The PRISE Framework

Walter Peissl
Maren Raguse

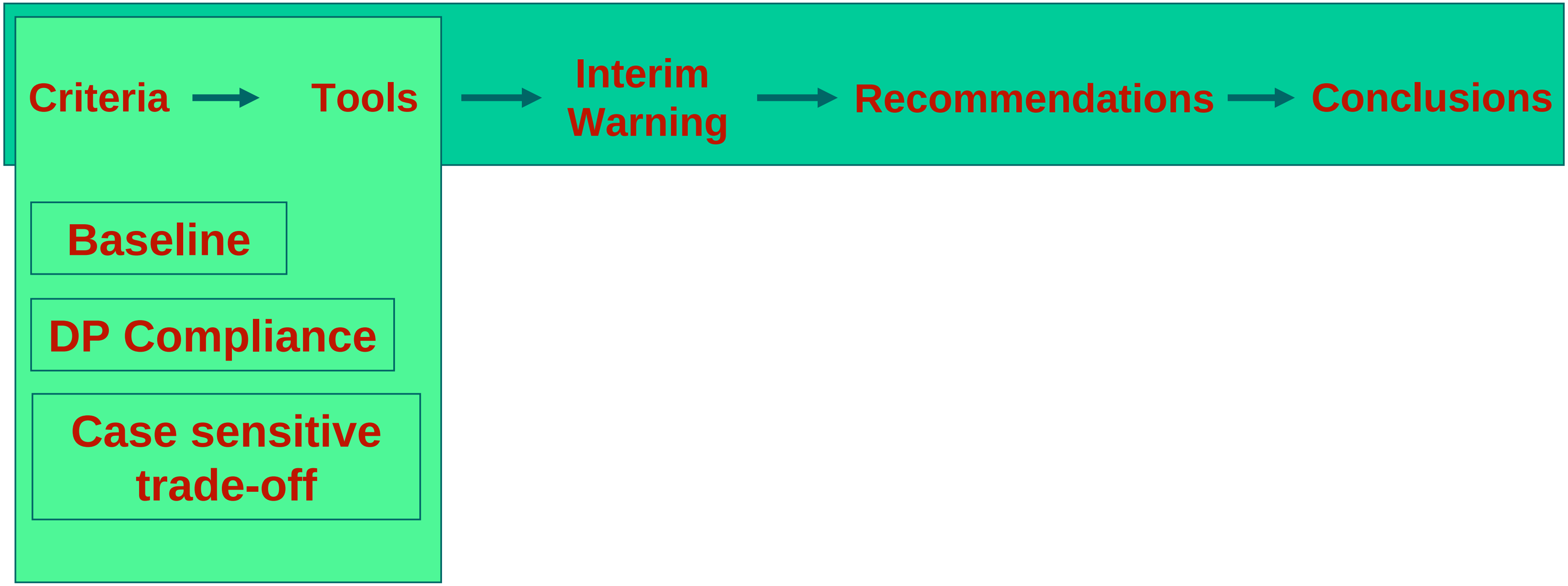
INSTITUTE OF TECHNOLOGY ASSESSMENT

Independent Centre for Privacy Protection

Agenda – The PRISE Framework

- Structure
  - The PRISE-matrix
  - The PRISE-handbook
  - The PRISE-check-list forms
- Existing approaches / standards
  - Product related
  - Process related
- 3 Layers
  - Legal
  - Organisational
  - Technical
- Examples of tools
- PRISE visions

The PRISE-Matrix



Criteria → Tools → Interim Warning → Recommendations → Conclusions

Baseline

DP Compliance

Case sensitive trade-off

The PRISE-Matrix

	Criteria	Tools			Warning Interim Status	Recommendations forÉ		Conclusions
	Questions	Legal	Organisational	Technical	Red/ Green Light	R&D	Users	
Baseline								
Data protection compliance								
Context sensitive trade-off								

The PRISE-Handbook

- Content of the PRISE-Matrix
  - Tools column
- Guidance for proposal writers
- Guidance for evaluators
- Guidance for R&D in general
- Guidance for users of security technologies

The PRISE-check-list forms

- Two forms, basically the matrix
  - form for proposal writers
  - form for evaluators
- Yes/No
- References to the PRISE-handbook
  - Proposal writer may find guidance
  - Evaluators may assess whether the tools are applied or not

Existing approaches / standards

- Categories: product or process related
- Main focus on IT-Security; approaches wrt Privacy and Data Protection exist too
- Standards in IT- Security
  - Common Criteria (ISO 15408)
  - Baseline Protection (ISO 27001; 17799, 27002)
- Approaches wrt Privacy:
  - Privacy Impact Analysis (PIA), e.g. Canada, UK, Australia, USA: DHS
  - CEN: Personal Data Protection Audit Framework
  - Certification schemes: regional in Schleswig-Holstein; European under development: EuroPriSe

Categories: product related / process related

Product related:

- Common Criteria
- Personal Data Protection Audit Framework
- Certifications schemes of Schleswig-Holstein and EuroPriSe
- PIA

Process related

- Baseline Protection
- Personal Data Protection Audit Framework

3 Steps, 3 types of tools:

- Assessment of privacy impact in three steps (Matrix)
  - Minimum level: intimate data
  - Privacy compliance
  - Context-sensitive trade-off

- Three types of tools to mitigate identified impact:
  - Legal (usually not applicable for consortium)
  - Technical
  - Organisational

Minimum level of protection: core sphere

- Core Sphere of private life style:
    - Derived from fundamental right of human dignity
    - Place of “last retreat” from the state
    - Right to unimpaired development and execution of very private actions
- Data concerning Core Sphere of private life style shall not be processed

Tools regarding core sphere

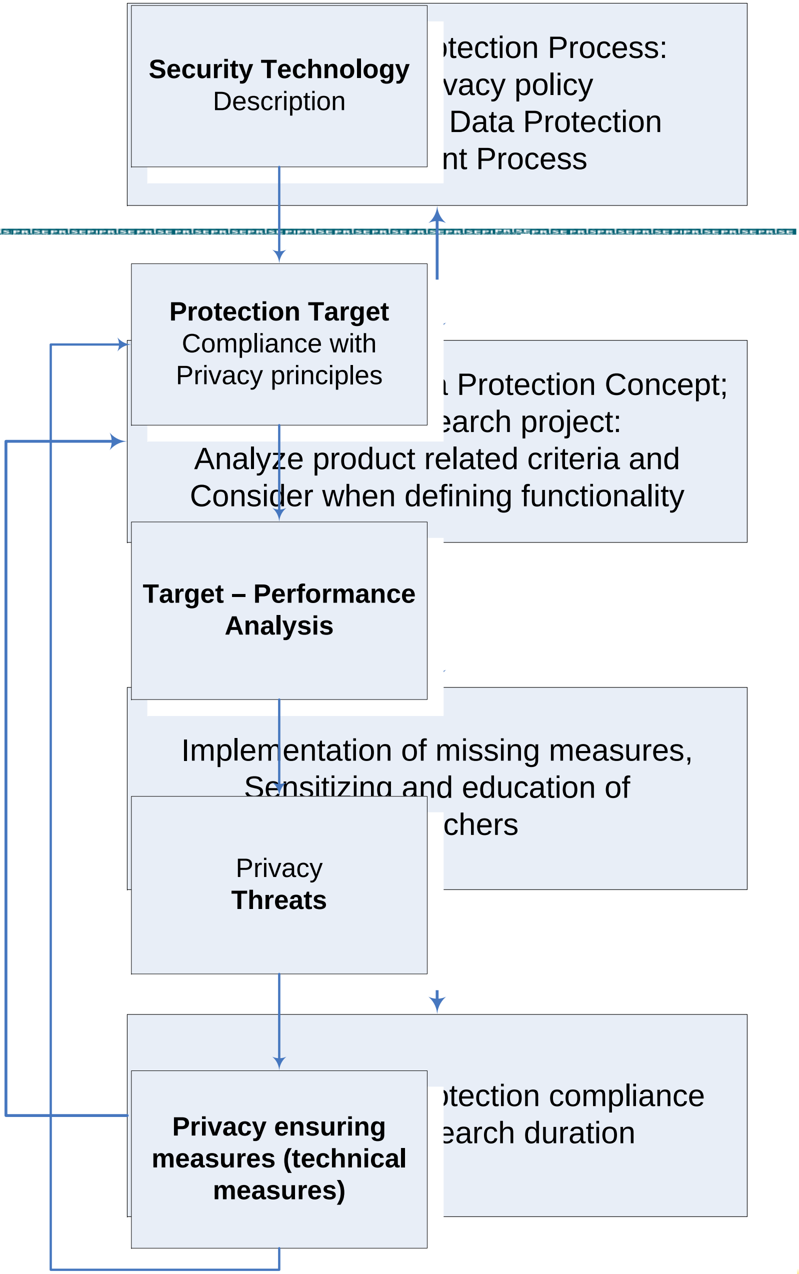
- Currently technically impossible to automatically identify core sphere data
- Hence, technology must allow
  - live monitoring of collection
  - immediate interruption of collection
  - audit trails (logging of use) to allow judicial scrutiny
- Legal: explicit regulation of intimate sphere protection; mandatory notification of data subject; court order

Tools regarding core sphere

- Legal:
  - mandatory security laws evaluation (alternatives? necessity?)
  - explicit regulation of intimate sphere protection
  - mandatory notification of data subject
  - court order
- Organisational:
  - manual for user of security technology
  - written information and training regarding intimate sphere

Privacy compliance

- Legitimacy
- Purpose Binding
- Proportionality
- Transparency
- Quality of Data
- Data Security



Security Technology Description

tection Process:
vacy policy
Data Protection
nt Process

Protection Target Compliance with Privacy principles

Protection Concept;
earch project:
Analyze product related criteria and
Consider when defining functionality

Target – Performance Analysis

Implementation of missing measures,
Sensitizing and education of
chers

Privacy **Threats**

Privacy ensuring measures (technical measures)

tection compliance
earch duration

Tools regarding Privacy Compliance

- Main technical tools: PETs
  - Data minimization, including unlinkability, anonymity and pseudonymity
  - Safeguards for personal data, e.g. encoding of rules and policies
  - Control by the user
  - Transparency of the system
  - Audit and checks
- Main organisational tools: DP Management Process (R&D and later user)

Context sensitive trade-off

- technology complies with privacy principles
- known security gain negligible

or

- technology does not comply with privacy principles
- known (estimated) security gain high

- Main problems
  - Assessment of security gain
  - Proportionality

PRISE envisions...

- Consortia thoroughly consider privacy impact prior to submitting proposal
- Consortia discuss options for privacy friendly design
- Evaluators reject proposals which
  - do not discuss privacy impact sufficiently
  - cannot present tools mitigating severe privacy impact
- Mandatory Privacy Report for all accepted projects
- Privacy consulting in case of processing of special categories of data or critical privacy impact

Thank you for your attention!

Walter Peissl
wpeissl@oeaw.ac.at.ac.at
http://www.oeaw.ac.at/ita/
+43 1 51581 6584

Maren Raguse
ULD63@datenschutzzentrum.de
http://www.datenschutzzentrum.de/prise
+ 49 431 988 1284