Privacy Management in Smart Cities

Antonio Kung

Chris Cooper

Introduction Speaker

- Antonio Kung, Trialog (www.trialog.com,FR)
  - Engineering background - CTO
  - ISO activities on privacy engineering (SC27/WG5)
  - OASIS activities on privacy-by-design (PMRM, PbD-SE)
  - Member ipen

- PRIPARE support action (pripareproject.eu)
  - Handbook (March 7th 2016 Press release)
    - Methodological Tools to Implement Privacy and Foster Compliance with the GDPR

Introduction Speaker

- Chris Cooper, KnowNow (www.kn-i.com,UK)
  - Chartered Engineer - CTO for KnowNow
  - 20 years in IT - Enterprise Architect
  - Member City Standards Institute @CitiesStandards
  - Participant in Open Consent Group (openconsent.org)
  - Active in Privacy & Data Trust Network (pdtn.org)
  - Participated in EIP-SCC since 2014
  - Involved in Citizen Centric Data since 2015

Privacy Management from the demand-side to the supply-side

GDPR: General Data Protection Regulation

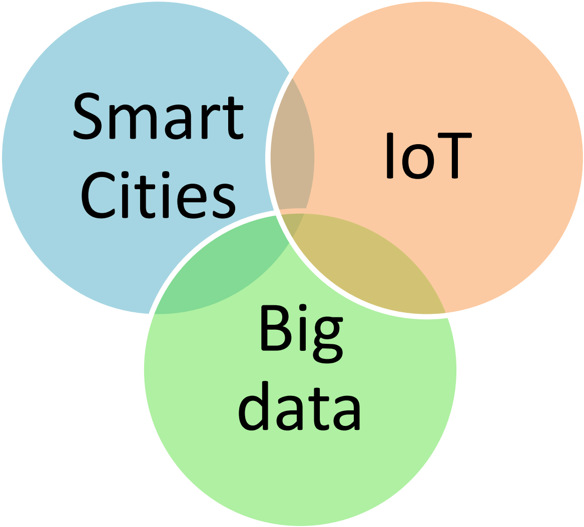
Published on May 4th 2016
Enter into force on May 24th 2016
Apply on May 25th 2018

- Privacy-by-design (PbD) and by-default
- Privacy Impact Assessment (PIA)
- Data Protection Officers
  - All public authorities
  - Companies processing more than 5000 data subjects
- Sanctions for breaches
  - up to 20,000,000 EUR
  - up to 4% of the annual worldwide turnover

Definitions

- Privacy-by-design: **PbD**
  - Institutionalisation of privacy management
  - Integration of privacy concern in the engineering of systems
- Privacy-by-default
  - Highest level of protection by default
- Privacy Impact assessment: **PIA**
  - Process that evaluates impact on privacy
- Note that the GDPR uses the term “data protection” instead of “privacy”

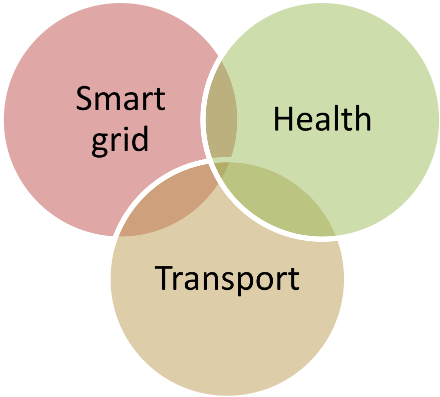
Privacy in Complex Ecosystems


Smart Cities

IoT

Big data

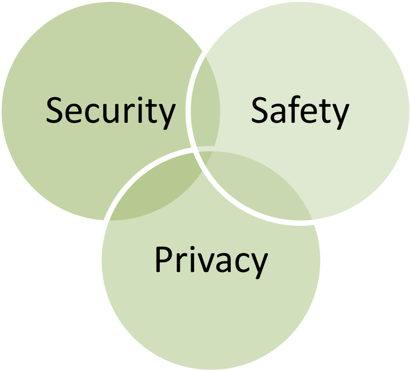
Ecosystems


Smart grid

Health

Transport

Domains

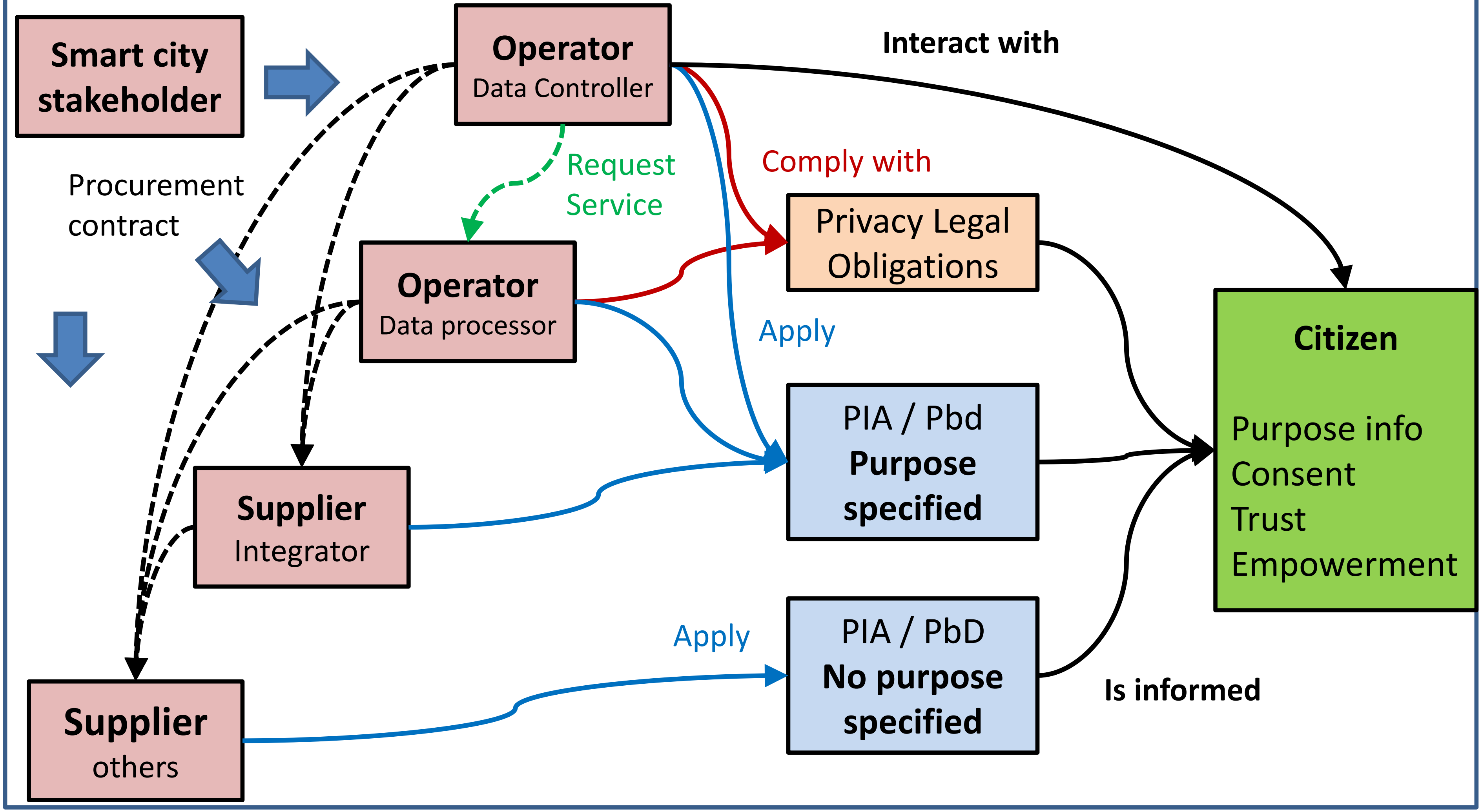

Security

Safety

Privacy

Concerns

Privacy Management in Ecosystem

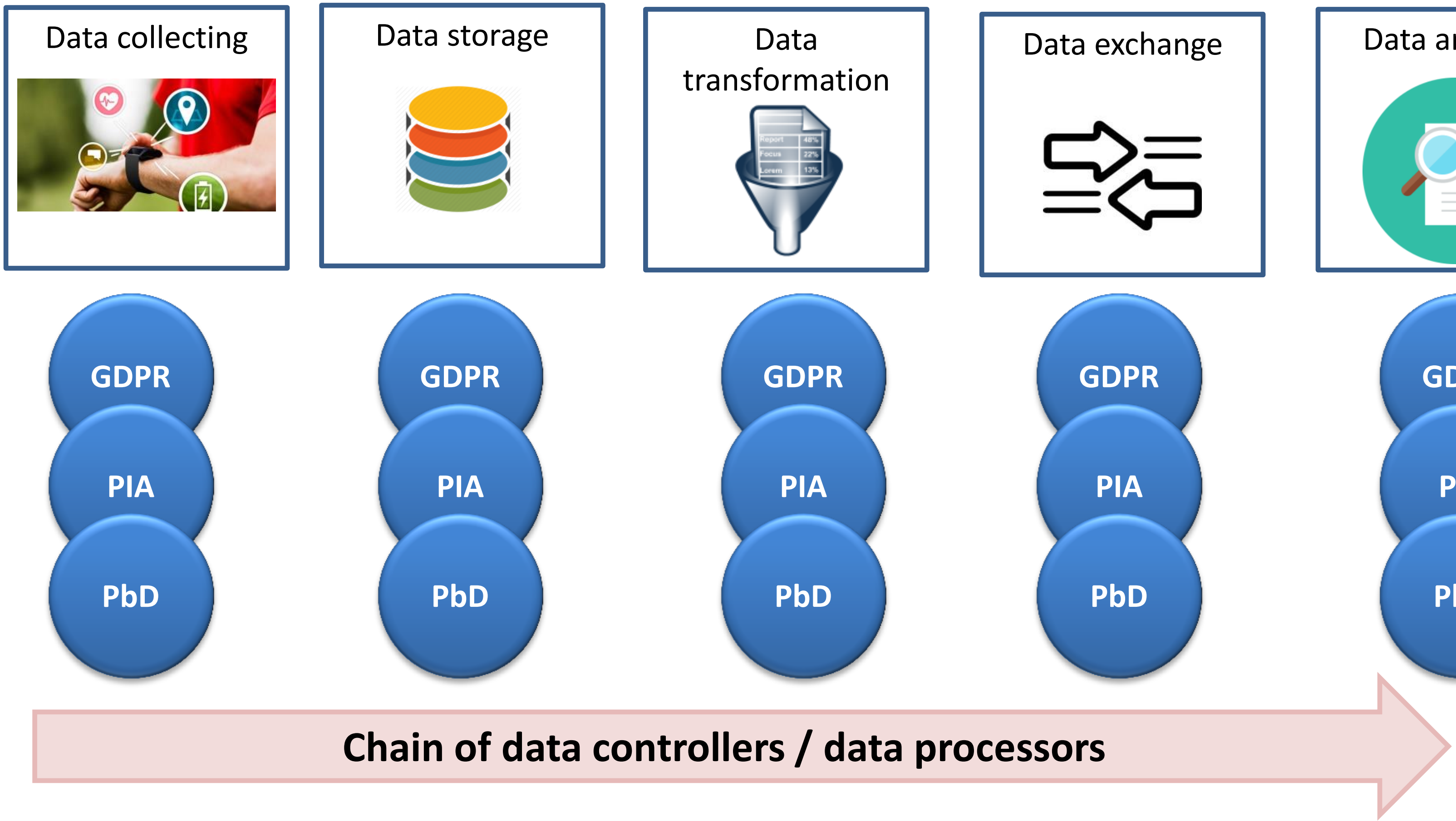


Several Types of Concerns

Stakeholder		Legal Compliance Level	Management Level	System Lifecycle Level
Demand side	Policy maker	**Compliance Check**		
↓	**Operator** Data Controller	Regulation **GPDR**	Privacy Impact Assessment **PIA**	Privacy-by-Design **PbD**
	Operator Data processor			
Supply side	**Supplier**	**Operators Requirements**		

Demand Side Concern

- Compliance Check for accountability



Data collecting

Data storage

Data transformation

Data exchange

Data analytics

GDPR

PIA

PbD

GDPR

PIA

PbD

GDPR

PIA

PbD

GDPR

PIA

PbD

GDPR

PIA

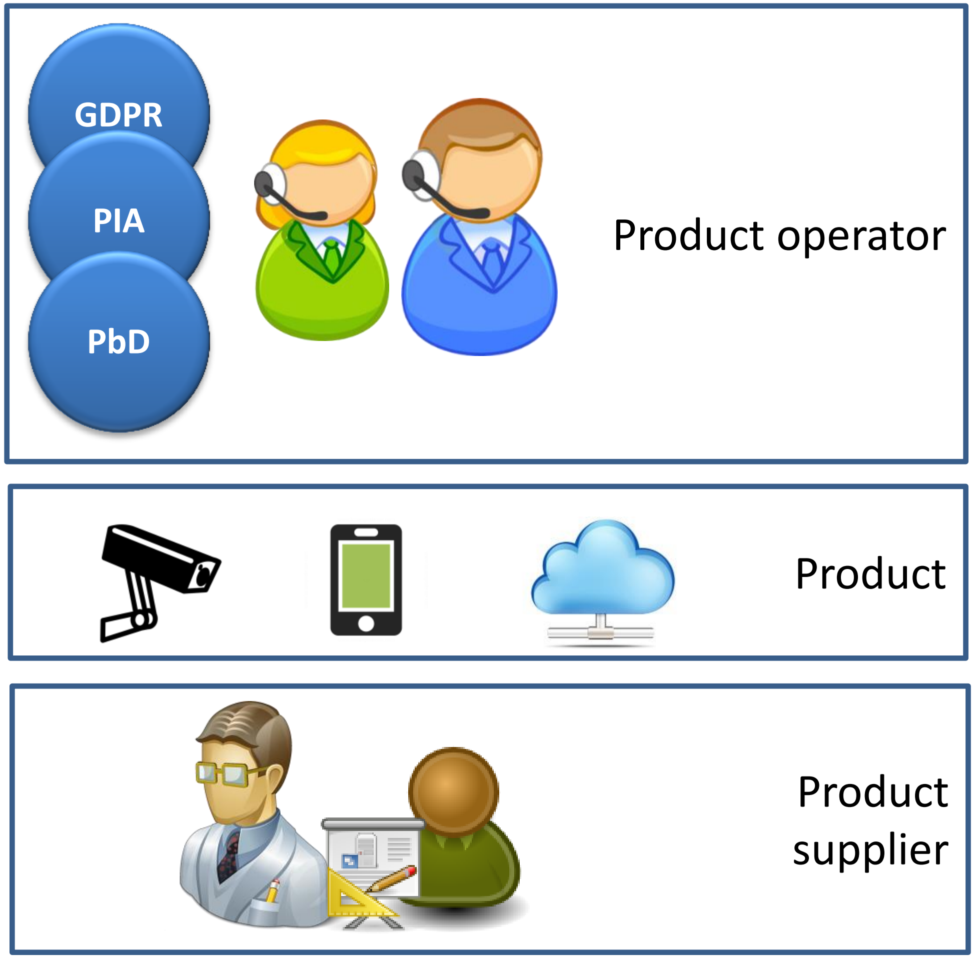
PbD

Chain of data controllers / data processors

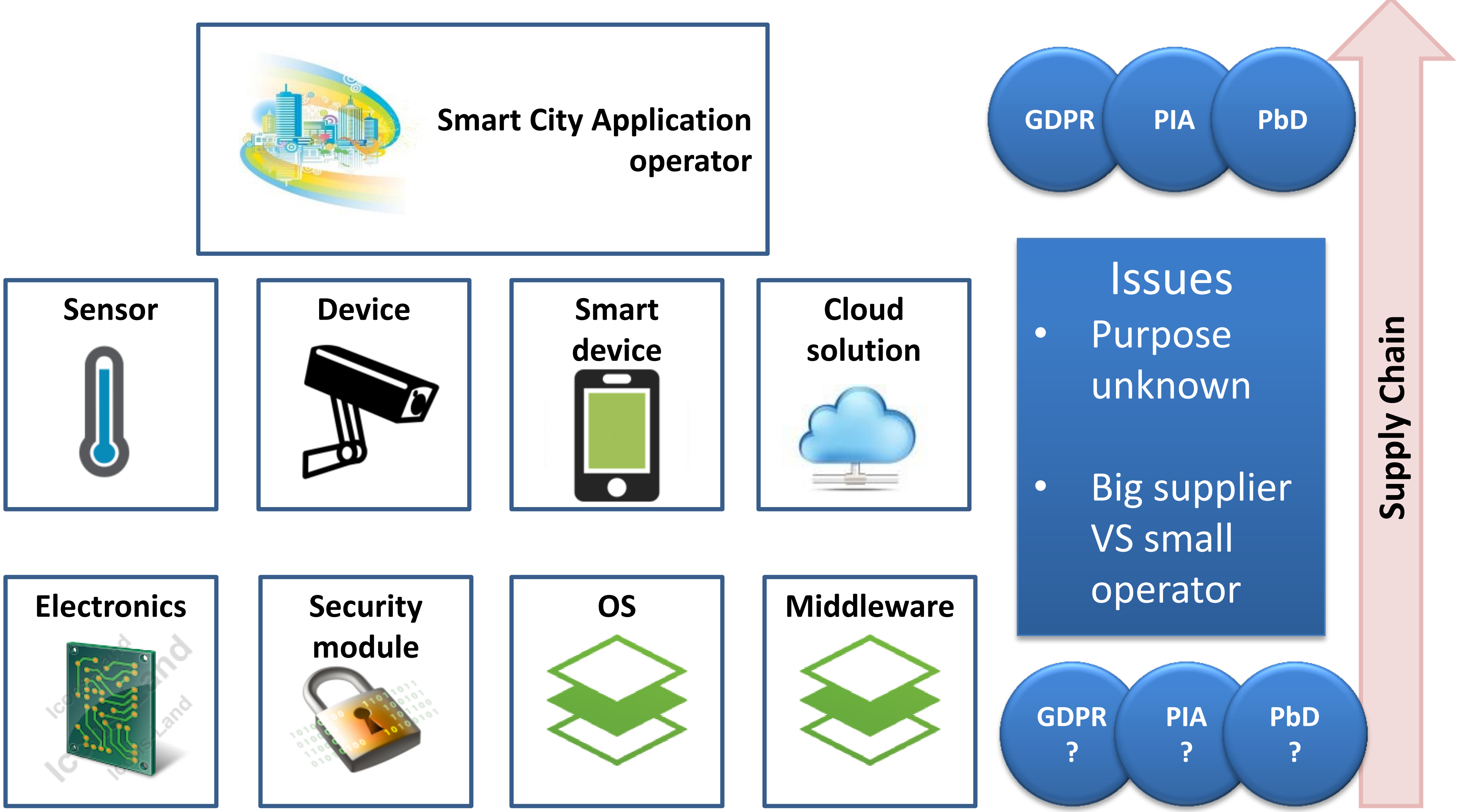
Operator vs Supplier Concerns

- Operator concerns
  - Data controller and data processor obligations in the data chain

- Supplier concerns?
  - Meet market demand



Supplier Concerns?



Smart City Application operator

Sensor

Device

Smart device

Cloud solution

Electronics

Security module

OS

Middleware

GDPR

PIA

PbD

Issues

- Purpose unknown
- Big supplier VS small operator

GDPR ?

PIA ?

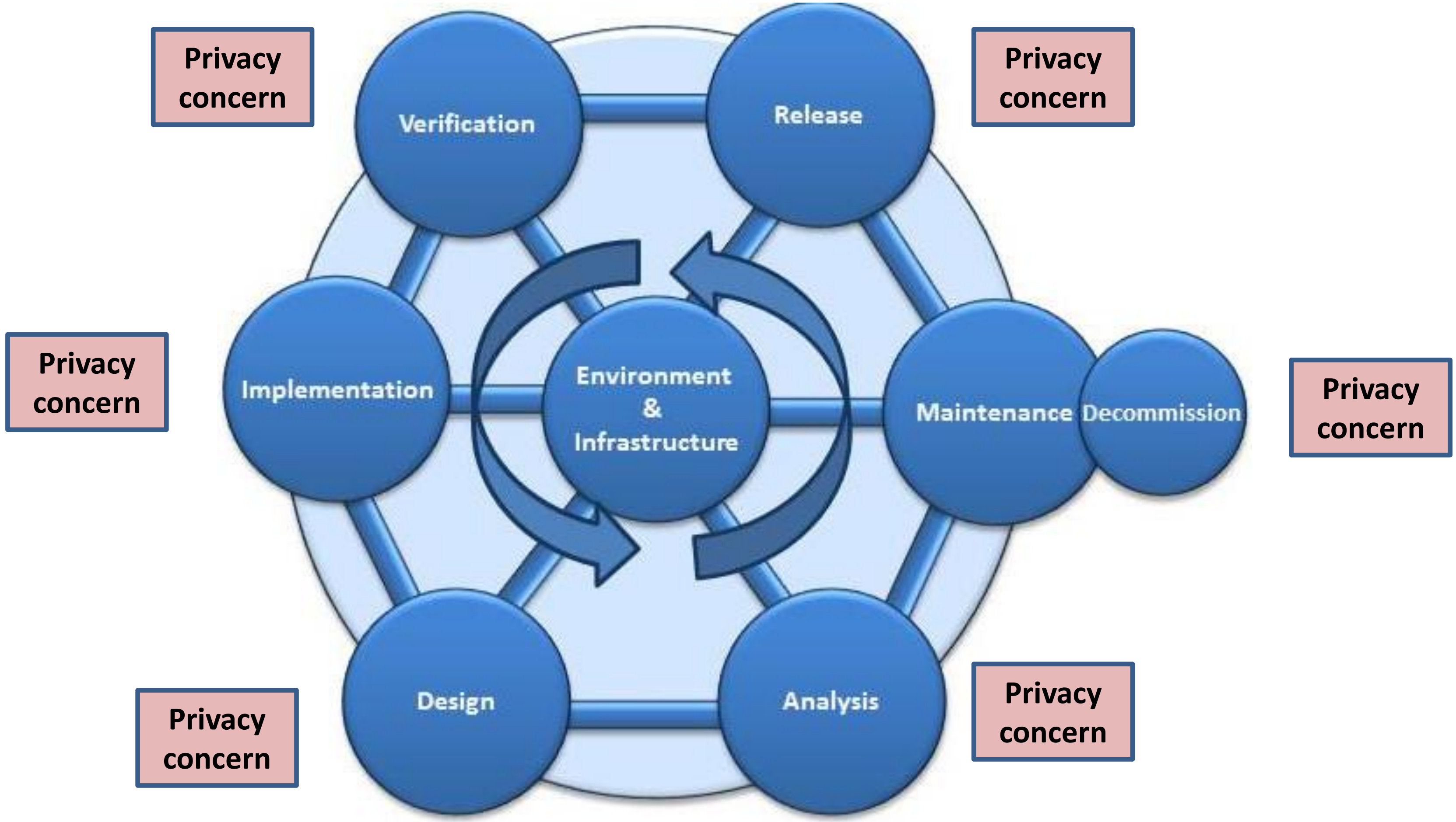
PbD ?

Supply Chain

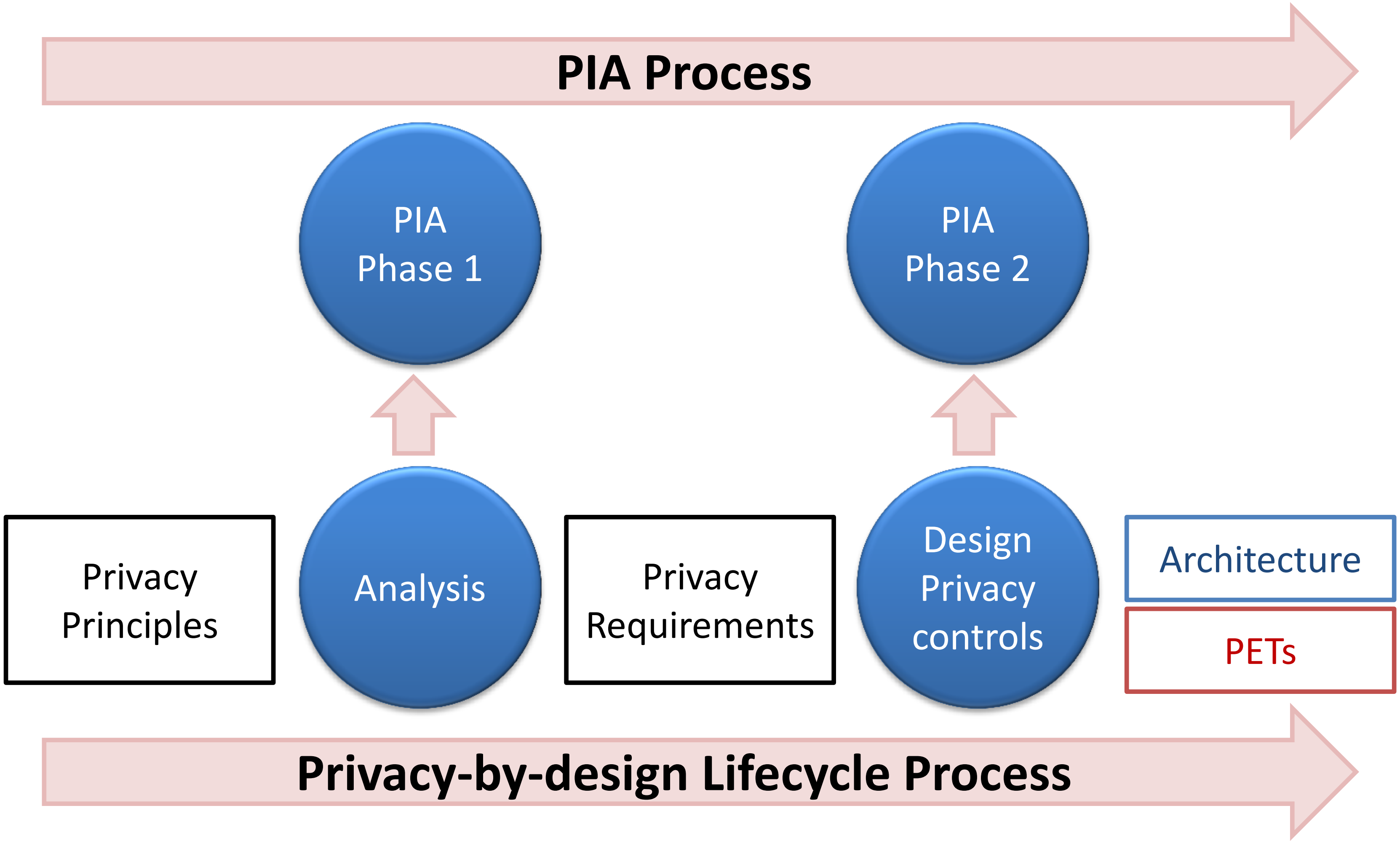
Privacy-by-design and Privacy Impact Assessment Engineering viewpoint

It’s all about integration

Integrating Privacy Concerns in the Lifecycle

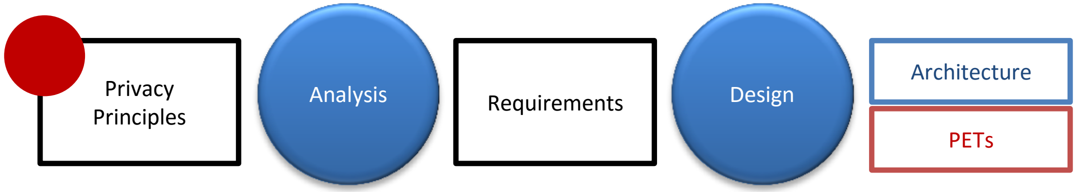


A Glimpse on the Process



Privacy Principles

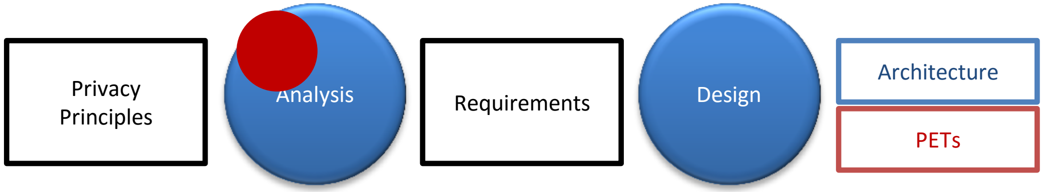
- Seven principles from Ann Cavoukian
  - Proactive not reactive, privacy as default setting, privacy-by-design, positive sum, security, transparency, user-centric
- ISO 29100 – privacy framework
  - Consent and choice, purpose, collection limitation, data minimization, use limitation, accuracy and quality, openness/transparency/notice, individual participation and access, accountability, security,



Analysis

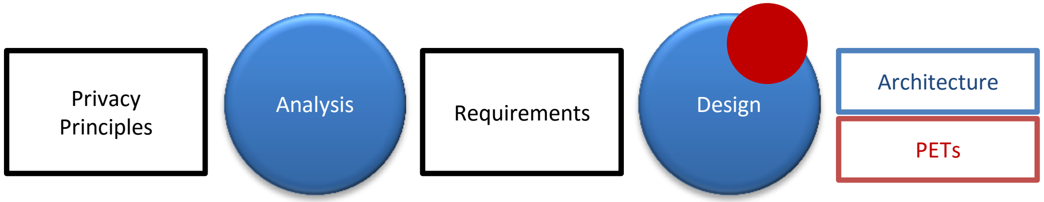
- Identify privacy policies and privacy management requirements

	Service	Purpose
OASIS PMRM Privacy Management Reference Model and Methodology	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 / Accountability
	Security	Safeguard privacy information and operations
	Interaction	Information presentation and communication
	Access	Data subject access to their personal data

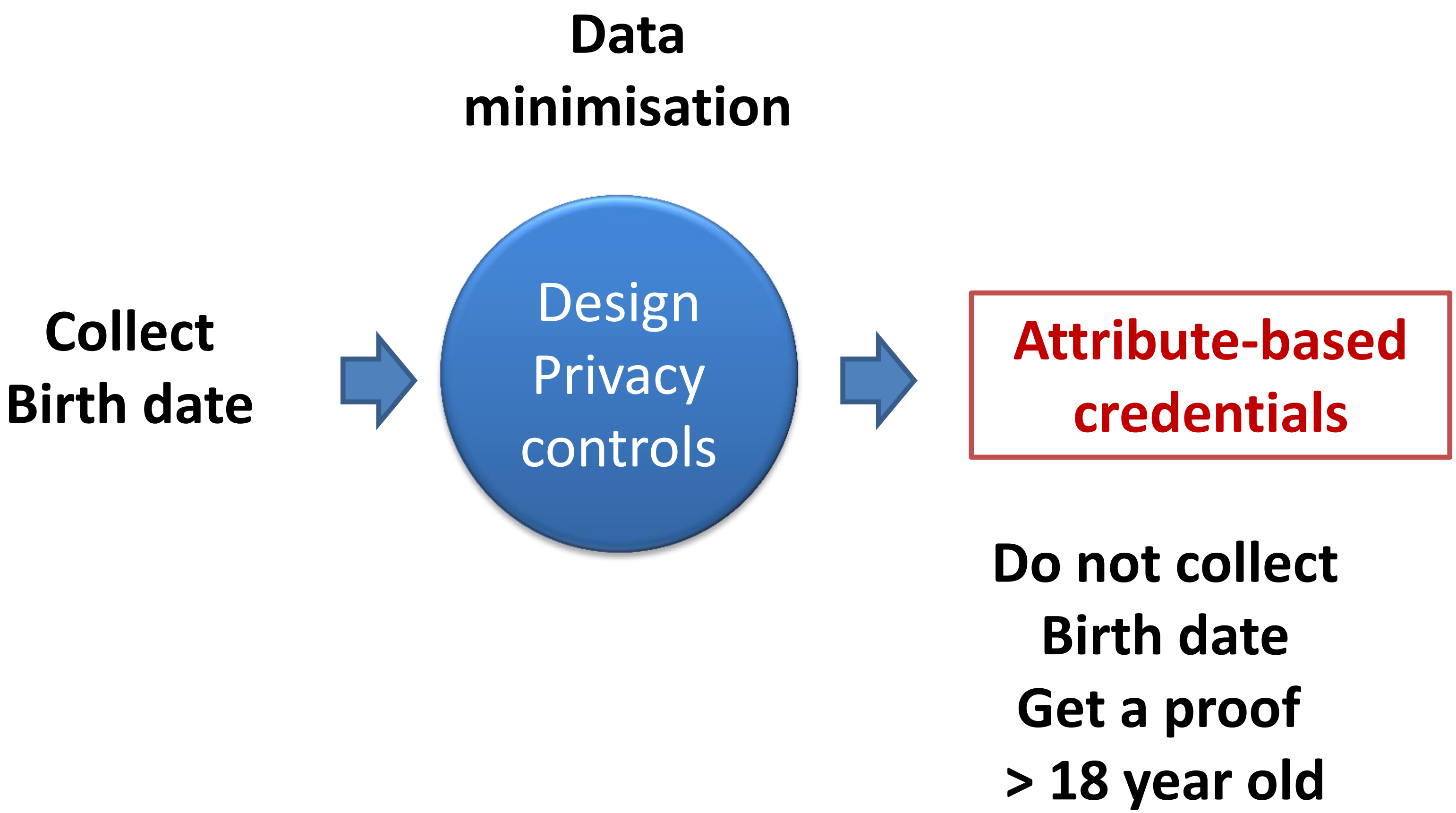


Design Strategies

Jaap Henk Hoepman Design strategies	1 Minimization	Select collecting, anonymisation / pseudonyms
	2 Hide	Encryption of data, mix networks, hide traffic patterns, attribute based credentials, anonymisation / pseudonyms
	3 Separate	Partitioning
	4 Aggregate	Aggregation over time, dynamic location granularity, k-anonymity, differential privacy
	5 Inform	Platform for privacy preferences, Data breach notification
	6 Control	User centric identity management, end-to-end encryption support control
	7 Enforce	Access control, Sticky policies and privacy rights management
	8 Demonstrate	Privacy management systems, use of logging and auditing



Design Strategies can Change Requirements



Data minimisation

Collect Birth date

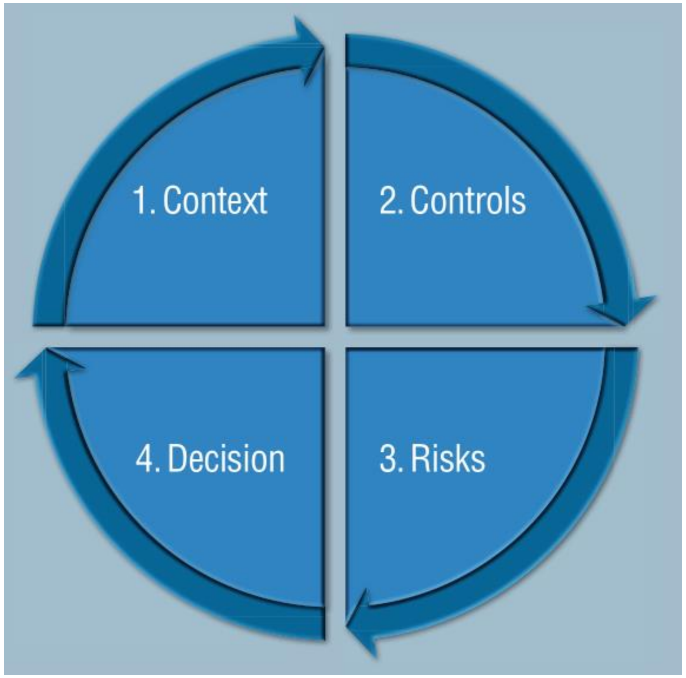
Design Privacy controls

Attribute-based credentials

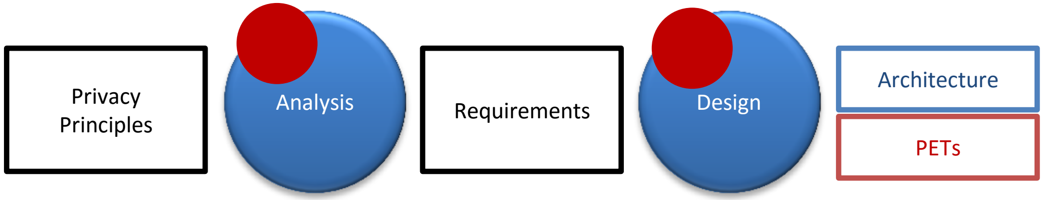
Do not collect Birth date Get a proof > 18 year old

PIA Process

- Risk analysis (example : CNIL risk analysis)



	Negligible Likelihood	Limited Likelihood	Significant Likelihood	Maximum 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				


Privacy Principles

Analysis

Requirements

Design

Architecture

PETs

Current Standards and Practices

It’s all about integration

Standards, References, Practices

- Principles
  - Ann Cavoukian seven's principles
  - ISO 29100 privacy framework (freely accessible)
- Impact assessment
  - ISO 29134 privacy impact assessment (in progress)
  - Data Protection Authority guidelines
    - UK
    - France
    - Spain
    - Germany (BSI)
  - Domain specific guidelines
    - Smart grid
    - Biometrics
    - RFid
    - Cloud

Standards, References, Practices

- Risk management
  - CNIL PIA methodology
  - NISTIR 8062 Privacy Risk Management Framework for Federal Information Systems
- Analysis and Design
  - OASIS Privacy management reference model and methodology
  - ISO 29151 personally identifiable information privacy control (in progress)
  - Privacy Patterns (in the making)
    - privacypatterns.org
    - Privacypatterns.eu

Standards, References, Practices

- Entire Lifecycle
  - PRIPARE methodology handbook (pripareproject.eu)
  - New ISO work item: Privacy engineering
  - And wealth of standards on engineering such as
    - Software and systems
      - ISO 29148 Requirements engineering
      - ISO 42010 Architecture
      - ISO 42020 Architecture Processes
      - ISO 15288 System Life Cycle Processes
      - ISO 12207 Software Life Cycle Processes
      - ISO 29110 Systems and Software Life Cycle Profiles and Guidelines for Very Small Entities
    - Domain specific standards
      - Automotive
      - Railways
      - Grid
      - …

It’s about Learning and Practicing

How can EIP-SCC help?

- EIP-SCC is the opportunity to work together
  - on the integration of privacy management
  - on compliance with GDPR
- EIP-SCC includes
  - Representatives of smart cities
  - Smart cities development projects
  - … and stakeholders promoting citizen focus

Smart Cities Representatives Concerns

- Ensuring compliance of supply side
  - Relation with application operators (data controllers/processors)
  - Overall compliance of chain of application operators
- Supervision and incident management
- Public relations management

Helping Smart Cities Representatives

- Identify approaches/guidelines/recommendations
  - for compliance assurance
    - GDPR
    - PIA practice
    - PbD practice
  - for supervision and incident management
  - for interactions with citizens
    - Consent
- Define privacy management integration plans
  - Synchronised with smart cities roadmap
- Experimenting with smart city projects

Application Operators Concerns

- GPDR compliance
- PIA compliance
- PbD compliance

GDPR

PIA

PbD

Purpose known

Data collecting

Data storage

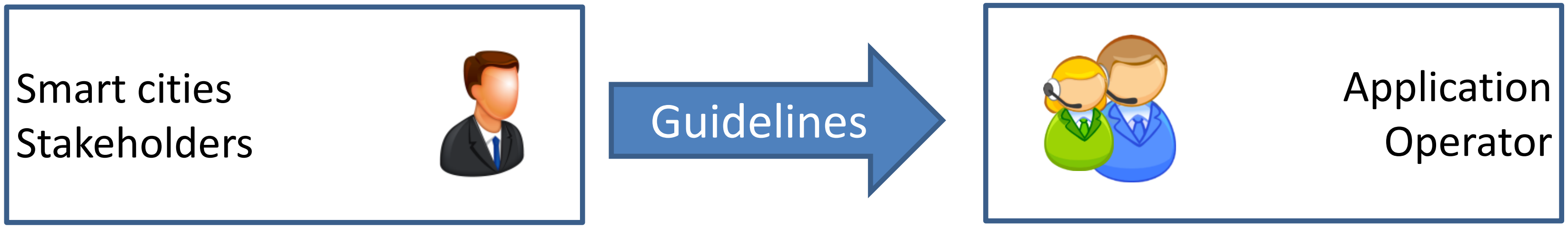
Data transformation

Data exchange

Data analytics

Helping Application Operators

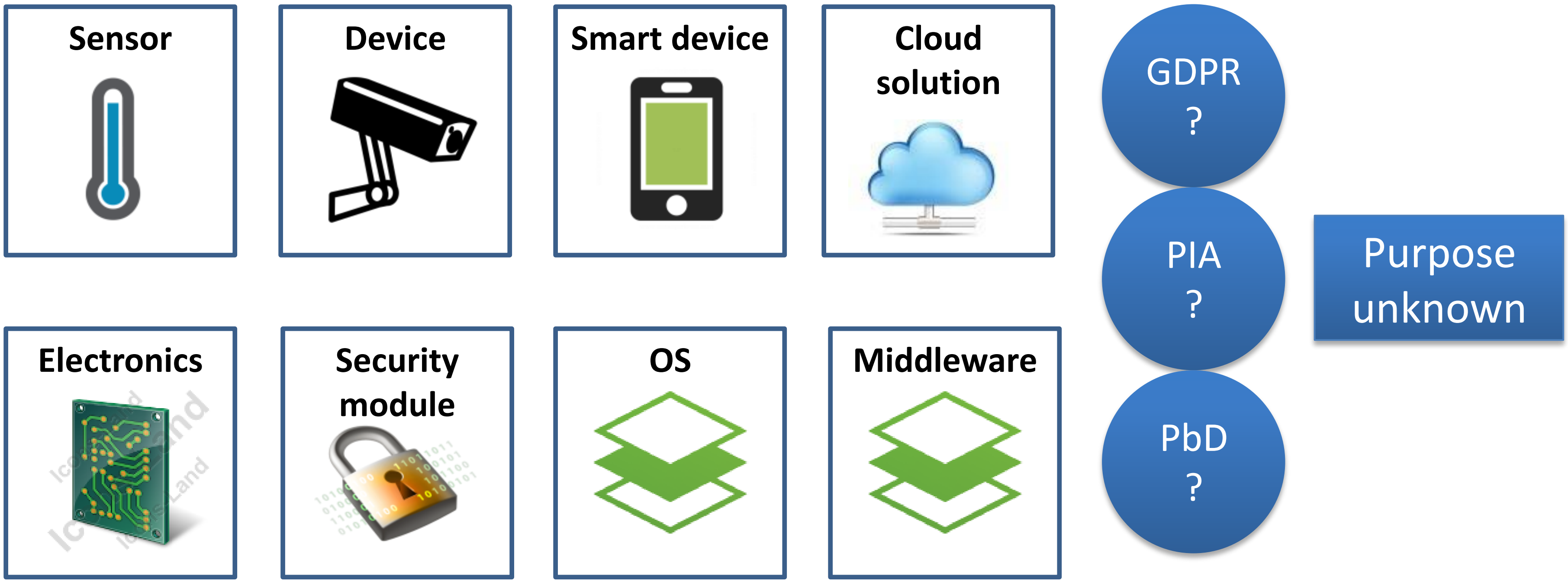
- Compliance guidelines



- Privacy impact assessment practice
- Privacy-by-design practice

Suppliers Concerns

- Categorised requirements



Sensor

Device

Smart device

Cloud solution

Electronics

Security module

OS

Middleware

GDPR ?

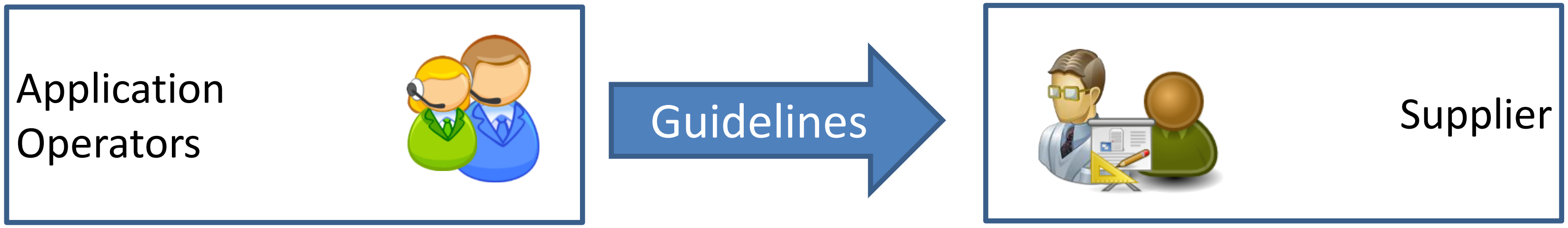
PIA ?

PbD ?

Purpose unknown

Helping Suppliers

- Categorised compliance guidelines



Application Operators

Guidelines

Supplier

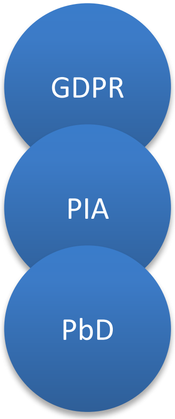
- Categorised privacy impact assessment practice
- Categorised generic privacy-by-design practice

Volunteering Smart Cities

- Nominate privacy officer
  - coordinates within SCC
- Participate to the work on approaches/guidelines/recommendations
  - for compliance assurance
  - for supervision and incident management
  - for interactions with citizen
- Get help in the definition of privacy management integration plans
  - Synchronised their roadmap
- Practice within smart city projects

Volunteering Smart City Projects

- Nominate a privacy officer stakeholder
  - Coordinates within SCC
- Participate to the definition of guidelines for operators
- Participate to the definition of guidelines for suppliers
- Practice
  - GPDR compliance
  - PIA compliance
  - PbD compliance



EIP-SCC Support

- Define a training program (and resource plan)
- Define a support program (and resource plan)
- Support volunteering cities and projects
  - Help define roadmap
  - Help define privacy management integration

Next steps

- Open discussion with a number of Smart City Stakeholders and Smart city Projects during general assembly

"BUILDING THE MARKET PLACE
FOR SMART CITIES IN EUROPE"
EUROPEAN
INNOVATION
PARTNERSHIP
SMART CITIES
AND COMMUNITIES
nl EU
2016
GENERAL
ASSEMBLY
EINDHOVEN | 24 MAY 2016