

[Applying Privacy-by-Design to the Hotel Booking Use Case Using the ICO Handbook

Martin Kost, Johann-Christoph Freytag

[Context

- 2nd joint meeting (Dec 2nd, 2009) - Presentation of use case Hotel Booking
 - eSafety forum / eSecurity WG
 - CVIS - PRECIOSA partnership concerning privacy
 - European R&D Program
 - Use case inspired by existing and future ITS
- Apply Privacy-by-Design to the Use Case
 - Presentation made by telephone by Judith Jones, ICO on privacy by design.
 - Document prepared by Antonio (eSecurity_2010-05-12_Privacy By Design ICO.ppt)

[Project Outline

■ *Hotel Booking on the Road*

- Specifics: use of backend services for customer specific needs

■ Scenarios include the **two phases**

- n **Calculating and updating** a Route plus schedule from the Current Position to Home
- n **Booking** a Hotel on the Road

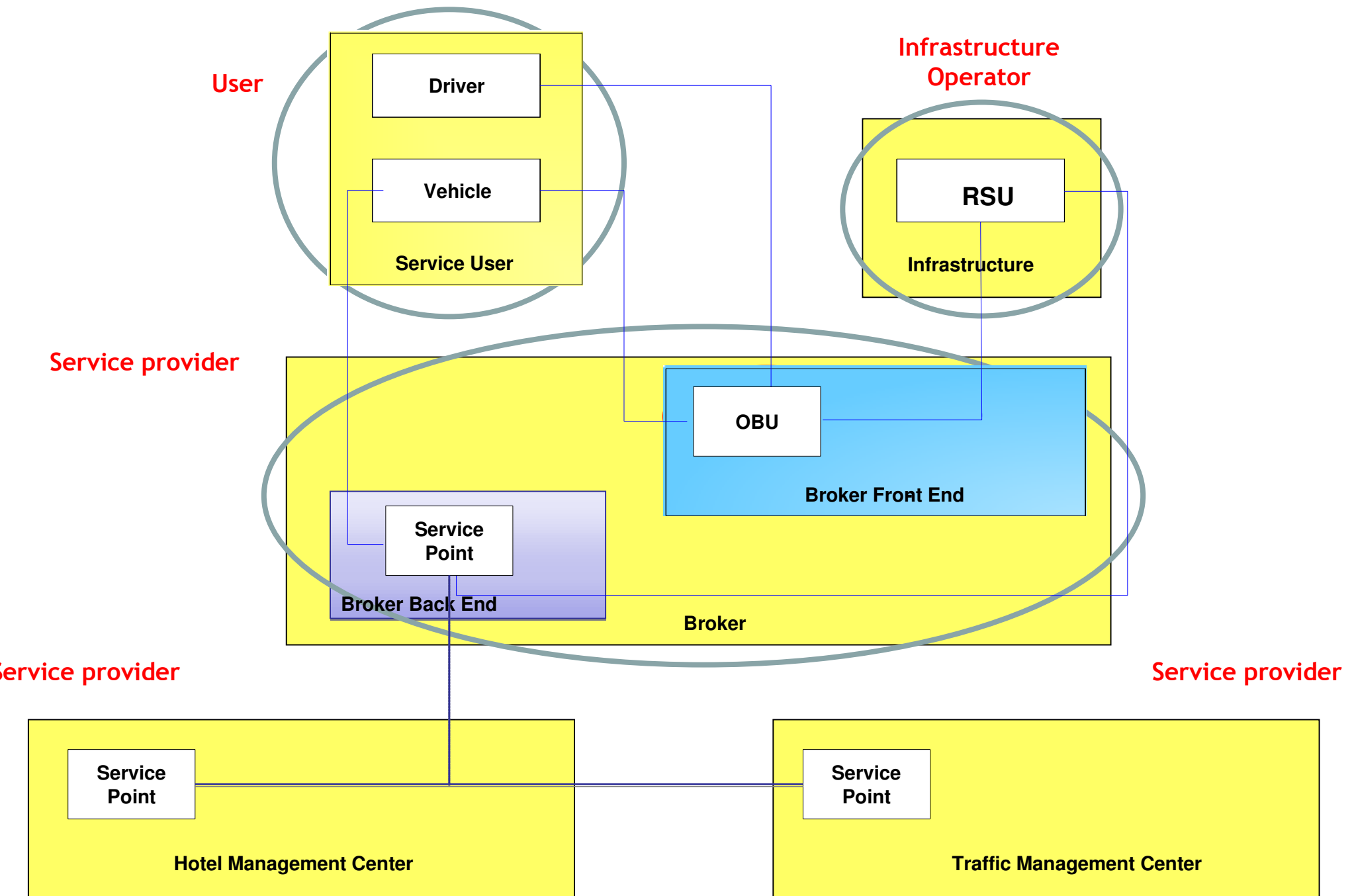
■ Motivation

- **Accessible Backend-Services** out of the car using one point of access
- Hotel booking & navigation info (road conditions) is “**up-to-date**”

■ Concepts

- **User/Driver** has one unique contract with **Broker** to access different backend services (**identity management**)
- **Easy access** to backend services (for example hotel booking) while driving (from the car) on long drives (vacation, business trips)
- Hotel booking when needed (**book-as-you-drive**)
- Using choices (personal ones) for booking (how far, which category, specific needs/desires)

Stakeholder Analysis



[Stakeholder Analysis

- **Stakeholders** and **Data Processing Units**
 - **Driver** has a contract with **Broker**
 - Infrastructure (provided by **infrastructure operator**) involves **Vehicle device**, **Road Side Unit (RSU)** and three Backend units (**Broker IS**, **TMC IS**, **HMC IS**)
 - **Vehicle device** acts as interface (preparation) and relay (communication)
 - **RSU** collects and forwards information about traffic status to the **TMC IS**
 - **Broker IS** manages customer data
 - **TMC IS** manages traffic status data
 - **HMC IS** manages hotel booking data
 - **Broker** interacts with **TMC** and **HMC** using their specific services

[What Else

- ITS Directive
- EDPS Opinion on BAT
- eSecurity - Article 29WG joint meetings

PIA Screening

1 Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?

- *Yes, identity management, centralized access to backend services, cooperative systems, location based services*

2 Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?

- *Yes, name of the user, credit card number, email address, home address, user id, vehicle id*

3 Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?

- *Yes, to judge the correctness of credit card payments by (legally) authorized parties*

4 Does the project involve multiple organisations, whether they are government agencies (eg in 'joined-up government' initiatives) or private sector organisations (eg as outsourced service providers or as 'business partners')?

- *Yes, public authorities, service providers, equipment manufacturers, infrastructure operator*

5 Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals?

- *Yes, personal information as about preferences, services, and contracts is stored and processed by the identity manager (broker)*

PIA Screening

- 6 Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?
 - *Yes, personal information as about preferences, services, and contracts.*
- 7 Does the project involve new or significantly changed handling of personal data about a large number of individuals?
 - *Yes, personal information as about preferences, services, and contracts.*
- 8 Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?
 - *Yes, identity manager provides necessary personal information as about preferences, services, and contracts. All other processing/communicating of personal information is prohibited.*
- 9 Does the project relate to data processing which is in anyway exempt from legislative privacy protections?
 - *No*
- 10 Does the project's justification include significant contributions to public security measures?
 - *No?*
- 11 Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?
 - *Maybe, the broker is responsible to sign contracts with service providers to guarantee applying privacy regulations*

[Full PIA is needed!

[*Next Screening Steps*

- *Privacy law compliance check*
- *Data protection compliance check*
 - *Template is based on the UK law*
 - *More appropriate for the data controller*
 - *Not for the supplier (he can second guess)*

[PIA

- Preliminary Phase
- *Preparation Phase*
- Consultation and analysis Phase
- *Documentation Phase*
- *Review and Audit Phase*

[Preliminary Phase

- *Review preliminary phase*
- *Update project outline*
- *Resource planning*
- *Preliminary discussion*
- Preliminary analysis of privacy issues
 - Confidentiality of communicated application messages and user information
 - Access to personal information (in memory and from data stores)
 - *Encryption*
 - *Anonymization (using Pseudonyms)*
 - *Access control*
 - *Limited Retention*

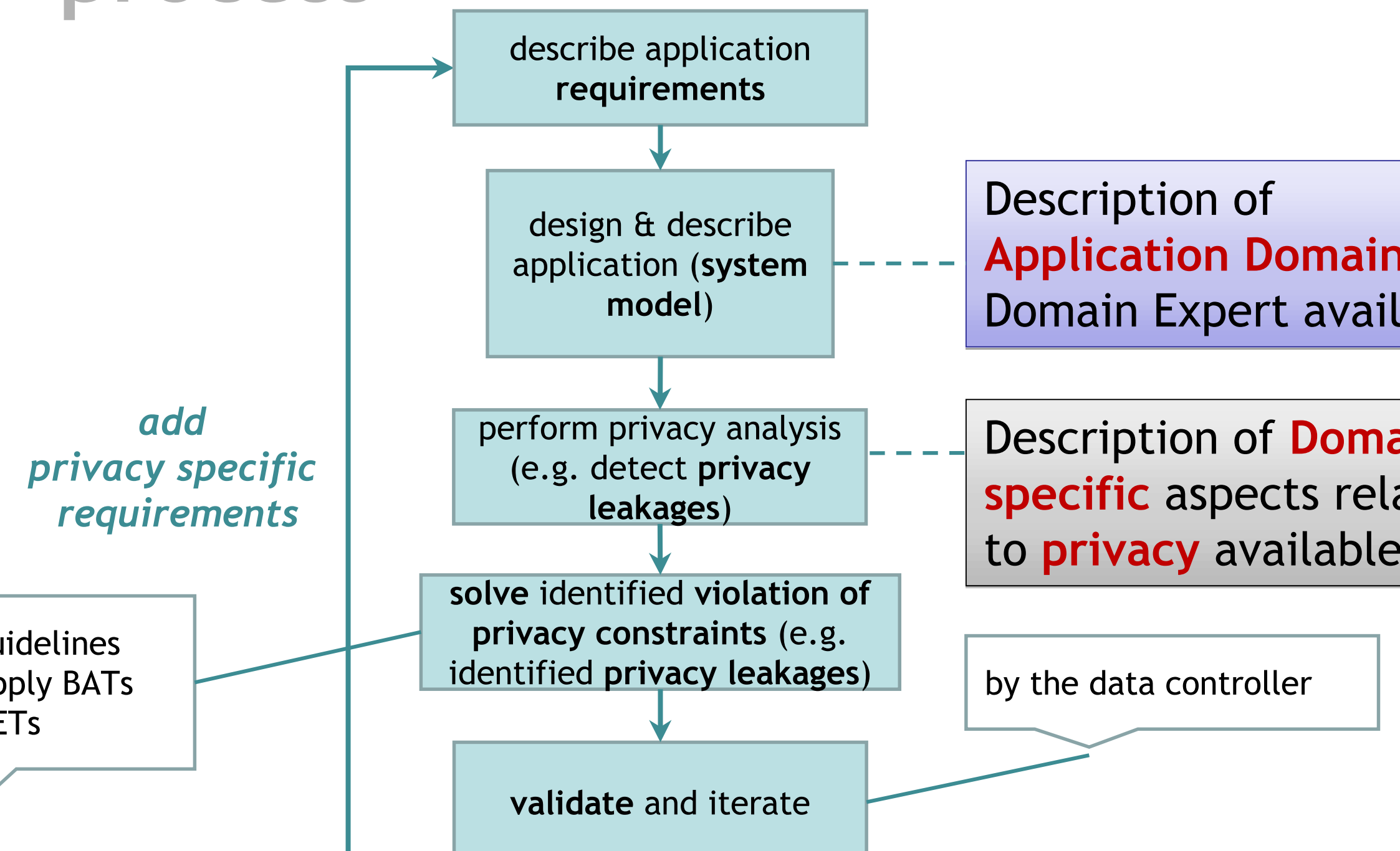
[Preparation Phase

- Consultation plan
 - *Manufactures, Service Providers*

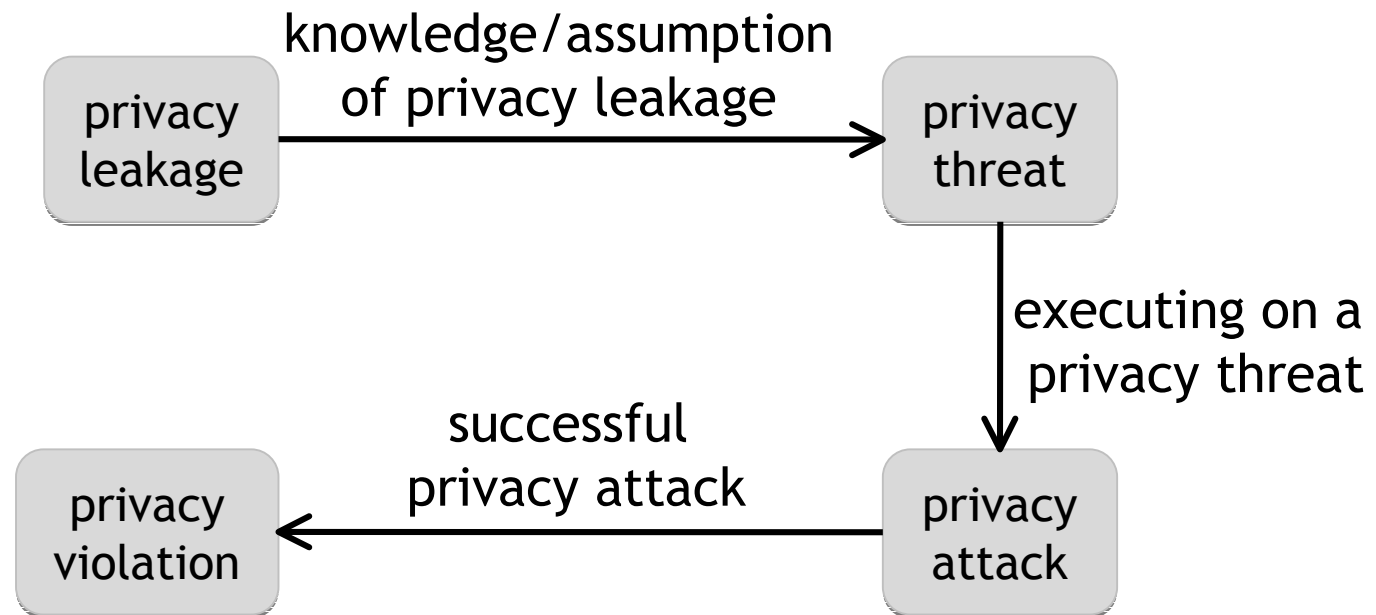
[Consultation and analysis Phase

- *Re-consider the design options*
- *Select a design*
 - *Privacy aware system design/development (technical approach)*
 - » *Privacy analysis (detect privacy issues and points of control and observation)*
 - » *Specification of privacy criteria of stakeholders (as requirements) and apply BATs or/and integrate PETs*
 - *translate privacy criteria into technical policies*
 - *redesign system (deployment)*
 - *...*
 - *Privacy aware architecture*
 - » *Confidential communication*
 - » *Enforcement of privacy policies*
 - » *...*
- *Provide the design features to the*
 - *PCG (PIA Consulting Group)*
 - *Project team*

Privacy aware system design - process



[Identify privacy leakages

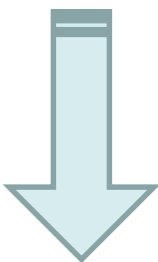


System model;
e.g. UML



transform model for
privacy analysis

part of system model;
e.g. information flow



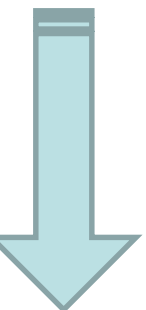
performing privacy
analysis; e.g. detect
privacy leakages

result of privacy
analysis



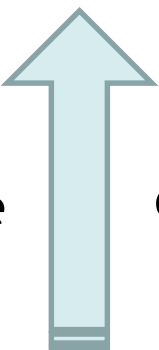
give information back
to app. designer

Privacy specific
properties and
requirements



Use guidelines and
apply BATs and PETs
to solve identified
privacy leakages

performing privacy
analysis; e.g. evaluate
privacy properties;



e.g. evaluation of
successful application
of appropriate measures
for solving identified
leakages

System model +
privacy measures



transform model for

part of system model;
with privacy
extensions

[Documentation Phase

- *Final document*
- *PIA report*
- *Make PIA available to PCG*
- *Publish PIA report*
 - *Could add the privacy law compliance study*
 - *Could add the data protection act compliance study*

[Review and Audit Phase

- *Undertake review*
- *Prepare review report*
- *Present report to PCG*
- *Make report public*

[Thanks