OSCE/ODIHR visions and data protection challenges for the use of population registers on a European level

eID and Public Registers

Hradec Králové, 07. April 2009

Kirsten Bock

ULD

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Unabhängiges Landeszentrum für Datenschutz
Independent Centre for Privacy Protection

- Office of the Privacy Protection Commissioner of Schleswig-Holstein, Germany

- 45 employees

Independent Centre for Privacy Protection

Control	Consulting	Education incl. DATEN-SCHUTZ-AKADEMIE	IT Lab	Model Projects	Privacy Seal	Audit
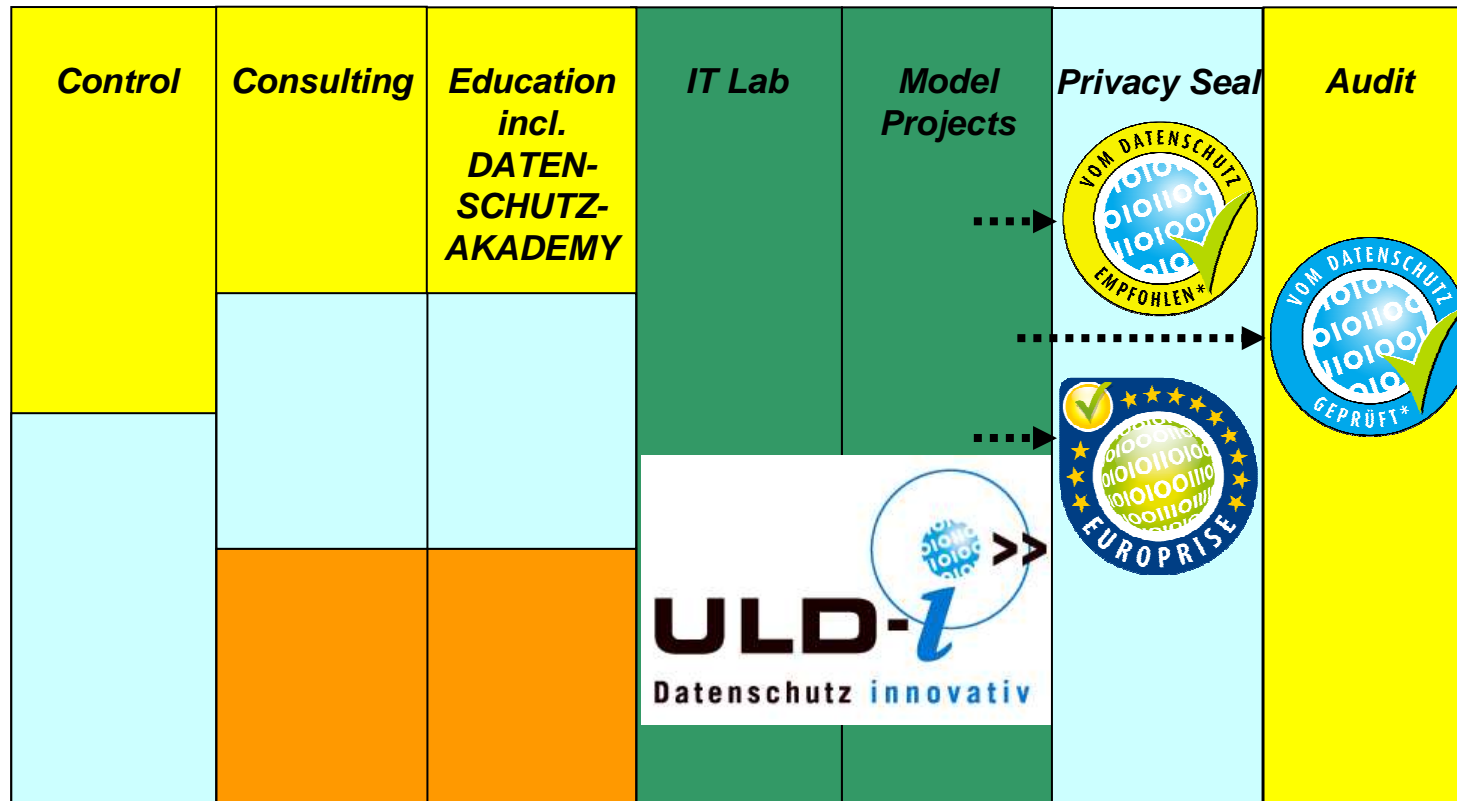
Primary Addressees:

- Administration (yellow)
- Business (light blue)
- Citizens (orange)
- Business, R&D, Administration (green)

OSCE/ODHIR Visions

OSCE/ODIHR Guidelines on Population Registration

- Work in progress
- Population registration and OSCE commitments
- ODHIR's approach to population registration
- Description and content of population registration
- Guiding principles and benefits
- Legislative framework
- Technical framework

Concept of Population Registration

- Registration of civil + life events

| Birth | Death | Marriage | Partnership | Adoption | Citizenship |

...

- Registration of place of residence

Main Elements of Legislation

- Responsibility
  - Tasks and powers
- Content
  - Civil events (life/vital and status), address
- Organisation
  - Central or local registers
  - Paper based, electronic
- Procedures
  - Registration
  - Data sharing among authorities
  - Controlling
- Protecting and ensuring rights of data subjects
- Data Security

Legal Framework

- Rule of law

- Purpose specification

- Collection limitation & data minimization

- Use, retention and disclosure limitation

- Accuracy and quality

- Openness and transparency

- Access

- Accountability

- Security Safeguards

Data Protection Challenges
for the use of Population Registers
on a European Level

Data Protection Challenges on European Level

- Availability of information poses new risks
- Obligation to register and the fundamental right to informational self-determination must be balanced
- Each step of processing of personal information requires a legal basis
  - Collection
  - Sharing
  - Disclosure
- Purpose specification must be consistent throughout Europe, e.g. IDnumber
- Control tasks must be assigned
- Protection of data subjects rights must be ensured and enforceable even if place of residence and place of processing are on different national territory
  - Different DP requirements and procedures compromise effective protection

Different Perspectives: Registers and ...

Privacy

Security

Identity Management

Legal
Technical
Organisational } **Approaches**
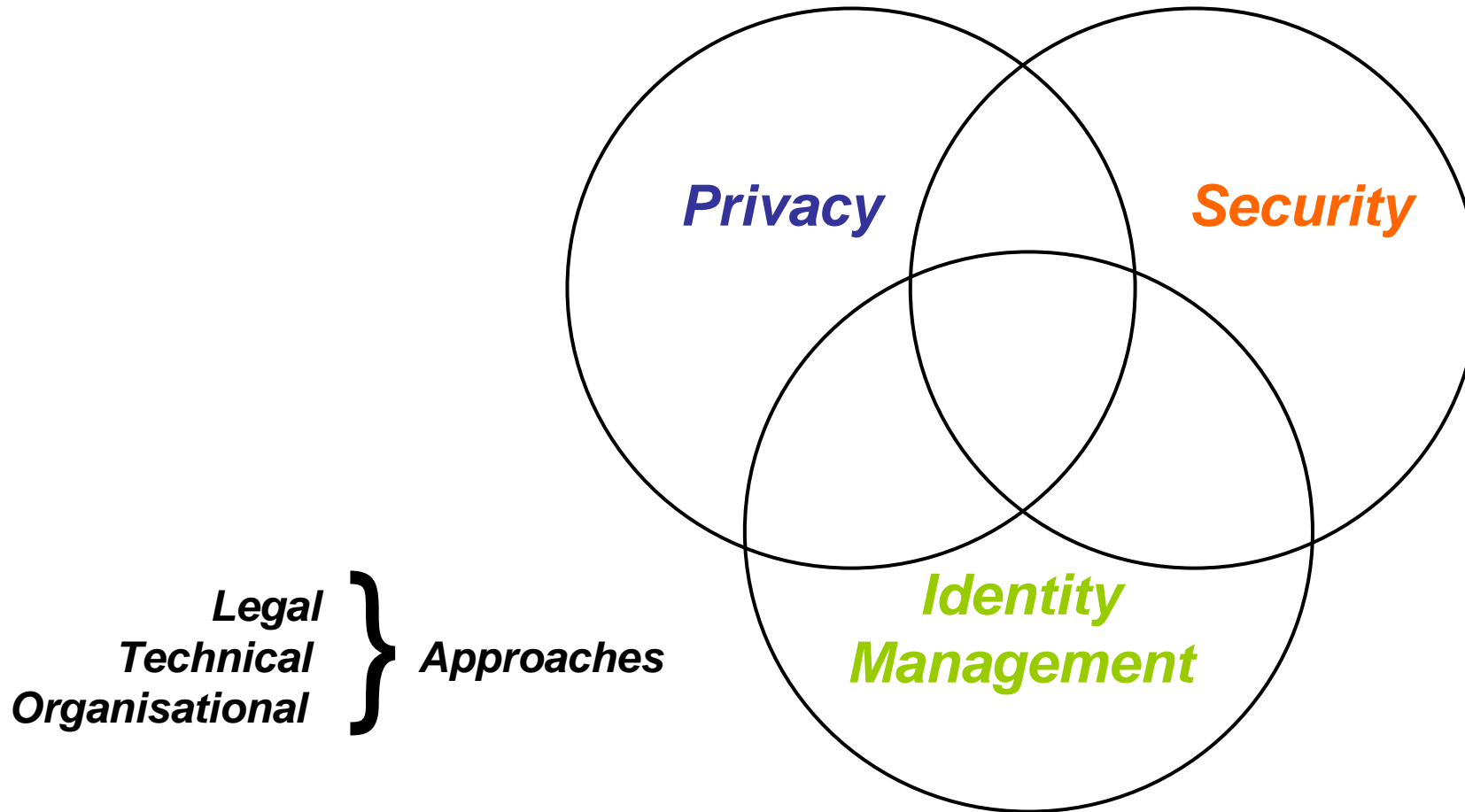
Identity Management in Civil Registration

- "Account management" for citizens

- "User-controlled identity management"

Population Registers and Privacy

- Objectives:
  - Respecting the individual's privacy
  - In line with data protection regulations
- Criteria:
  - Data minimisation
  - Purpose specification, use limitation
  - Separation of data for specific sectors
  - Information of individuals
  - Empowerment of individuals to exercise their right to privacy, e.g. design of ID-cards

Population Registers and Security

- Objectives:
  - Safeguards for personal information
  - Integrity of administrative decisions
- Criteria:
  - Confidentiality, integrity, availability
    - Data on eID media
    - Data in back office system
    - Data while being transferred
  - Multilateral security requirements, e.g. mutual authentication
  - For eIDs: On-line key generation on card
  - End-to-end security
  - Non-repudiation
  - Protection against Identity Theft

Population Register and Identity Management

- Objectives:
  - Communication management
  - Address and reachability management
- Criteria:
  - Support of the individual's sovereignty in managing their own identity
  - Separation of contexts:
    different identifiers, different keys, …
  - Traceability of own identity-related information
  - Interoperability

Some Privacy-Enhancing Technology (PET) Components Related to Civil Registration

- Workflow design for separation of contexts
- Sector-specific PINs
- Server-side derived IDs
- Private credentials

Conclusions

- Objective: Citizen centred approach
- In particular: Respect the citizen's right to privacy
  - By minimising personal data and their linkability
  - By enhancing the understanding of processes
  - By enabling informed choices

More Information

Projects:

- RISERid – Registry Information on European Residents
  http://www.riserid.eu

- EuroPriSe – European Privacy Seal
  https://www.european-privacy-seal.eu

- PrimeLife   http://www.primelife.eu/

Concepts:

- Sector-specific PINs: http://www.a-sit.at/pdfs/20070228%20MODINIS-WS5%20Case-Austria.pdf

Thank you very much for your attention!

Kirsten Bock

kbock@datenschutzzentrum.de