



PRIPARE: Preparing Industry to Privacy-by-design by supporting its Application in REsearch

PRIPARE: un projet Européen visant à définir une pratique intégrée de protection de la vie privée par construction

PRIPARE: towards an integrated privacy-by-design practice

27 Mai 2015

Antonio Kung. Trialog. www.trialog.com





PRIPARE (pripareproject.eu)

PReparing **I**ndustry to **P**rivacy-by-design by supporting its **A**pplication in **RE**search

Support Action Mission:

- Define and Support practice of privacy-by-design
- Provide educational material to foster risk management culture





Integrates disconnected practices

PIA

Ontario IPC PbD principles



Privacy Impact Assessments

Privacy Management Reference Model (PMRM)



Microsoft Security Development Lifecycle

Risk management



PEARs

Privacy Enhancing Architectures

ISO Standards (29100, 29101, 24760, 29134, 29151)





Outline

- Privacy-by-design?
 - An example of what can be achieved
 - One important phase: Risk analysis
 - One important phase: Design
 - Integrating Risk analysis and Design?
- Privacy-by-design in Practice
- On-going standardisation



 **PRIPARE**

PReparing Industry to Privacy-by-design by
supporting its Application in REsearch

Privacy-by-design?





Privacy-by-Design (PbD)?

- A possible definition
 - Institutionalisation of the concepts of privacy and security in organisations and integration of these concepts in the design of systems
 - See blog (<http://www.securityengineeringforum.org/blog/show/id/27>)



PRIPARE

PReparing Industry to Privacy-by-design by
supporting its Application in REsearch

Example

Electronic Tolling Systems (ETS)

PrETP: Privacy-Preserving Electronic Toll Pricing J.Balasch. et al. 19th USENIX Security
Symposium 2010





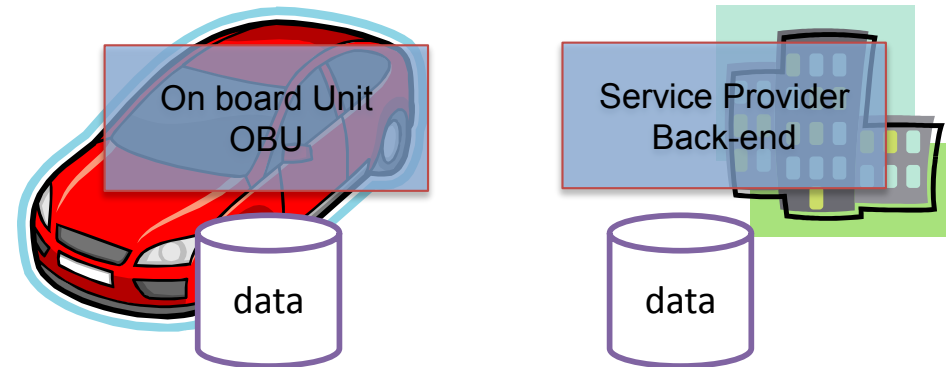
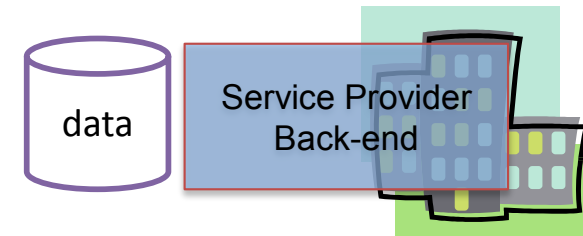
Description

- User pays for using roads, depending on context
 - Type of road
 - Time/date
 - Traffic
 - Type of vehicle, ...
- Public authority manages infrastructure using policies
 - Congestion
 - Energy
 - Big event (sports game...)



Approaches

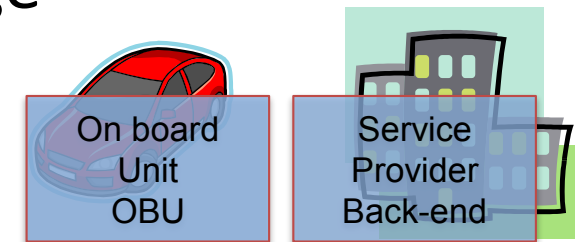
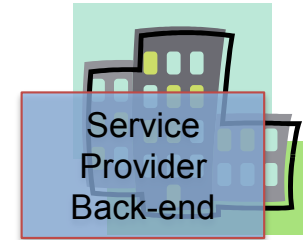
- **Model A:** personal data and fees handled by SP backend
- **Model B:** fees handled by SP backend, personal data handled by OBU





Comparison

- **Model A:** Data kept at SP level (millions of users)
- **Model B:** Data kept in vehicles (one user). Proofs sent to SP (zero-knowledge technology)
- Model B preserves privacy
- But different architectures...,
- But different interoperability requirements...





 **PRIPARE**

PRPreparing Industry to Privacy-by-design by
supporting its Application in REsearch

One Important PbD Phase

Risk Management





Risk management

- Identification, assessment, and prioritization of risks
- A generic process
 - identify, characterize **threats**
 - assess the **vulnerability** of critical **assets** to specific threats
 - determine the risk (i.e. the expected **likelihood** and **consequences** of specific types of **attacks** on specific assets)
 - identify ways to reduce those risks
 - prioritize risk reduction measures based on a strategy



Security Risks: STRIDE cheat sheet

| Property | Description | Threat |
|---|---|---|
| Authentication (<i>authentification</i>) | The identity of users is established (or you're willing to accept anonymous users). | S poofing (<i>usurpation</i>) |
| Integrity (<i>intégrité</i>) | Data and system resources are only changed in appropriate ways by appropriate people. | T ampering (<i>altération</i>) |
| Nonrepudiation (<i>non répudiation</i>) | Users can't perform an action and later deny performing it. | R epudiation (<i>répudiation</i>) |
| Confidentiality (<i>confidentialité</i>) | Data is only available to the people intended to access it. | I nformation disclosure (<i>divulgation de l'information</i>) |
| Availability (<i>disponibilité</i>) | Systems are ready when needed and perform acceptably. | D enial Of Service (<i>déni de service</i>) |
| Authorization (<i>autorisation</i>) | Users are explicitly allowed or denied access to resources. | E levation of privilege (<i>élévation de privilège</i>) |



Privacy Risks: LINDDUN cheat sheet

| Type | Property | Description | Threat |
|--------------|-------------------------------------|--|--|
| Hard privacy | Unlinkability | Hiding the link between two or more actions, identities, and pieces of information. | L inkability (possibilité de créer un lien) |
| | Anonymity | Hiding the link between an identity and an action or a piece of information | I dentifiability (possibilité d'identifier) |
| | Plausible deniability | Ability to deny having performed an action that other parties can neither confirm nor contradict | N on-repudiation (non répudiation) |
| | Undetectability and unobservability | Hiding the user's activities | D etectability (possibilité de détecter) |
| Security | Confidentiality | Hiding the data content or controlled release of data content | D isclosure of information (divulcation d'information) |
| Soft Privacy | Content awareness | User's consciousness regarding his own data | U nawareness (méconnaissance) |
| | Policy and consent compliance | Data controller to inform the data subject about the system's privacy policy, or allow the data subject to specify consents in compliance with legislation | N on compliance (non conformité) |



CNIL Privacy Risk Analysis

- French DPA
- Feared Events
- Threats



From CNIL methodology document



Risk = f(Severity, Likelihood)

| | | | | |
|----------------------|-----------------------------------|--------------------------------------|------------------------|--------------------|
| Maximum Severity | Must be avoided or reduced | Absolutely avoided or reduced | | |
| Significant Severity | | | | |
| Limited Severity | These risks may be taken | Must be reduced | | |
| Negligible Severity | | | | |
| | Negligible Likelihood | Limited Likelihood | Significant Likelihood | Maximum Likelihood |



 **PRIPARE**

PRPreparing Industry to Privacy-by-design by
supporting its Application in REsearch

One Important PbD Phase

Design





OASIS PMRM (Privacy Management Reference Model): Services

| | Service | Purpose |
|-----------------|----------------|--|
| From OASIS PMRM | Agreement | Management of permissions and rules |
| | Usage | Controlling personal data usage |
| | Validation | Checking personal data |
| | Certification | Checking stakeholders credentials |
| | Enforcement | Monitor operations and react to exceptions |
| | Security | Safeguard privacy information and operations |
| | Interaction | Information presentation and communication |
| From PRIPARE | Access | Data subject access to their personal data |
| | Accountability | Log and audit management |



Kung: PEARs

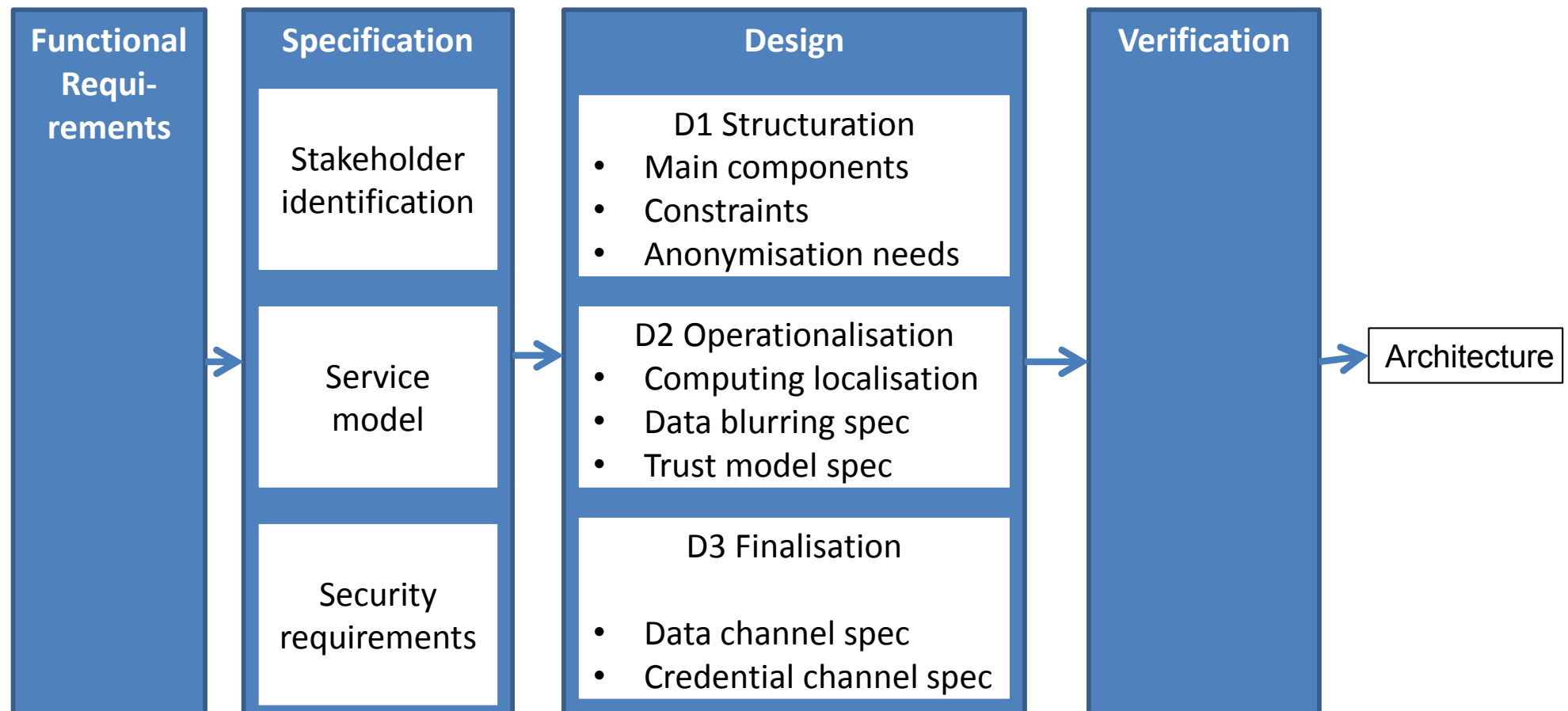
Antonio Kung. PEARs: Privacy Enhancing ARchitectures. Annual Privacy Forum. Lecture Notes in Computer Science Volume 8450, 2014

| Strategy | | Tactics Examples |
|--|--|---|
| 1 Minimization | Collection of personal information should be kept to a strict minimum | <ul style="list-style-type: none">• Anonymize credentials (e.g. Direct anonymous attestation)• Limit processing perimeter (e.g. client processing, P2P processing) |
| 2 Enforcement (application) | Provide maximum protection of personal data during operation | <ul style="list-style-type: none">• Enforce data protection policies (collection, access and usage, collection, retention)• Protect processing (e.g. storage, communication, execution, resources) |
| 3 Transparency and accountability (redevisibilité) | Maximum transparency provided to stakeholders on the way privacy preservation is ensured | <ul style="list-style-type: none">• Log data transaction• Log modifications (policies, crypto, protection)• Protect log data |
| 4 Modifiability | Cope with evolution needs | <ul style="list-style-type: none">• Change Policy• Change Crypto Strength and method• Change Protection Strength |



Thibaud Antignac PhD Thesis

- Formal methods for Privacy-by-design. February 25th, 2015
 - Include a process proposal focusing on minimisation
 - Includes a formal verification framework proposal





Hoepman: Design Strategies

Jaap-Henk Hoepman. Privacy design strategies . In ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco

| Strategy | | Patterns Examples |
|----------------|--|--|
| 1 Minimization | Amount of processed personal data restricted to the minimal amount possible | <ul style="list-style-type: none">• select before you collect• anonymisation / pseudonyms |
| 2 Hide | Personal data, and their interrelationships, hidden from plain view | <ul style="list-style-type: none">• Storage and transit encryption of data• mix networks• hide traffic patterns• attribute based credentials• anonymisation / pseudonyms |
| 3 Separate | Personal data processed in a distributed fashion, in separate compartments whenever possible | <ul style="list-style-type: none">• Not known |
| 4 Aggregate | Personal data processed at highest level of aggregation and with least possible detail in which it is (still) useful | <ul style="list-style-type: none">• aggregation over time (used in smart metering)• dynamic location granularity (used in location based services)• k-anonymity• differential privacy |
| 5 Inform | Transparency | <ul style="list-style-type: none">• platform for privacy preferences• Data breach notification |
| 6 Control | Data subjects provided agency over the processing of their personal data | <ul style="list-style-type: none">• User centric identity management• End-to-end encryption support control |
| 7 Enforce | Privacy policy compatible with legal requirements to be enforced | <ul style="list-style-type: none">• Access control• Sticky policies and privacy rights management |
| 8 Demonstrate | Demonstrate compliance with privacy policy and any applicable legal requirements | <ul style="list-style-type: none">• privacy management systems• use of logging and auditing |



 **PRIPARE**

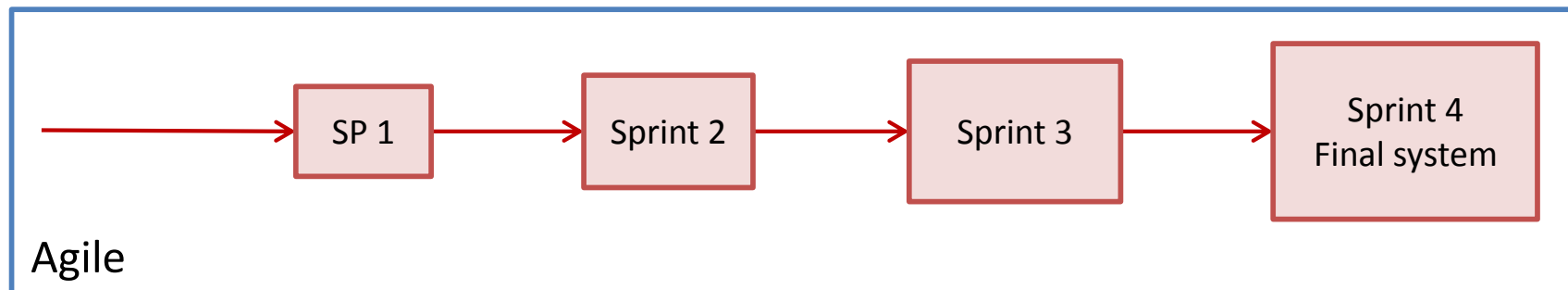
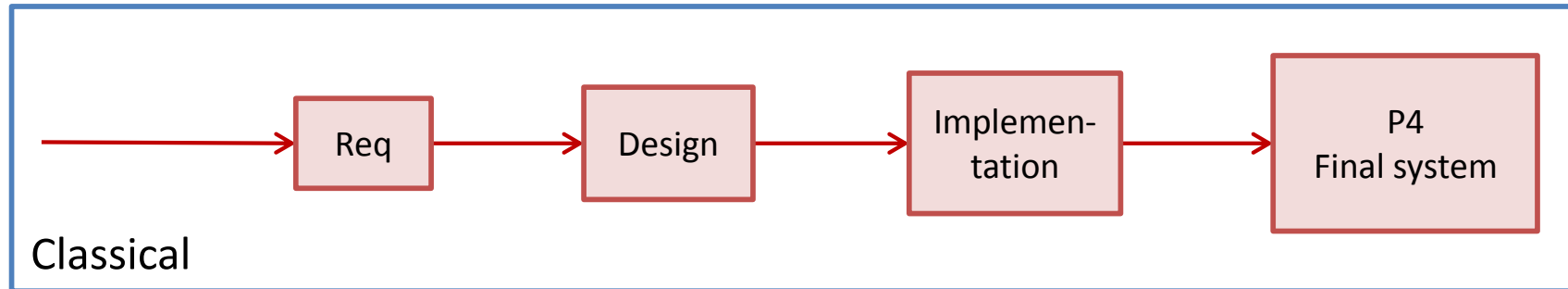
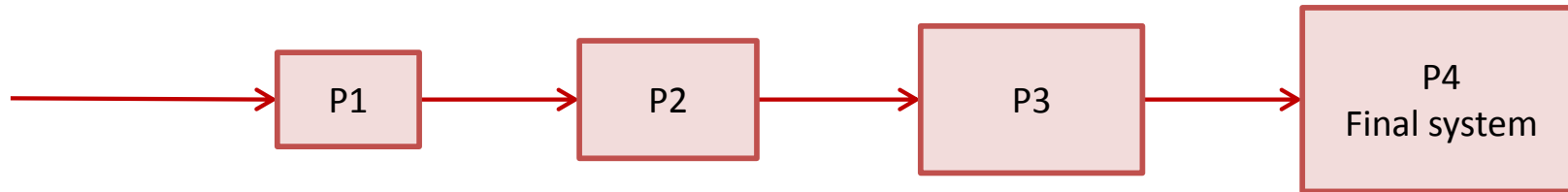
PReparing Industry to Privacy-by-design by
supporting its Application in REsearch

Integrating Risk analysis and Design?



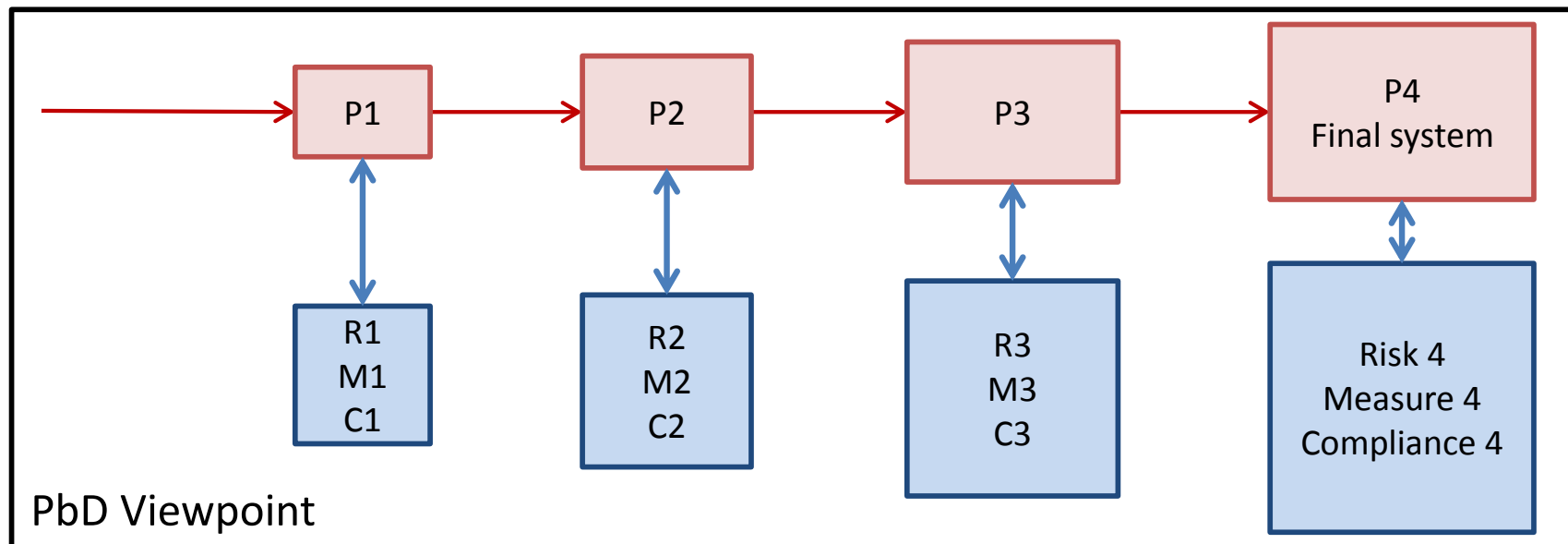
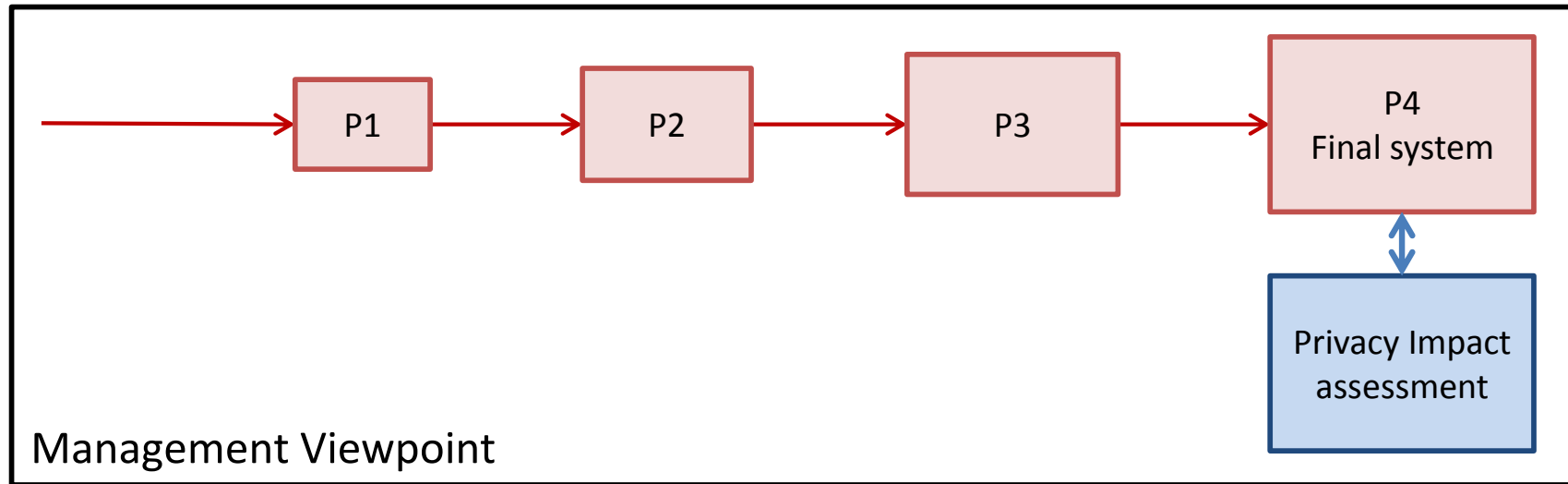


A Process Vision





Integration of Risk and Design in Process





 **PRIPARE**

PRPreparing Industry to Privacy-by-design by
supporting its Application in REsearch

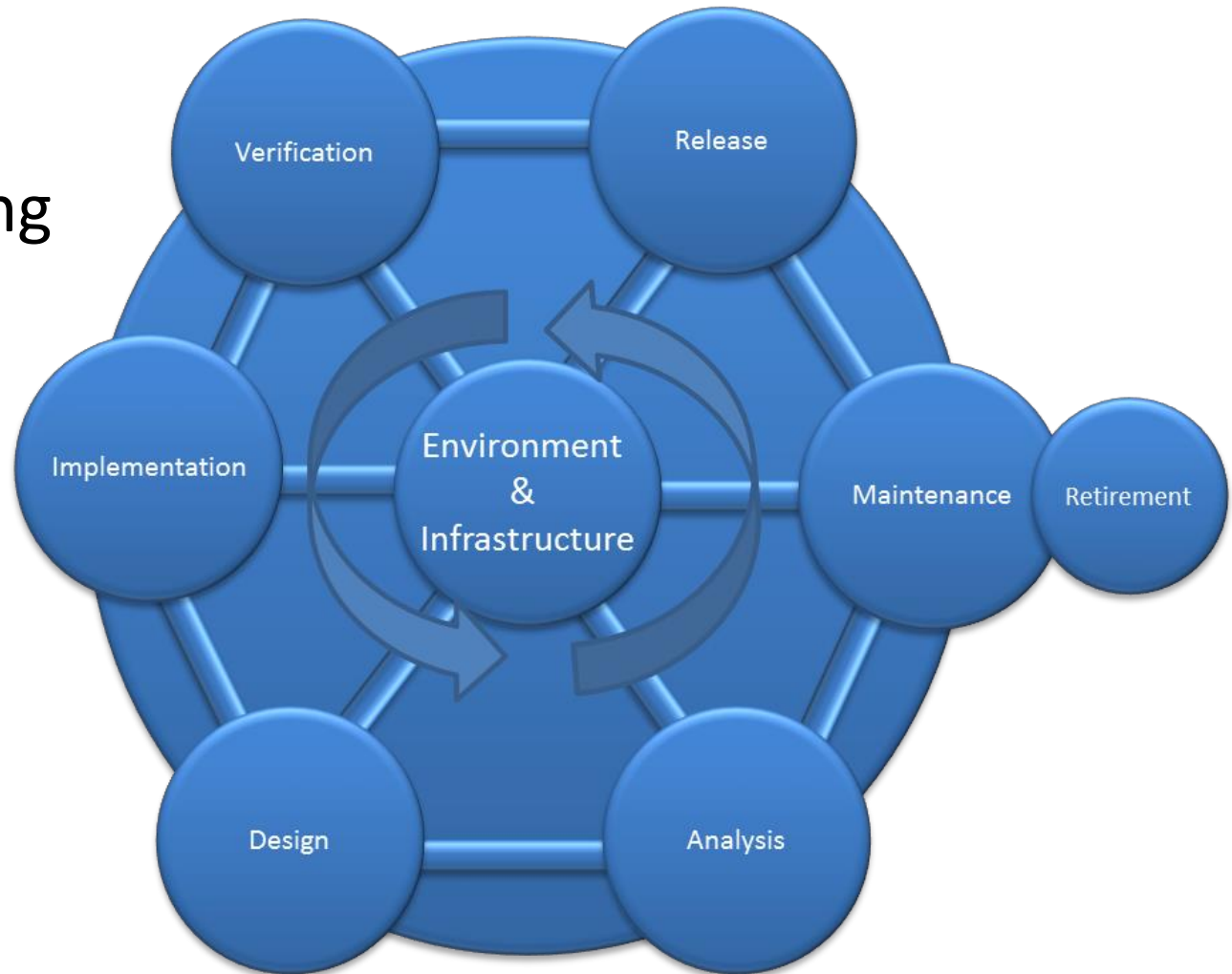
Privacy-by-design in Practice?





PRIPARE PbD Methodology

- Covers entire life cycle
- Focuses on two privacy engineering activities
 - Privacy risk analysis
 - Design for privacy preservation
- Focuses on one privacy management activity
 - Compliance management





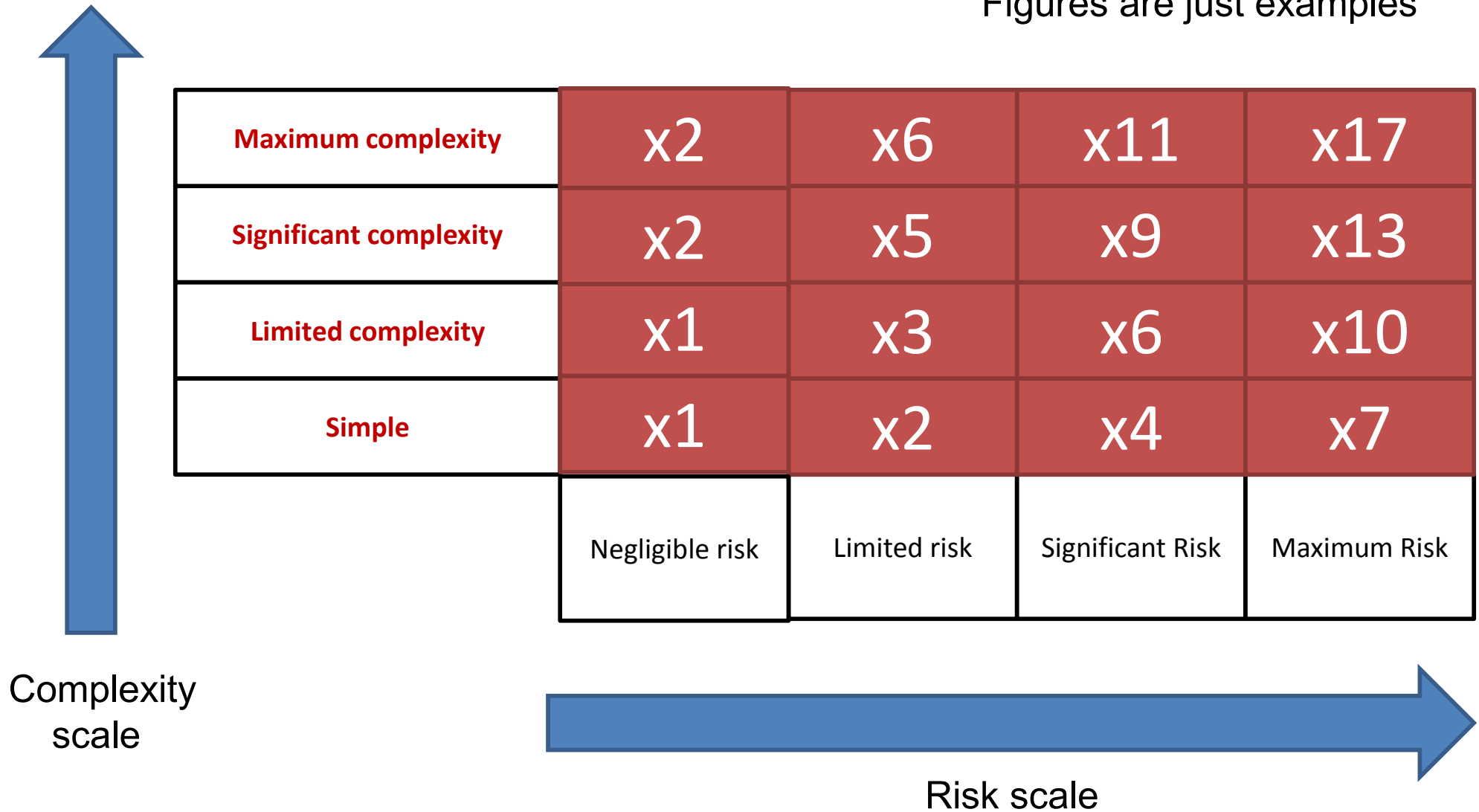
Practicing PbD

- Depends on type of system
 - Risk scale
 - Complexity scale
- Depends on type of development
 - Research (we must integrate PbD even at research level)
 - Innovation
 - Industry
- Depends on type of integration
- Depends on stakeholder viewpoint



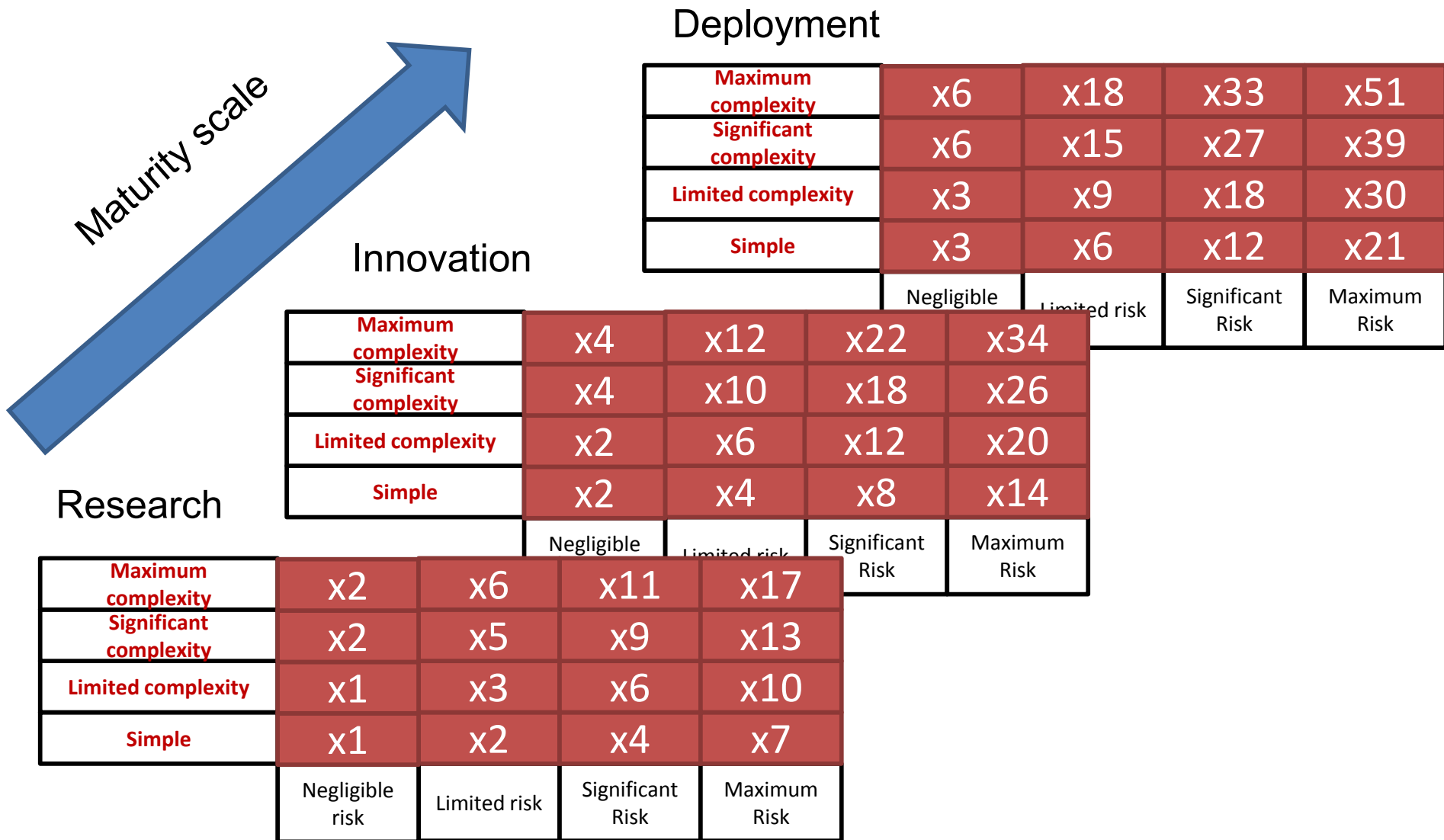
Type of System

Figures are just examples





Type of Development





Integration / Stakeholder Viewpoint

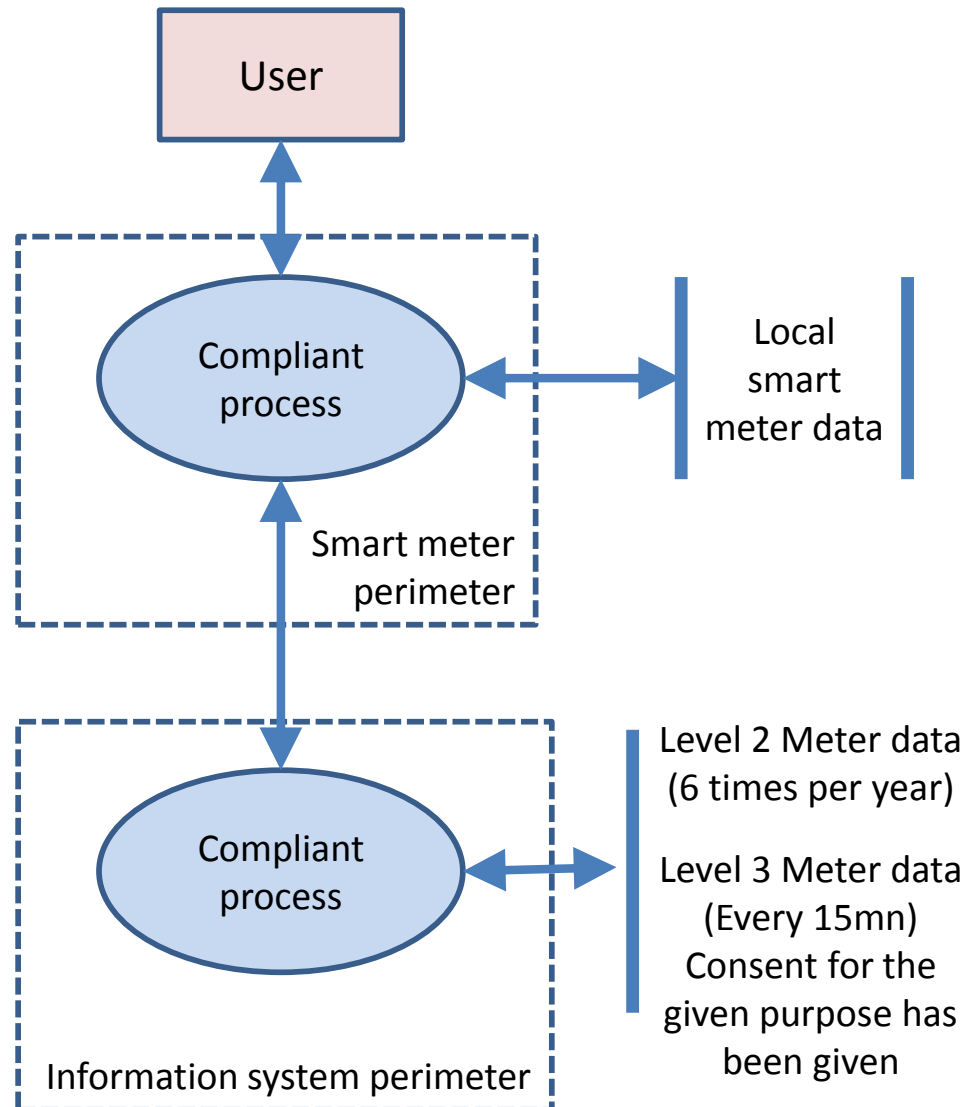
- Integration
 - Platform vs Application
 - System vs subsystem
- The stakeholder viewpoint
 - Citizen / Corporate
 - Manager / Designer / Lawyer / Ethicist



Smart Grid Example

Input from
CRISALIS
FP7 Project
training workshop

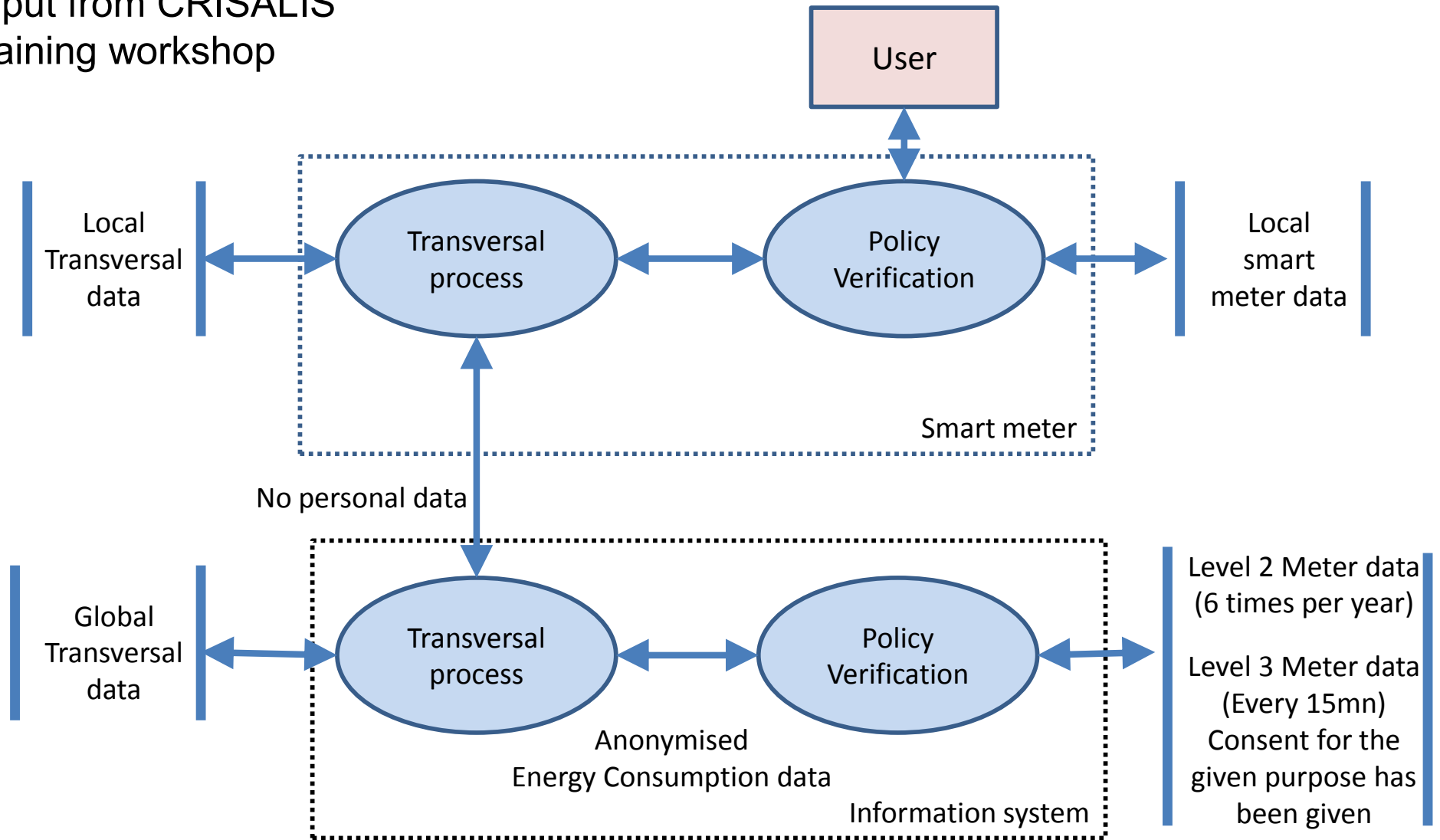
Based on
Netherlands
Regulation





Transversal System PbD in Smart Grid

Input from CRISALIS training workshop





Impact on PbD Practice

- In the case of a nominal case that is well understood (e.g. smart meter)
- PbD process for additional transversal features must follow an incremental PbD process where the **constraints and properties resulting from the nominal case must be preserved**



 **PRIPARE**

PRPreparing Industry to Privacy-by-design by
supporting its Application in REsearch

Existing initiatives/standards





Platforms and Standards

- Platforms
 - NIST Privacy engineering workshops
 - IPEN: Internet Privacy Engineering Network
 - Workshop Leuven. June 5th 2015.
- Standards
 - OASIS
 - PMRM Privacy Management Reference Model
 - PbD-SE Privacy-by-design for software engineers
 - ISO/IEC SC27/WG5
 - 29100 Privacy framework
 - 29134 Privacy impact assessment
 - 29151 Code of practice for personally identifiable information
 - ...
 - JWG8 CEN/CENELEC: PbD for security products



 **PRIPARE**

PReparing Industry to Privacy-by-design by
supporting its Application in REsearch

Thanks

Antonio Kung. Trialog. Antonio.kung@trialog.com
www.trialog.com

