PRISE – Privacy and Security

Copenhagen 29 January, 2007
Workshop A

Mapping of privacy impacts and options for privacy enhancing design

Maren Raguse
Independent Centre for Privacy Protection
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein, ULD

D-24103 Kiel, Holstenstr. 98
Tel.: +49-431-988-1284
Fax: +49-431-988 1223
mailto:prise@datenschutzzentrum.de
http://www.datenschutzzentrum.de/prise/

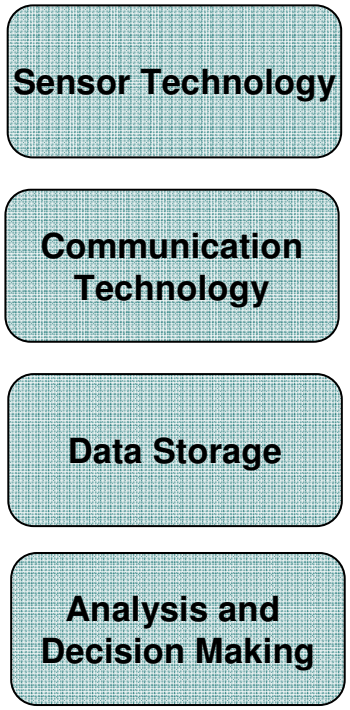
Agenda

- Legal Work in PRISE
  - Privacy impacts of security technologies
  - Limits of privacy restrictions in the context of police powers
- Proposals
- Questions

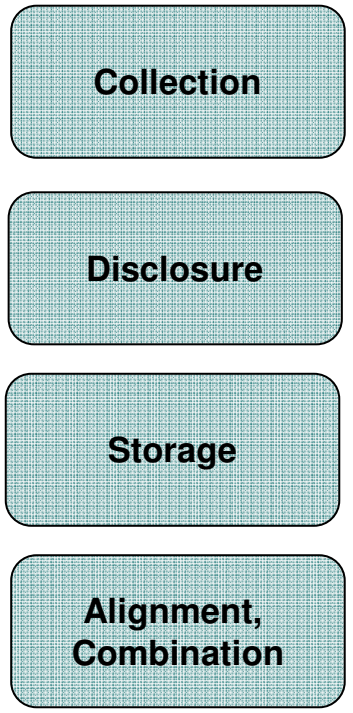
Legal Work

- Privacy impact determined by technical features

Identified Basic Technologies:



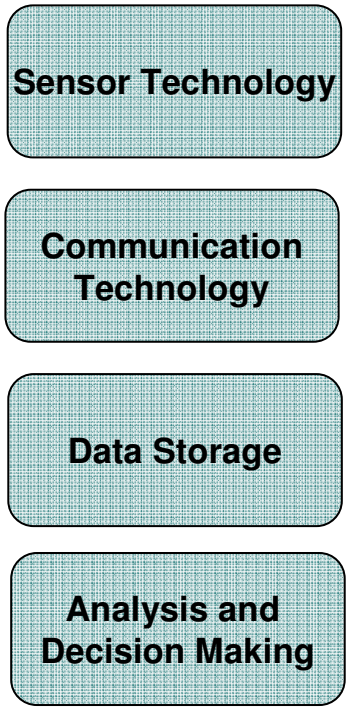
Related data processing:



Legal Work

- Privacy impact determined by technical features

Identified Basic Technologies:



Known privacy threats:

- Lack of transparency
- Violation of purpose binding
- Remote collection of sensitive data
- Necessity to collect data?

- Lack of transparency
- Violation of purpose binding
- No sufficient protection (authentication, encryption)

- No sufficient protection (authentication, encryption)
- Linking of data from different sources
- Retention of data without concrete suspicion - Proportionality

- Lack of transparency
- Violation of purpose binding
- Proportionality

Legal Work in PRISE

- Privacy impact determined by legal provisions

Collection of Information

- Regulated in national law
- Use of technology and thus impact on privacy is determined by national law (exception: ePass)

Sharing of Information

- Approach on European Level: Prüm Convention (outside EU framework) on information exchange of fingerprints and DNA
- Focus of German EU Presidency

Legal Work in PRISE

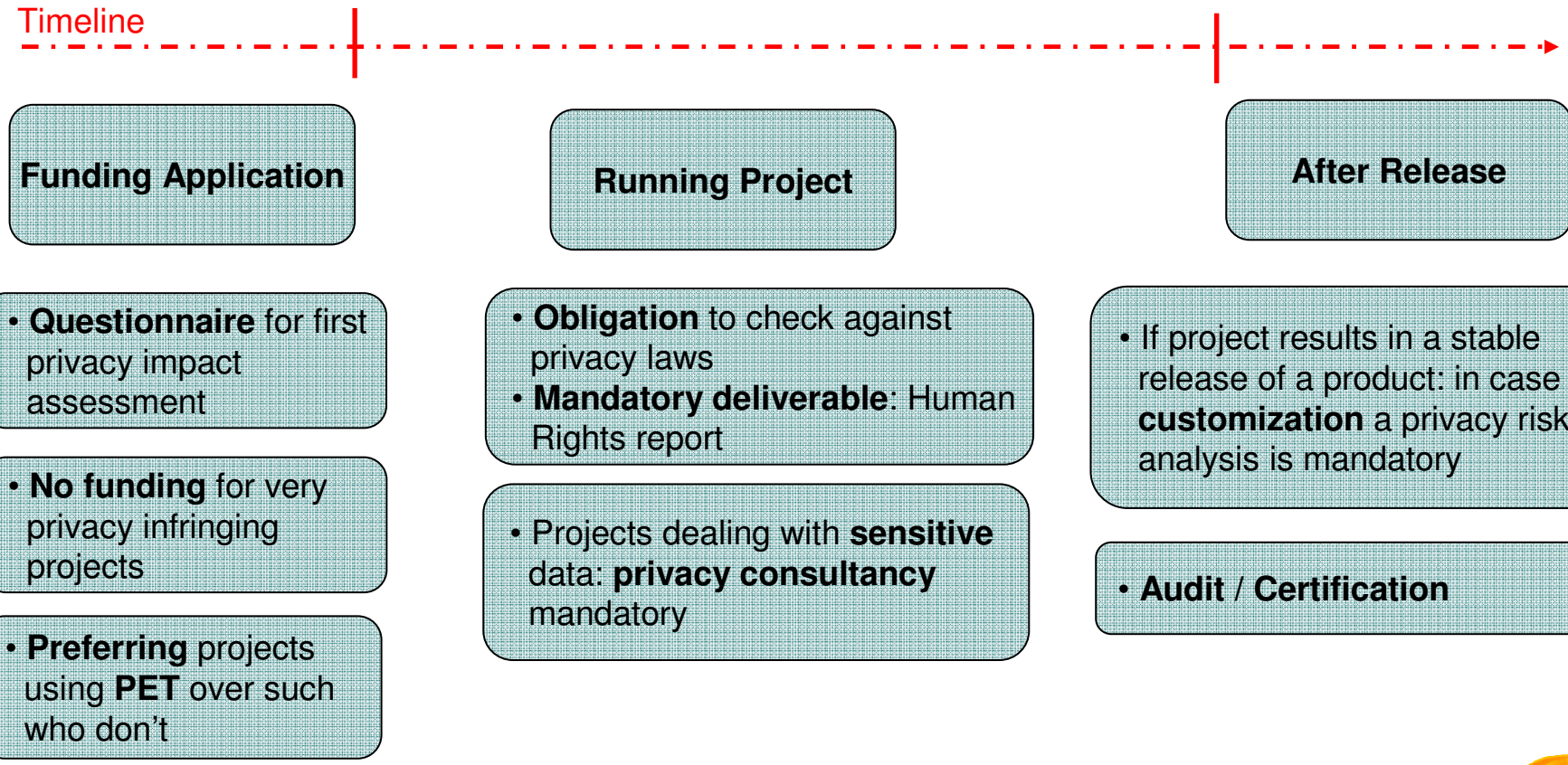
- Minimum Level of Privacy

  Example: German Constitutional Court rulings

  - Court has acknowledged a core sphere of privacy which may not be infringed
  - This core sphere covers intimate and personal conversations and expressions in the suspect's domicile
  - Preventive surveillance and investigation (without a concrete suspicion of a criminal act) require a concrete enumeration of crimes which may initiate the investigative measure at question
  - The general threat of possible terrorist attacks is not sufficient to justify a computerized screening of databases (i.e. from universities or commercial sources); a concrete threat to significant rights must exist

PRISE Proposals

- Organisational:
  Privacy Rights / Ethical Check upon Application for FP7 Funding



PRISE Proposals

- Legal Proposals:
  - Mandatory prior checking for security technologies with a strong impact on privacy (efficiency of technology, level of privacy impact, used based on a concrete suspicion or on a general suspicion?)
  - Mandatory evaluation of new police and secret service powers after a short-term period (2-3 yrs)
  - Introduction of sunset clauses (law expires if no or a negative evaluation is conducted)
  - Police information sharing

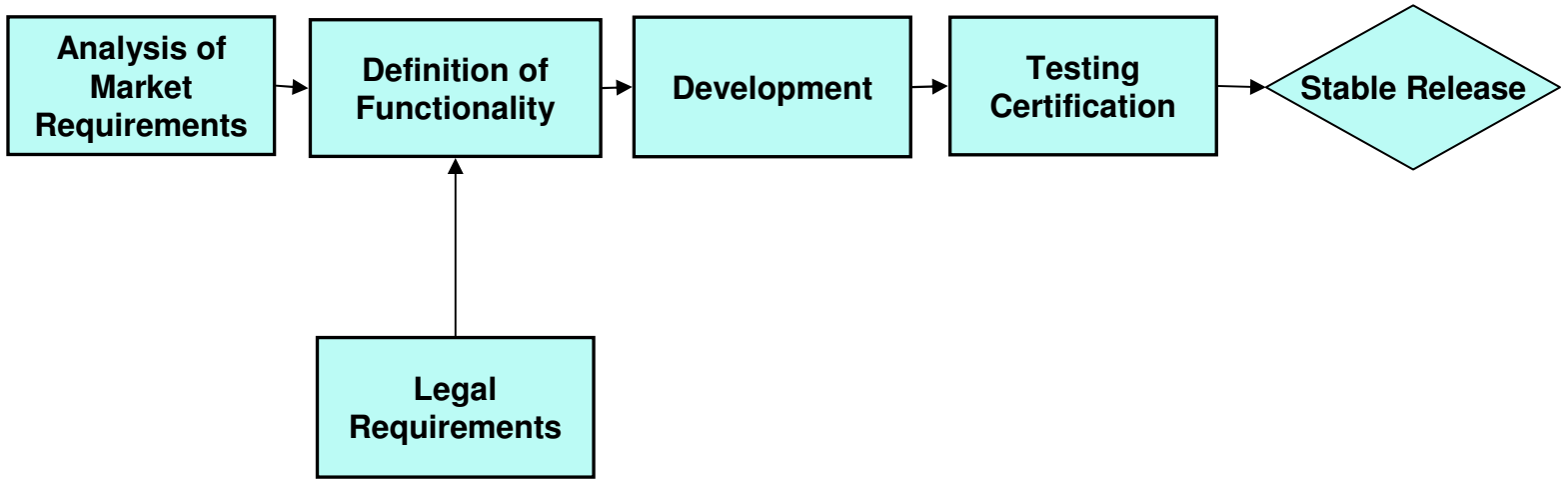
    Outside EU: only if adequate level of data protection

    In Europe: merging information from police and intelligence sources requires the introduction of clear provisions on which information may be shared and by whom it may be used; separation of intelligence and police might be circumvented

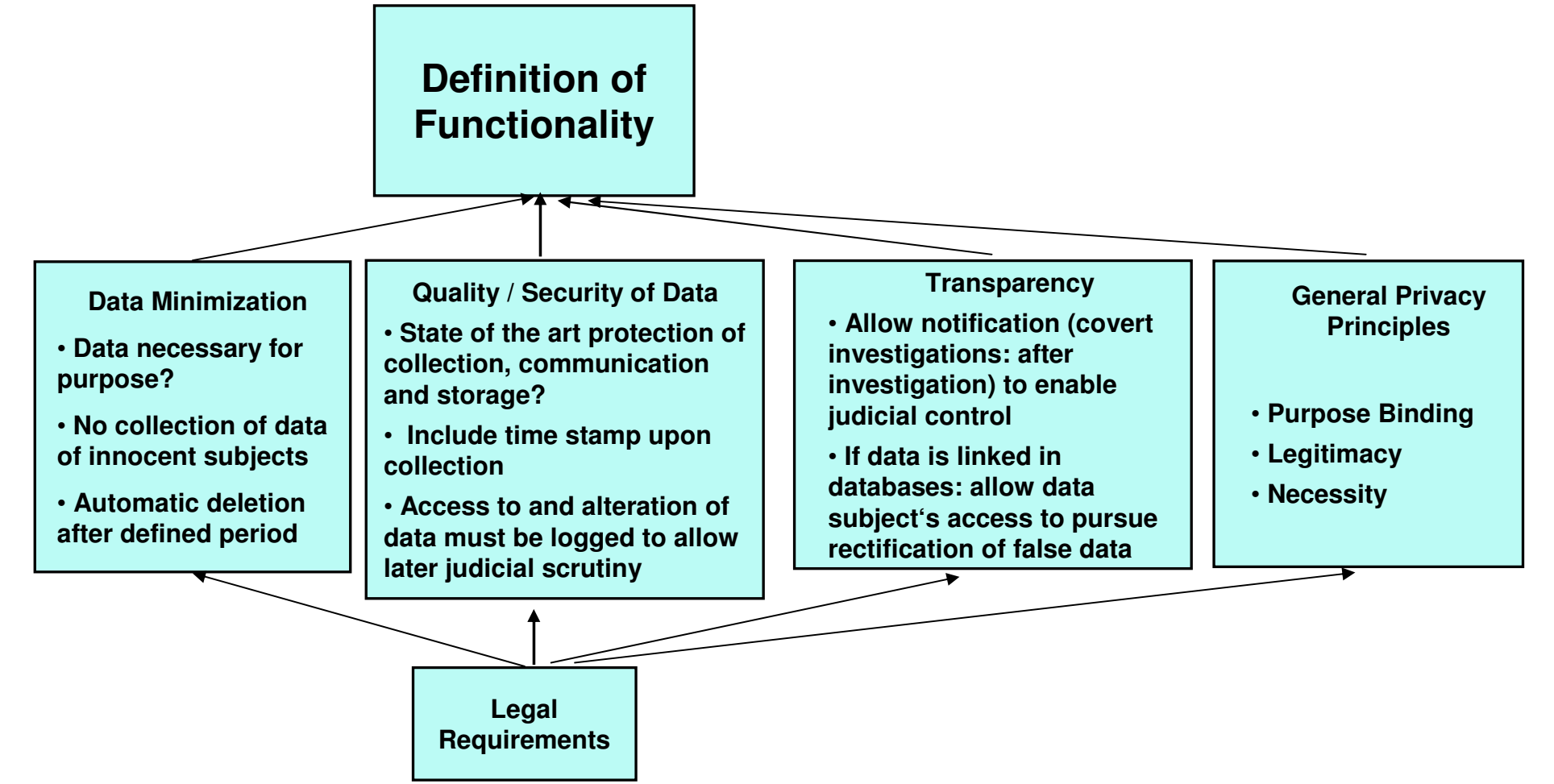
PRISE Proposals

- Privacy impact of security technologies is determined by technical features of the technology and legal provisions on the application of the technology

Research and Development process



PRISE Proposals



Questions

- Directive 1995/46/EC allows for restriction of privacy in order to safeguard public security. What limits exist to this restriction of privacy?

- As the actual intensity of privacy impact of a security technology is determined by national police law, what approach on a European level is possible at all?

Thank you

Backup slides

More Questions

- How can PRISE address not only EU research (via FP 7 funding) but impact national research; is this a reasonable aim?

- Standardisation of security technology is, due to interoperability reasons, often not decided on only by the EU but rather by international standardisation bodies like ICAO. How can the EU influence this process more and introduce European privacy standards in these bodies instead of arguing the EU has to comply with standards in place?

- PRISE proposes the introduction of Data Protection Management into security research and development in order to operationalise data protection compliance. Can EU driven efforts impact what kind of customised technology national law enforcement authorities apply or will EU 'competence' be denied by pointing at the context between national police law and technology used by police authorities?

More Questions

- Will the introduction of Data Protection Management be an efficient approach to bring about data protection compliance considering the fact that companies developing security technologies aim at selling their products to as many buyers as possible and thus may tend to follow their – not necessarily privacy friendly – demands?

- Privacy compliance and even privacy enhancement can be a competitive advantage in selling products customers can trust in. Is this consideration relevant at all in the context of security technology? Security technologies are used with the justification to fight organised crime and terrorism and thus claim to aim at protecting citizens. Is there a public lack of trust in these technologies which could be appealed to? Or do governments basically not have to fear the citizens' response to intense security measures and thus possibly privacy infringing technologies? Does privacy compliance thus not work as a competitive argument in the context of security technology?

More Questions

- Could this antagonism (the state as legislator of police powers and at the same time buyer of security technology driving the implementation of features which may be privacy intrusive vs. the state as legislator and keeper of privacy and human rights) be resolved by making a prior checking of security technology mandatory? This would include a civil rights risk analysis and a prior evaluation of the human rights impact of a technology used by law enforcement authorities.

- Which instruments exist on a European level for the introduction or maintenance of a reasonable level of privacy even under the Article 13 restriction (the right to privacy may be restricted when such a restriction constitutes a necessary measures to safeguard public security)?

More Questions

- Is a mandatory evaluation of anti-terrorism legislation and other privacy infringing laws and the introduction of sunset clauses (which will lead to an expiry of a law which has not been evaluated positively) a reasonable step to put more emphasis on the protection of privacy and human rights?

- Security technologies can foster the collection of data/information and/or the further sharing of these collected data. The German EU Presidency puts a focus on advocating the sharing of collected data in linked databases by introducing the Prüm Convention into the EU legal framework. What requirements should the continuous sharing of data meet? Also not verified information collected by intelligence agencies may be shared. This may lead to false suspicions. Is the merging of police and intelligence information reasonable?

More Questions

- What restrictions need to be introduced concerning a US or other third countries' access to the joint database? Or should an operationalised and automated access be denied at all?

- It is difficult for the supervising national data protection authorities to enforce privacy compliance of technologies used during police investigations. Often a detailed analysis of security technologies is rejected by police or other responsible authorities. Are the existing legal provisions sufficient (and currently just not applied entirely) or is an amendment of the supervising regulations necessary? Or is the enforcement of privacy compliance in the context of security technologies left up to the judiciary system of the Member State?

- What steps would support the enforcement of data protection compliance of security technologies?

PRISE Proposals

- Organisational:

  Privacy Rights / Ethical Check upon Application for FP7 Funding

  - Funding Application phase

    PRISE will draft a questionnaire allowing privacy impact assessment.

    No funding shall be granted to very privacy infringing projects

    PRISE will advocate projects using PET shall be preferred over such projects which don't use PET
  - Accepted Projects:

    Projects obliged to check their project against privacy requirements and address Human Rights compliance in a deliverable

    Projects dealing with sensitive data: privacy consultancy mandatory
  - After Release:

    In case of customization or changes in the product: privacy risk analysis mandatory

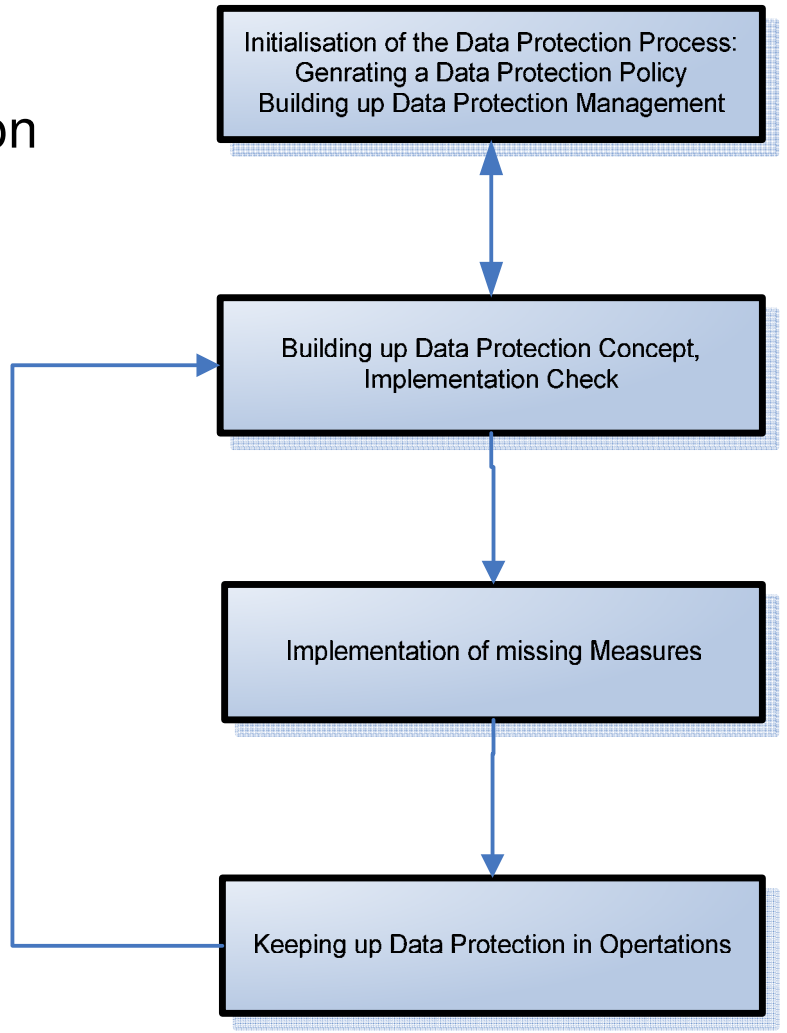
Data Protection Management

- Organisational:

  Introduction of Data Protection Management in R&D

  Taking into account:

  Protection Profiles



Data Protection Management

- Organisational:
  Introduction of Data Protection Management in R&D