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

Privacy Management in Smart cities and Communities

Version: v0.20
Date: 01/9/2016
Confidentiality: Public
Author/s: Antonio Kung (Trialog)

PRIPARE has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no ICT-610613

Table of Contents

Document History

Version	Status	Date
V0.01	Initial version of the Table of contents	01/06/2016
V0.10	Initial version	25/08/2016

Author		
	Name	**Date**
	Antonio Kung	01/06/2016

List of Figures

List of Tables

Abbreviations and Definitions

Abbreviation	Definition
BSI	Bundesamt für Sicherheit in der Informationstechnik
CNIL	Commission nationale de l'informatique et des libertés
DPA	Data Protection Authority
DPO	Data Protection Office
EC	European Commission
EIP-SCC	European Innovation Platform on Smart Cities and Communities
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
OASIS	Advanced Open Standards for the Information Society
OWASP	Open Web Application Security Project
PbD	Privacy by Design
PbD-SE	Privacy by Design Documentation for Software Engineers
PEAR	Privacy Enhancing ARchitecture
PET	Privacy Enhancing Technology
PI	Personal Information
PIA	Privacy Impact Assessment
PII	Personal Identifiable Information
PMRM	Privacy Management Reference Model
PRIPARE	PReparing Industry to Privacy-by-design by supporting its Application in REsearch

Table 1: Acronym table

Executive Summary

This document provides and analysis of Smart cities and communities ecosystems in terms of privacy management needs.

It provides first an overview of what is at stake in terms of privacy management in a smart city ecosystem. It identifies three types of stakeholders in such ecosystems, the smart city representative, the smart city application operator, and the suppliers, and it explains their different viewpoints and concerns.

It then provides an overview of the engineering viewpoint in terms of privacy-by-design (PbD) and privacy impact assessment (PIA), covering the integration of privacy concerns in the lifecycle, the integration of PIA, privacy principles, the analysis phases, the design strategies and the PIA process.

It concludes with three recommendations:

- Reusing current standards and practices
- Learning and practicing in real cases, separating the practices of the three types of stakeholders (smart city representatives, smart city application operators and suppliers)
- Establishing guidelines for the smart city ecosystem using a framework approach.

In the case of Europe, it suggests to take advantage of the citizen approach for data initiative of the European Innovation Platform on smart cities and communities.

1 Introduction

Privacy is a concern that will have to be taken into account in smart cities and communities. In Europe the General Data Protection Regulation of GDPR was published on May 4th 2016. It will have to be applied by May 25th 2018. The GDPR will require

- the use of Privacy-by-design (PbD) and Privacy-by-default and the use of Privacy Impact Assessment (PIA) in the design of ICT systems involving personal data processing,
- the nomination of data protection officers for all public authorities and companies processing personal data for more than 5000 data subjects

Taking into account the GDPR will be business-critical as sanctions for breaches could amount to up to 20,000,000 EUR or up to 4% of the annual worldwide turnover.

To address the advent of the GDPR, PRIPARE[1] was started in October 2013 as a support action funded by the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 610613. Its mission has been twofold:

- facilitate the application of a privacy- and security-by-design methodology, support its practice by the ICT research community to prepare for industry practice; and
- foster risk management culture through educational material targeted to a diversity of stakeholders.

In December 2015, PRIPARE released the following material

- a set of documents describing the practice of privacy engineering,
- a set of educational material, and
- contribution to research.

The privacy- and security-by-design methodology handbook is the most important contribution of PRIPARE on privacy engineering. It captures and integrates the existing standards, practices and research proposals on privacy engineering [1].

But to be effectively used, the PRIPARE handbook must also be complemented with guidelines on how and who should use it. One of the most important most important challenges in today complex ICT ecosystems is to understand the roles and responsibilities of the various stakeholders in an ecosystem.

This document provides and analysis of Smart cities and communities ecosystems in terms of privacy management needs.

Note that while this document was prepared further to interactions with European stakeholders, in particular in the frame of the European Innovation Platform on Smart Cities and Communities[2], we believe that most of the content is general.

[1] See pripareproject.eu
[2] https://eu-smartcities.eu

2 Privacy Management In Smart Cities and Communities

2.1 Definitions

We will use the following terms in the document[3]:

- Privacy-by-design or PbD is defined as
    - the institutionalisation of privacy management in a company
    - the integration of privacy concern in the engineering of systems
- Privacy-by-default means that the highest level of protection is taken by default
- Privacy impact assessment or PIA is a process that evaluates the impact on privacy. It integrates risk analysis.

2.2 Privacy in Complex Ecosystems

Understanding how to manage privacy properly in complex ecosystem is a challenge (see Figure 1). When we talk today about smart cities, Big Data, of the Internet of things, we refer to complex ecosystems:

- They integrate business domains such as smart grid, health, transport
- They integrate concerns such as privacy, security or others, for instance safety

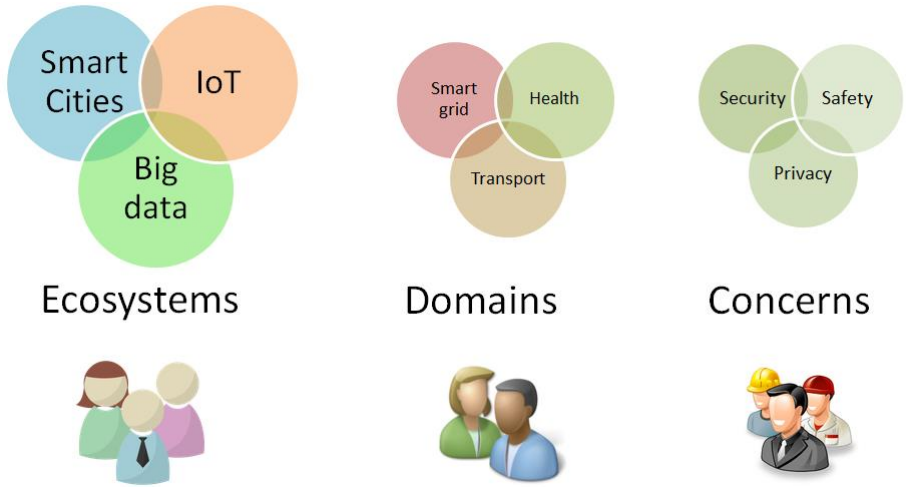

Figure 1: Concerns in Complex Ecosystems

From a privacy management perspective, we identify the following stakeholders in a smart city ecosystem (see Figure 2):

- The smart city public authority stakeholders, or policy maker.
- Application operators which collect personal data during operations (e.g. a transport application). Such operators interact with citizens on aspects such as purpose information, consent, transparency, empowerment. Operators must comply with regulation (e.g. GDPR in the EU), i.e. they must apply processes such as PbD and PIA upon building a system they operate. There are two types of operators, the data controller

[3] Note that the GDPR uses the term data protection by design and data protection by default instead of privacy-by-design and privacy-by-default

and the data processor. The data processor works for the data controller under some contractual relationship.

- Suppliers to application operators. They are also two types of suppliers: Integrators and suppliers to integrators. Integrators are in charge of building and providing a complete system to operators (e.g. a complete transport application). They are thus aware of the details of personal data collection during these systems operations, they know the purpose for which data is collected and processed. They will have to comply with contractual obligations set out by operators. They can apply PIA and PbD on the system they are integrating. On the other hand, suppliers to integrators (e.g. a storage system, a traffic sensor device, a user interface subsystem) are not aware of the purpose for which some personal data can be collected when they have designed the system they supply. They cannot apply fully PIA and PbD.

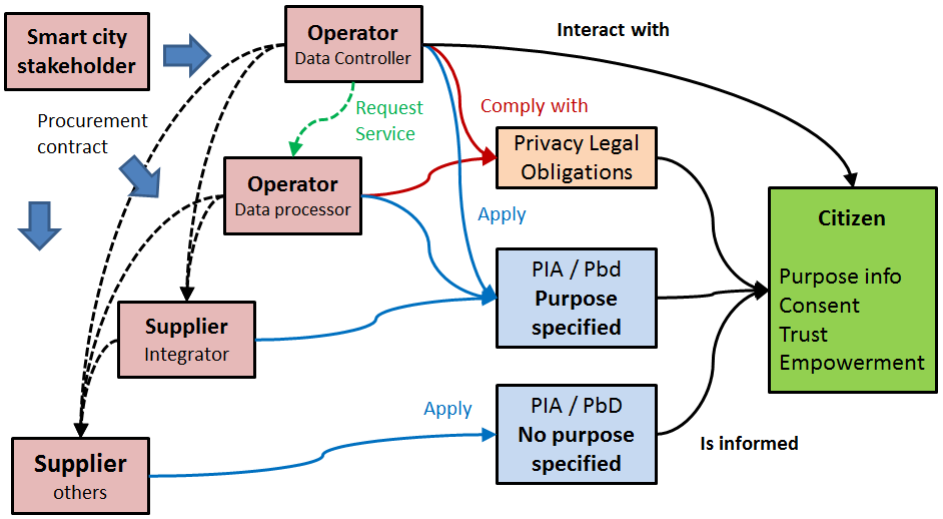

Figure 2: Stakeholders in Smart Cities Ecosystems

The concerns of the various stakeholders will differ. Figure 3 lists the types of stakeholders on the left column, from the demand side to the supply side. They include the policy maker, the operators and the suppliers. Each type of stakeholder has to deal with concerns as showed by each column on the right (legal compliance concern, management concern, system lifecycle concern) :

- The policy maker concern is to ensure overall compliance
- The operators concern is (1) to meet regulation, (2) to carry out the proper PIA practice from a management point of view, and (3) to carry out the proper PbD practice from system lifecycle viewpoint.
- The suppliers concern is to meet the operators requirements

<table>
<tr><th colspan="2">Stakeholder</th><th>Legal Compliance Level</th><th>Management Level</th><th>System Lifecycle Level</th></tr>
<tr><td rowspan="4">Demand side

Supply side</td><td>Policy maker</td><td colspan="3">Compliance Check</td></tr>
<tr><td>Operator Data Controller</td><td rowspan="2">Regulation GPDR</td><td rowspan="2">Privacy Impact Assessment PIA</td><td rowspan="2">Privacy-by-Design PbD</td></tr>
<tr><td>Operator Data processor</td></tr>
<tr><td>Supplier</td><td colspan="3">Operators Requirements</td></tr>
</table>

Figure 3: Stakeholder Concerns on Privacy

2.3 Smart City Stakeholder Concerns

The main concern of the demand side, i.e. public authorities and policy makers in a smart city environment is to ensure compliance. Figure 4 shows an example of application chain involving different operations on data, e.g. data collecting, data storage, data transformation, data exchange, data analytics, These operations can be managed by one or several application operators. Smart city stakeholder will require

- that each operator complies in terms of regulation (e.g. GDPR), management practice (PIA), and lifecycle practice (PbD);
- that the whole chain of applications also complies.

The smart city stakeholder has therefore to create a chain of responsibilities, from individual operators to himself, as the ultimate accountable stakeholder.

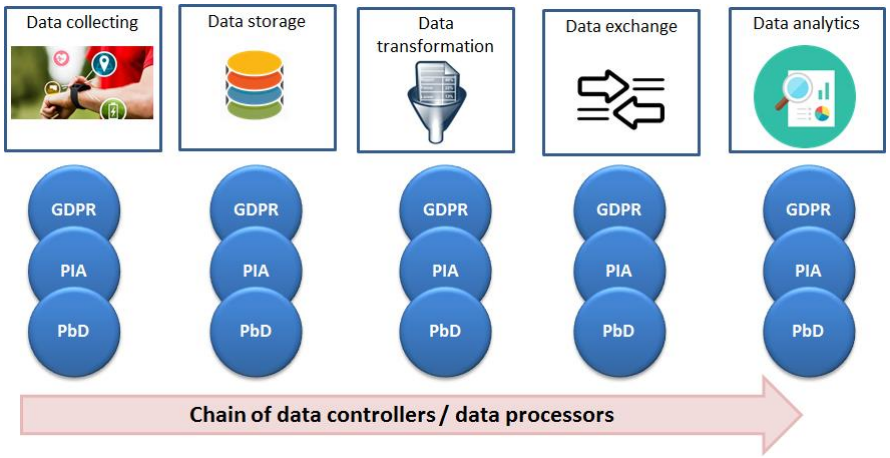

Figure 4: Smart City Stakeholder Concerns

2.4 Operator vs Suppliers

Application operators and suppliers have different concerns as showed in Figure 5:

- operators wish to meet the compliance requirements set out by the smart city stakeholders. Their concerns are related to the data controller and data processors

concerns, they want to follow the regulation and comply in terms of PIA and PbD practice

- suppliers provides products which the operator is using. The supplier concern is to meet the market demand.

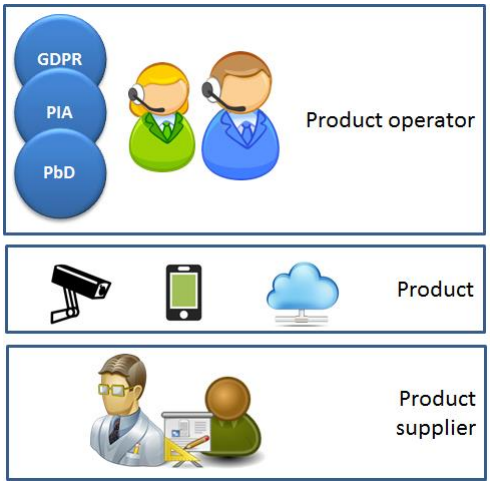

Figure 5: Operators vs Suppliers

2.5 Supply Side Concern

It is difficult to characterize the suppliers concern in terms of compliance with GDPR, or compliance with PIA and PbD practice. This is because of the following issues:

- there is *a wide spectrum of suppliers*. Figure 6 shows the following types of products involved:
    - end-products such as sensors, devices, smart devices, cloud solutions
    - component products such as electronics, security modules, operating systems, middleware.
- unless it is a bespoke system that is supplied, the *purpose for collecting data is unknown to the supplier*. For instance the supplier of storage system does not know the purpose for which the storage system will be used. Consequently, the supplier of such systems will have no incentive to provide data protection capabilities, unless the customer explicitly requires it;
- there is a *potential unbalance between big suppliers and small operators*. It seems as if suppliers will have to meet operators requirements. This is rarely the case when suppliers are dominating. A small operator company (e.g. a local SME in a city) will have literally no influence on the products he is using (e.g. a smart phone operating system).

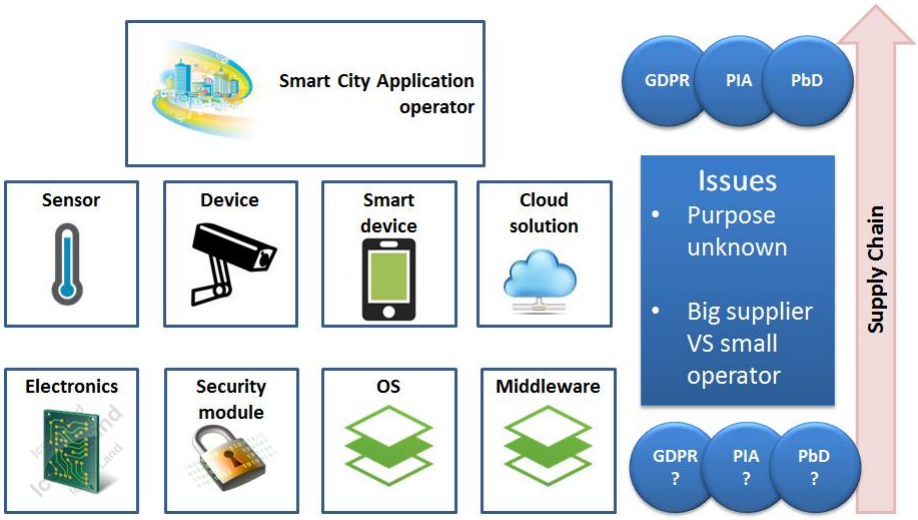

Figure 6: Supply Side Concerns

3 Privacy-by-design and Privacy Impact Assessment Engineering Viewpoint

The purpose of this section is to provide an overview on the problem of integrating PbD and PIA in an engineering design process.

3.1 Integrating Privacy Concerns in the Lifecycle

From an engineering viewpoint, the main objective is to integrate privacy concerns along the lifecycle process. Figure 7 is taken from the PRIPARE handbook [1]. It shows

- the various phases from the analysis, design, implementation, verification, release, maintenance and decommissioning. Each of these phases will have to integrate privacy concerns.
- a central item called environment and infrastructure which consists of company knowledge, best practice, assets. Design practices rely on this environment. When an external party (i.e. a smart city stakeholder) is in the process of selecting a supplier (i.e. a smart city application developer) this environment could be a key criteria to assess the supplier maturity in terms of privacy management practice.

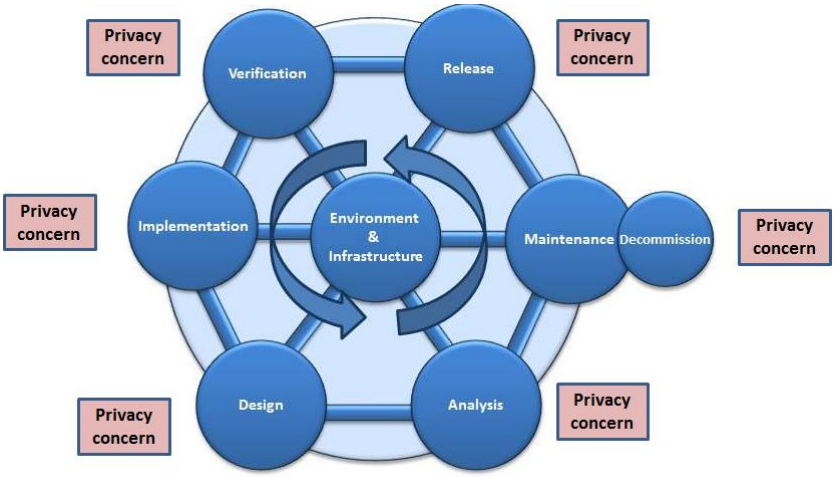

Figure 7: Integrating Privacy Concerns in Lifecycle

3.2 A Glimpse into the PbD Process

Figure 8 shows an example of how privacy impact assessment can be integrated in the privacy-by-design process, The example focuses on two phases of the lifecycle, analysis and design:

- the analysis phase is about transforming high level privacy principles into privacy requirements
- the design phase is about transforming privacy requirements into architecture decisions and mechanisms – often called PETS (privacy enhancing technologies) or privacy controls

3.2.1 Example of Integration of PIA in the Lifecycle

Figure 8 shows that the PbD process is carried out in parallel with the PIA process. In particular the PIA process is started during the analysis phase, and further continued in the design phase. During the analysis phase, the PIA process will focus on whether appropriate risks for privacy

breaches have been taken into account when identifying product requirements. During the design phase, the PIA process will focus on whether appropriate risks for privacy breaches have been taken into account when identifying privacy controls.

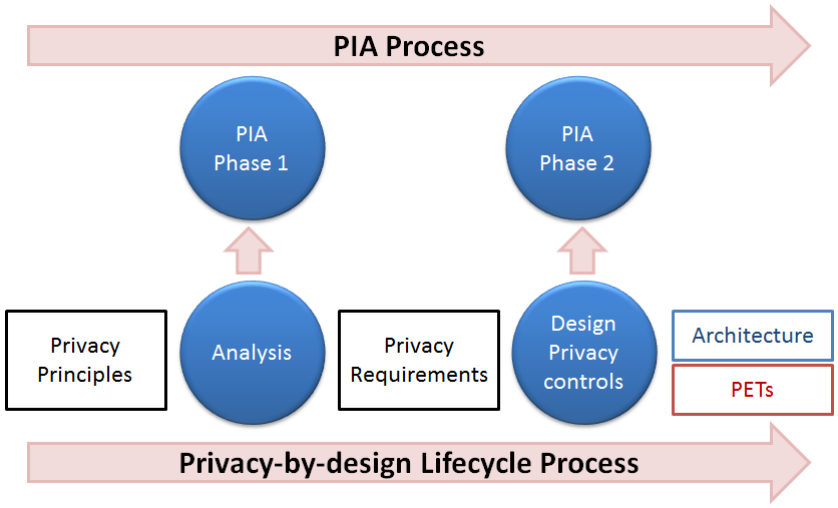

Figure 8: Integrating Privacy Impact Assessment in the Process

3.2.2 Privacy Principles

As showed in Figure 9, the Privacy-by-design process starts with the privacy principles. We can use for instance

- Ann Cavoukian seven principles [5]: proactive not reactive, privacy as default setting, privacy-by-design, positive sum, security, transparency, user-centric
- ISO 29100 standard [6]: Consent and choice, purpose, collection limitation, data minimization, use limitation, accuracy and quality, openness/transparency/notice, individual participation and access, accountability, security

Figure 9: Privacy principles in the Lifecycle

3.2.3 Analysis

The objective of the analysis phase is to transform privacy principles into privacy management services requirements. As showed in Figure 10, the starting point is the privacy principles. The analysis phase will yield a number of requirements on the system concerning privacy.

Figure 10: Requirement Analysis in the Lifecycle

The OASIS PMRM standard [2] addresses this phase. PMRM stands for Privacy Management Reference Model and Methodology. The PMRM methodology is use-case based and of iterative nature. The approach is to specify use cases, to consider privacy principles, and come up with privacy service requirements, following the categories of service listed in Table 2. For instance privacy principles related to accountability could be taken into account by the enforcement service category.

Service	Purpose
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

Table 2: PMRM Services

3.2.4 Design Strategies

Once the privacy management service requirements have been defined we must design the privacy controls, as showed in Figure 11. This phase will provide (1) architecture decisions and (2) technology decisions (PETs).

Figure 11: Design Strategies in the Lifecycle

Jaap Henk Hoepman [7] provides a list of design strategies as showed in Table 3. There are two groups of design strategies: data collecting strategies and data processing strategies. Each strategy can be associated with two types of privacy control decisions*: architecture decisions* (they are showed in italics green, for instance partitionning, or dynamic location granularity); *technology PETS decisions* (they are showed in red, for instance differential privacy).

Strategy	Privacy Control Decisions
Minimization	*Select collecting*, anonymisation / pseudonyms
Hide	Encryption of data, mix networks, hide traffic patterns, *attribute based* credentials[4], anonymisation / pseudonyms
Separate	*Partitioning*
Aggregate	Aggregation over time, *dynamic location granularity*, k-anonymity, differential privacy
Inform	Platform for privacy preferences, Data breach notification
Control	User centric identity management, end-to-end encryption support control
Enforce	Access control, Sticky policies and privacy rights management
Demonstrate	Privacy management systems, use of logging and auditing

Table 3: Design Strategies

[4] Attribute-based credentials integrate technology decisions as well as architecture decisions

Note that the application of design strategies can change requirements. Figure 12 shows an example related to collecting the birth date (for instance to check that a person is over 18 years old). The data minimisation strategy could lead to the use of PETs such as attribute-based credentials where it is sufficient to collect a proof that the person is above 18 years old. The initial requirements (e.g. collect birth date) can be modified to a less privacy intrusive requirement (e.g. collect proof that person is over 18).

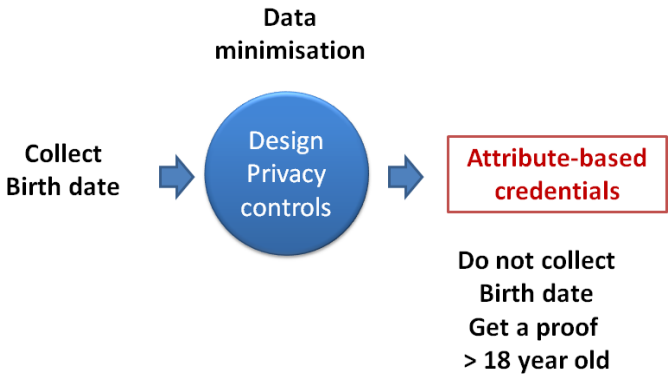

Figure 12: Design can change Requirements

3.2.5 PIA Process

The PIA process must be carried out both during the analysis phase and the design phase in the example of Figure 13 (note that in practice a PIA process must be carried out during the entire lifecycle process. We focus on the first two phases for the sake of the example).

Figure 13: PIA in the Lifecycle

The analysis phase and the design phase include a risk analysis part. This can be considered as the common intersection between the PbD process and the PIA process. In the following example we have taken the PIA methodology proposed by CNIL [3], the French DPA. It includes a number of phases (Figure 14):

- describe context ;
- identify existing or planned controls ;
- assess privacy risks. This assessment implies an impact analysis and a positioning in a heat map (Figure 14). The map has two dimensions, on the X axis, likelihood that the risk is materializing, on the Y axis, the severity of the impact;
- decide (whether the controls to be used is sufficient).

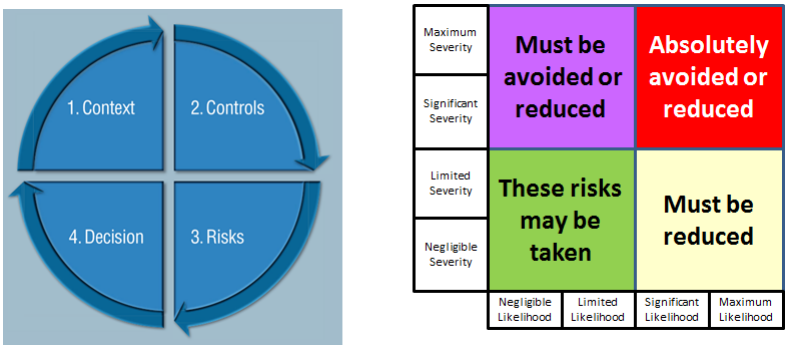

Figure 14: CNIL PIA Methodology

4 Recommendations

The following recommendations are made:

- Reuse current standards and practices
- Learn and practice
- Establish guidelines for smart cities and communities using a framework approach

4.1 Reusing Current Standards and Practices

Here is a short list of applicable standards and practices.

- At the level of principle, Ann Cavoukian's principles [5] or ISO 29100 [6]
- At the level of impact assessment
    - We have a standard that is nearly final (Draft International standard level), ISO 29134 Privacy impact assessment -- Methodology Privacy impact assessment - Guidelines
    - The data protection authorities have produced guidelines for instance in the UK[5], France[6], Spain[7] or Germany[8]
    - In addition there are domain specific guidelines for smart grid, biometrics, RFID, and the cloud.
- At the level of risk management we can mention the CNIL PIA methodology [3], or the the NIST privacy risk management framework [4]
- At the level of analysis and design we can mention
    - OASIS PMRM already presented [2]
    - The draft international standard, ISO 29151 Code of Practice for PII Protection
    - As well as initiatives for sharing privacy design patterns[9]
- Concerning the entire lifecycle we can mention
    - The methodology handbook contributed by PRIPARE [1]
    - its continuation at the standardisation level[10]
    - and a wealth of existing standards related to system and software engineering (in ISO/IEC SC7)[11]

[5] https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
[6] https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf
[7] https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
[8] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Kurzfasssung.pdf?__blob=publicationFile&v=1
[9] Such as http://privacypatterns.eu/ or http://privacypatterns.org/
[10] A new work item : ISO/IEC 21876 Privacy Engineering has being established.
[11] http://www.iso.org/iso/iso_technical_committee%3Fcommid%3D45086

4.2 Learn and Practice

It is important that each smart city undertaking the deployment of ICT applications also undertakes the associated privacy management practice. Establishing collaboration and coordination between cities is also the opportunity to exchange learning experience and practices and therefore accelerate the adoption of effective best practices. This must involve the following stakeholders: smart city representatives, smart city applications operators, and suppliers.

4.2.1 Smart City Representatives Learning and Practicing

We saw in section 2.3 that smart city representatives concerns are about ensuring compliance in terms of regulation, management practice and lifecycle practice. Representatives will have to learn and practice the following

- practicing supervision and compliance verification. This includes their interactions with application operators, at procurement level, operation level, incident level. It also includes the supervision of the global chain (i.e. whether the suppliers to the application operators comply);
- practicing incident management. In case of a privacy breach;
- practicing interactions with citizens. This is also known as public relations. It covers the information that must be provided to the citizens on how smart city applications handle privacy, on reporting incidents that may happen and management the solving of incidents.

4.2.2 Application Operators Learning and Practicing

We saw in section 2.4 that smart city application operators concerns are about ensuring regulation compliance, PIA compliance and PbD compliance. Application operators will have to learn and practice the following

- interacting with smart city representatives on privacy requirements, on privacy monitoring and on privacy incident management;
- regulation compliance verification practice;
- privacy impact assessment / Risk analysis practice;
- privacy-by-design / Privacy engineering practice;
- interacting with suppliers on privacy requirements[12].

4.2.3 Suppliers Learning and Practicing

We tried to characterize suppliers concerns in section 2.5. Their concern is to meet the market demand. They do not have to comply with regulation or privacy-by-design, but in a fully working market they would have to provide support for privacy-by-design. Suppliers will have to learn and practice the following

- interacting with the whole ecosystem on a privacy framework for their category of product (e.g. a privacy framework for cloud, for big data, for sensors…);
- interacting with application operators on privacy management features their subsystems can provide.

[12] We saw that isolated application operators might have too small weight. This is the reason why it will be important that application operators coordinate their needs (with the help of smart city representatives)

4.3 Establish Guidelines for the Smart City Ecosystem

In order to benefit from the overall exchange of practices, it is important to establish subsequently guidelines in such a way that a common set of recommendations and practices can be agreed upon why allowing specific aspects to be explained in customised profiled use case. We believe that a three-phase approach must be taken:

- Phase 1: Learning and practicing privacy management in specific cities
- Phase 2: Extracting a common set of recommendations and establishing a smart city privacy management framework
- Phase 3: Categorizing existing practices into domains or profiles and establishing specific requirements (e.g. at country level, at domain level such as smart grids)

4.4 Proposal for Europe

4.4.1 Taking Advantage of EIP-SCC as a Common Platform

The European Innovation Partnership on Smart Cities and Communities (EIP-SCC)[13] is an initiative supported by the European Commission bringing together cities, industry, SMEs, banks, research and other smart city actors. The coordination platform includes 370 commitments from 4000 organisations in 31 countries.

To foster a coordinated learning and practice, the citizen centric approach to data initiative has been launched in EIP-SCC[14]. The objective is to implement a privacy-by-design approach to protect citizen rights for privacy. The aim of this group is to institutionalize concepts of privacy in organisations involved in the Smart City value chain and integrate these concepts in the design of systems. All this will be possible through data protection guidelines with a focus on a citizen-centric viewpoint.

4.4.2 Citizen Centric Approach to Data Initiative

The citizen centric approach to data initiative proposes the following plan:

- Identify a number of cities and projects that are willing to participate to the programme. The benefits for these volunteers will be to learn and practice faster.
- The actions carried out by smart cities could be the following:
    - nominate a data privacy officer who will participate to the initiative;
    - establish a pilot project involving application operators and suppliers who will practice privacy management with the support of EIP-SCC;
    - participate to the work on approaches/guidelines/recommendations.
- The actions carried out by a project (which in general could include several cities) could be
    - nominate a project data privacy officer who will participate to the initiative;
    - establish a pilot project involving application operators and suppliers who will practice privacy management with the support of EIP-SCC;
    - participate to the work on approaches/guidelines/recommendations.

[13] https://eu-smartcities.eu/
[14] https://eu-smartcities.eu/content/citizen-centric-approach-data-privacy-design

- The actions carried out by EIP-SCC could be
    - undertake a training program (and resource plan);
    - undertake a support program (and resource plan);
    - lead the establishment of guidelines;
    - promote the guidelines at standardization level.

5 References

[1] PRIPARE Methodology Handbook. http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf

[2] Organization for the Advancement of Structured Information Standards (OASIS), *Privacy Management Reference Model and Methodology (PMRM)*, Version 1.0. July 2013. http://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.pdf

[3] CNIL, "PIA Manual 1 - Methodology (how to carry out a PIA)". https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

[4] National Institute of Standards and Technology (NIST), *NISTIR 8062 (Draft): Privacy Risk Management for Federal Information Systems*. http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf

[5] Ann Cavoukian. Privacy-by-Design. The seven foundational principles. https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf , last visited on 21.06.2016

[6] ISO/IEC, ISO/IEC 29100. Information technology — Security techniques — Privacy framework, freely available at the following link: http://standards.iso.org/ittf/PubliclyAvailableStandards/c045131_ISO_IEC_TR_29108_2013.zip

[7] Jaap Henk Hoepman, Privacy design strategies. ICT Systems Security and Privacy Protection - 29th IFIP TC 11 Int.Conf, SEC 2014, Marrakech, Morocco