IPSE Report on Data Protection 2002

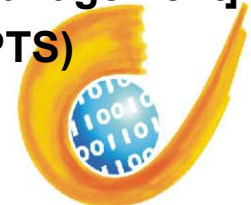
Next tasks of IPSE:

- Identify common European set of voluntary best practices for data protection
- Monitor developments in ISO
- Develop generic set of control clauses and terms (Art. 17 EUD: Security of processing)
- Prepare inventory of data protection auditing practices
- Conduct survey of web seals for future standardization
- Report on impact of technology on data protection incl. PET
- Privacy standards in education and practice



EU Projects and Policies

- **Information Society Technologies (IST) Programme:**
 - Research objective: a **user-friendly information society**
 - “Privacy and identity management”
- **Some Privacy Projects in IST Programme (until -2003)**
 - Pioneering Advanced Mobile Privacy and Security (PAMPAS)
 - Privacy Incorporated Software Agent (PISA)
 - Privacy Enhancement in Data Management in E-Health (PRIDEH)
 - Roadmap for Advanced Research in Privacy and Identity Management (RAPID)
- **Initiatives at Joint Research Centres:**
 - Ispra, Italy: Institute for the **Protection and the Security of the Citizen** (IPSC)
[e.g. P3P Demonstrator, Privacy ontology, Privacy and identity management]
 - Seville, Spain: Institute for **Prospective Technological Studies** (IPTS)
[e.g. Future of Identity in Information Society]



EU Policy: Support of “Privacy-Enhancing”

- Principles for Privacy-Enhancing Technologies (PET)
 - Data **minimization**
 - **Transparency**
 - System integration: **built-in** privacy protection
 - User **empowering**: do-it-yourself privacy protection
 - Multilateral security: **minimal trust** required
- New generation of law
 - Since ~**1997** integrated into law of some EU countries
 - Requirement to **prefer** using / buying / developing PET
 - **Facilitations** for parties using PET



Example: PET in German Law

- **Teleservices Data Protection Act (1997/ 2001)**

§ 4 (6): The provider shall make it possible for the user to utilize and pay for teleservices **anonymously or under a pseudonym** if this is **technically possible** and can be accomplished at **reasonable effort**. The user shall be informed of this possibility.

- **German Federal Data Protection Act (2001):**

§ 3a: **Data reduction and data economy**

Data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data or as little personal data as possible.

In particular, use is to be made of the possibilities for aliasing and rendering persons anonymous, **in so far as this is possible and the effort involved is reasonable** in relation to the desired level of protection.





Privacy Seals

- Many different privacy and consumer-oriented seals
- Privacy seal for privacy IT: Schleswig-Holstein, Germany
 - A **law-based privacy seal** (March 2001)
 - Attests compliance to privacy law
 - Including data minimization, transparency ...
 - Obligation for civil service to prefer the use of products with such seal



Freiwillige
Prüfung durch
RWTÜV nach
Kriterien der
Verbraucher-
Zentrale



Voluntary Validation



Legally based Privacy Seal

- **State Data Protection Act Schleswig-Holstein, 2000**

§ 4 Data avoidance and data economy, data protection audit

(1) The data-processing body shall observe the principle of data avoidance and data economy.

(2) Preference shall be given to products whose **conformity with the data protection and data security provisions** have been established by means of a **formal procedure**.

The State Government shall make orders regulating the content and format of the procedure and who is authorised to carry it out.

- **State in March 2003**

- 3 products with privacy seals
- Approx. 15 in the pipeline



Implications on Data Systems

- **Minimal privacy baseline:**
 - As required by law
 - As enforced by Privacy Commissioners (& press ...)
- **Defining the boundaries:**
 - **“State of the Art”**: possible and feasible, reasonable effort
 - (Explicit) consent
 - PET
- **Implications on**
 - Design
 - Operation
 - Use
 - Quality Assurance



Outlook & Conclusion

- **Effect of PET until now:**
 - Hardly any effect by now, **no PET standard** products
 - Some products with **optional** PET functionality
 - Almost no enforcement: “**State-of-the-art** is enough”?
- **Incorporating PET can become a competitive advantage,**
 - E.g. with privacy seals,
 - Recommendations of privacy commissioners etc.
- **At the horizon: new legislation on data retention**
 - Relationship to data minimization?
 - Always “**dual use problem**”
 - ⇒ **Solutions: seeking a balance**

