How to prevent data breaches

Marit Hansen
Deputy Privacy and Information Commissioner
Schleswig-Holstein

EDPS/ENISA Seminar “Responding to Data Breaches”
Brussels, October 23, 2009

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Setting of ULD in Schleswig-Holstein

Source: en.wikipedia.org/wiki/Schleswig-Holstein

Schleswig-Holstein	
Flag	Coat of arms
 Details	 Details
Location	
	
Time zone	CET/CEST (UTC+1/+2)
Administration	
Country	Germany
NUTS Region	DEF
Capital	Kiel
Minister-President	Peter Harry Carstensen (CDU)

- Data Protection Authority (DPA) for both the public and private sector
- Both privacy and freedom of information
- Projects on EC level in 2009:

PrimeLife

fidis

OS PRIVACY

EuroPriSe European Privacy Seal

www.maps-for-free.com

Data breaches also in our region

- In 2008 several incidents
- 6 million customer data records including
  - financial accounts,
  - phone numbers,
  - sometimes age or profession

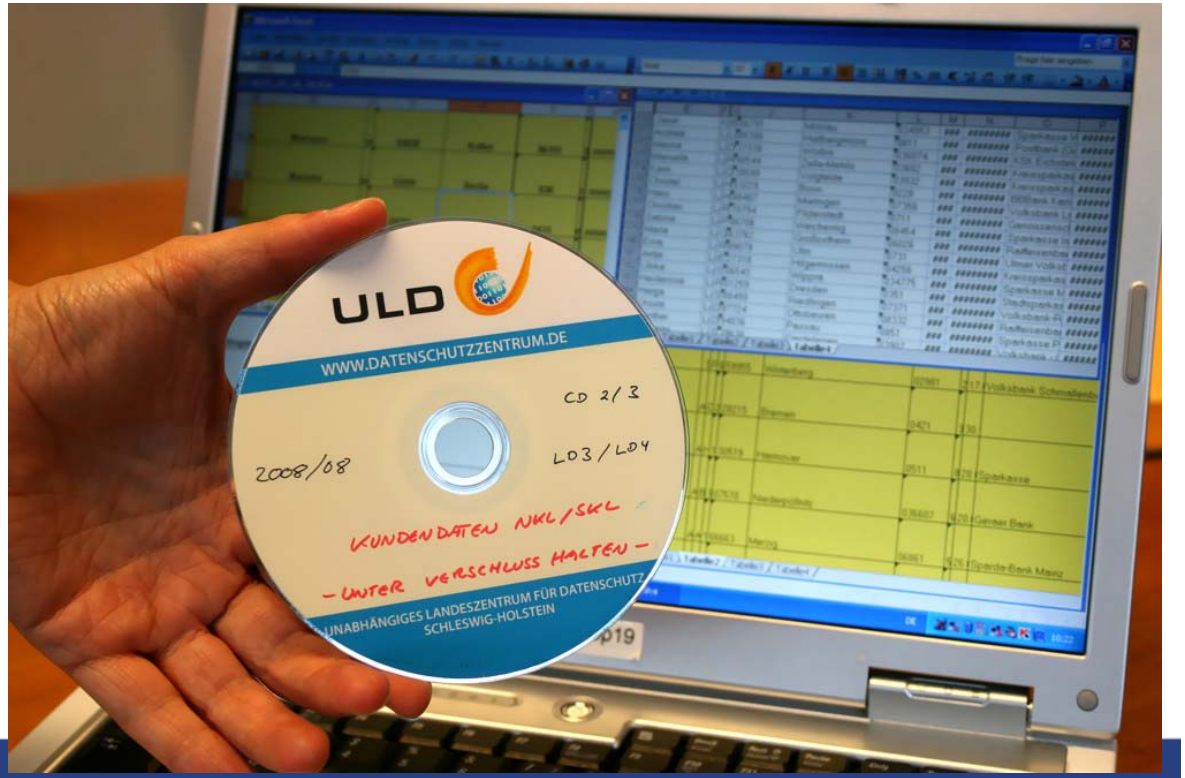


Photo: Markus Hansen, ULD

Overview

- Perspective of a supervisory authority
- European Privacy Seal as a solution?
- Data Protection Management Systems
- The full picture

Perspective of a supervisory body

To prevent data breaches:

be compliant with the data protection law
and minimise risks by privacy-enhancing technologies

⇒ Have a look at the EuroPriSe criteria

EuroPriSe
European
Privacy Seal

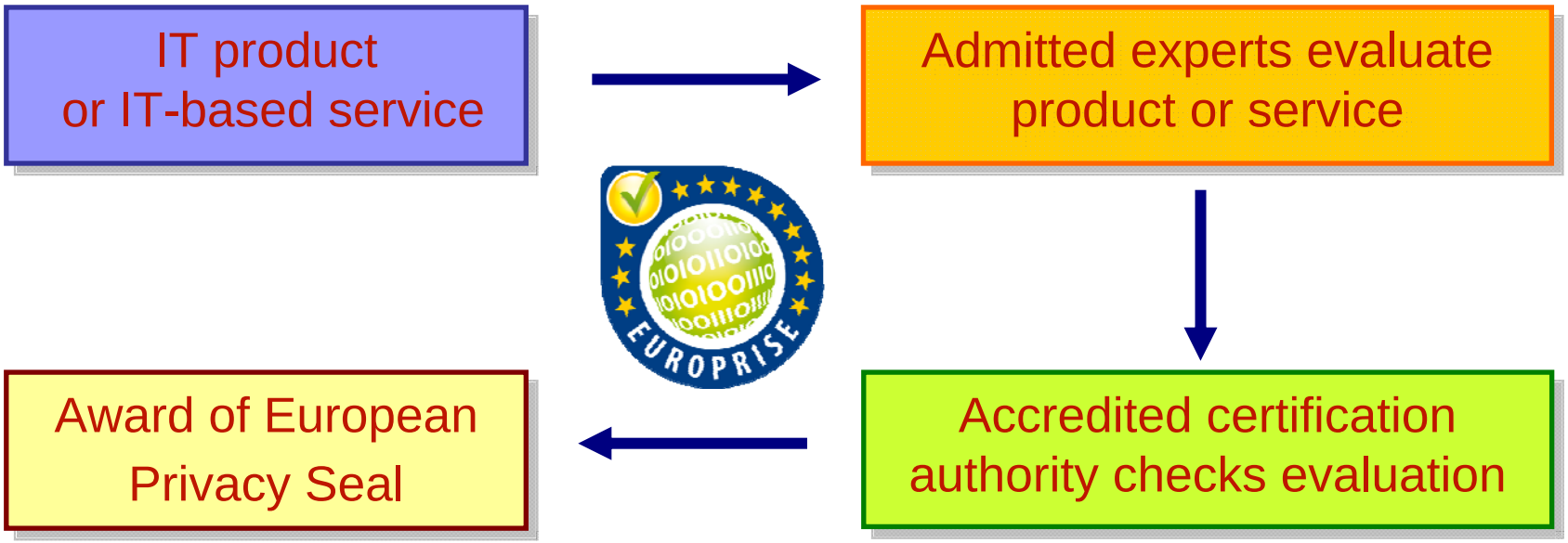
Scope of EuroPriSe

The European Privacy Seal certifies that an IT product or IT-based service facilitates* the use of that product or service in a way compliant with European regulations on privacy and data protection.

*) “facilitates the use” = allows to use it in an easy way

© EuroPriSe®

EuroPriSe Procedure



Validity: 2 Years

EuroPriSe Certification Criteria

1. Fundamental issues
   - Data minimisation
   - Transparency
2. Legitimacy of data processing
   - Legal basis
   - Purpose limitation
   - *Note: also for log data!*
3. Technical-organisational measures
   - Security safeguards
     Incl. separation of data, encryption, logfiles, security policy, risk analysis, test & release, incident management, ...
4. Data subjects' rights
   - Provision of info / notification
   - Right of access, correction, erasure, objection
   - In comm.networks: right to be informed of security risks

maybe
No risk: no fun!

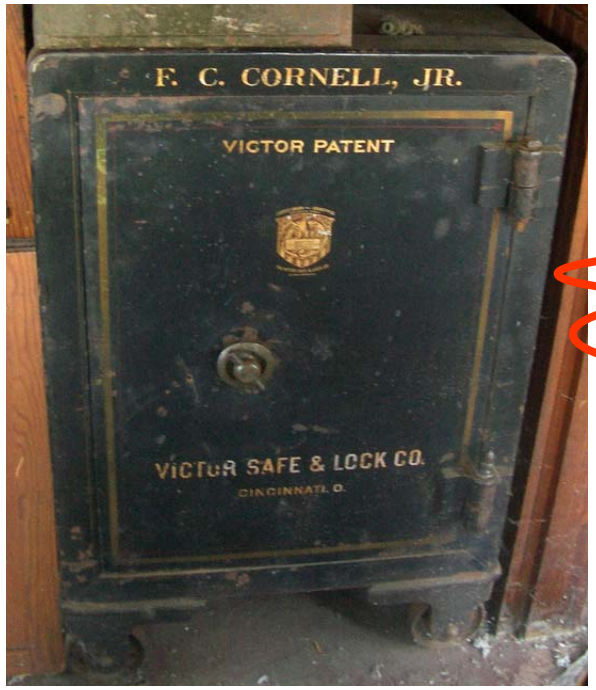
No personal data ⇒ no risk

⇒ Data minimisation

Directive 95/46/EC, Recital 46

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

Directive 95/46/EC, Art. 17



Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Two important properties of ICT security

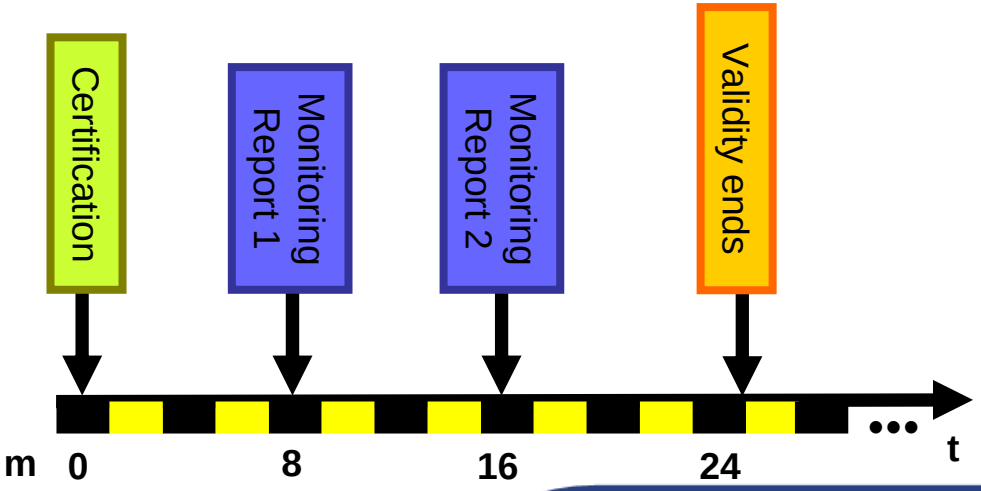
1. Security is like a chain – only as secure as the weakest link.

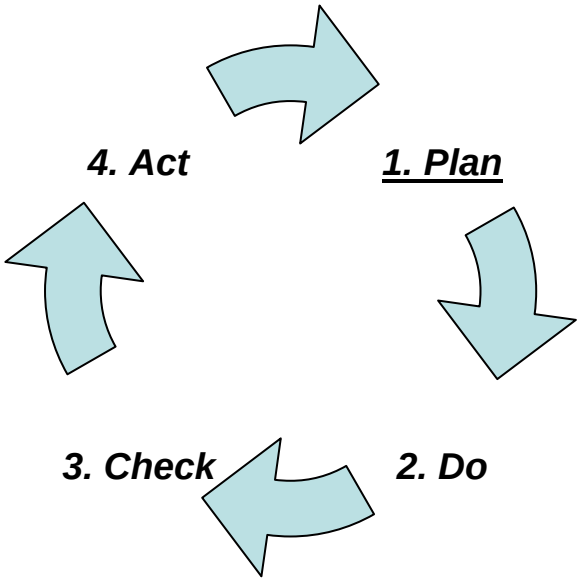
2. Security is not a status, but a process
   – effort is needed to keep the desired level over time.

Data Protection Management System

- ISMS = Information Security Management System
- Analogue: Data Protection Management System
  - Permanent tasks in defined processes (derived from ISO 9000 quality management)

EuroPriSe approach:
monitoring for IT-based services





Deming Cycle

~~Three~~ Two important properties of ICT security

1. Security is like a chain – only as secure as the weakest link.

2. Security is not a status, but a process
   – effort is needed to keep the desired level over time.

3. There is no 100% security – at least it's not affordable.

   ⇒ Establish processes to deal with data breaches

Full picture

- Be compliant with the data protection law
  and minimise risks by privacy-enhancing technologies

- Technological solutions alone are not sufficient:
  Risks may also stem from
  - Overgrowing complexity
    of ICT systems
  - Dependencies, e.g.,
    from admins or data processors
  - Unaware staff
  - Disgruntled employees

Cathy Cole

Conclusion

- EuroPriSe plays a role in preventing data breaches
- Legally demanded breach notification processes of IT products or IT-based services are part of the EuroPriSe evaluation
- Data Protection Management Systems complement Information Security Management Systems: regular and ongoing checking necessary
- Think of the full picture!

Thank you for your attention!

Any questions?

Marit Hansen
ULD6 (at) datenschutzzentrum.de

EuroPriSe
European
Privacy Seal

www.european-privacy-seal.eu

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein