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

Consistent Set of Standards for Privacy in Smart Cities

Version:	v0.10
Date:	24/03/2017
Confidentiality:	ISO/IEC JTC1
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

Author		
	Name	**Date**
	Antonio Kung	21/03/2017

List of Figures

List of Tables

Abbreviations and Definitions

Abbreviation	Definition
EIP-SCC	European Innovation Platform on Smart Cities and Communities
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
PIA	Privacy Impact Assessment
PRIPARE	PReparing Industry to Privacy-by-design by supporting its Application in REsearch

Table 1: Acronym table

1 Introduction

This contribution is based on:

- Findings from the European Innovation Platform on Smart Cities and Communities (EIP-SCC) in the initiative Citizen Approach to Data: Privacy-by-Design[1]. A PRIPARE recommendation document was published and submitted to the ISO/IEC JTC1/SC27/WG5 study period on Privacy in Smart Cities for the Dubai meeting in October 2016 [1].
- Discussions in a workshop that was organised by the H2020 SharingCities project on GDPR compliance [2]. This workshop involved representatives of the cities of London, Milan and Lisbon.
- The PRIPARE contribution for the SP security guidelines for the IoT and the privacy guidelines for the IoT [4].

2 Privacy in Complex Ecosystems

Privacy in ICT ecosystems is complex.

Figure 1 (taken from [1]) shows the multiple ecosystems (e.g. smart cities, IoT, big data), domains (e.g. smart grids, health, transport) and multiple concerns (privacy, security, safety) that must be taken into account.

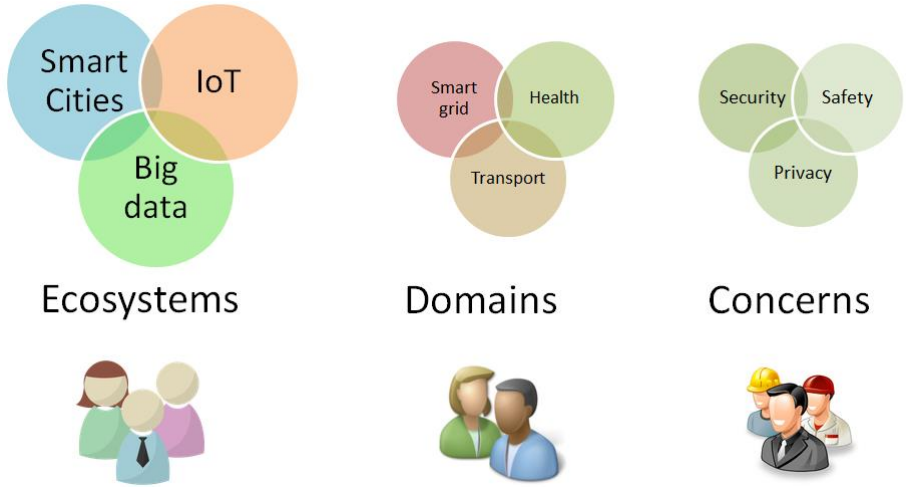

Figure 1: Ecosystems, domains and concerns

Figure 2 (taken from [1]) shows the stakeholders' specific roles in a smart city undertaking:

- Municipalities
    - define a a privacy management plan,
    - build and deploy a privacy management system.
- Data controllers
    - obtain consents from citizens (PII principals),
    - comply with privacy legal obligations,

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

- negotiate with data processors,
- carry out privacy impact assessment and practice privacy engineering.

- Data processors
  - comply with privacy legal obligations,
  - carry out privacy impact assessment and practice privacy engineering.
- Integrators
  - carry out privacy impact assessment and practice privacy engineering.
- Suppliers
  - do not know the purpose of the system in which their product will be integrated,
  - must still practice privacy engineering i.e. identify the privacy capabilities that they could offer to their customers.
- Citizens (or PII principals)
  - interact with data controllers on consent,
  - are informed through transparency mechanism,
  - enjoy the resulting smart city applications,
  - must still practice privacy engineering i.e. identify the privacy capabilities that they could offer to their customers.

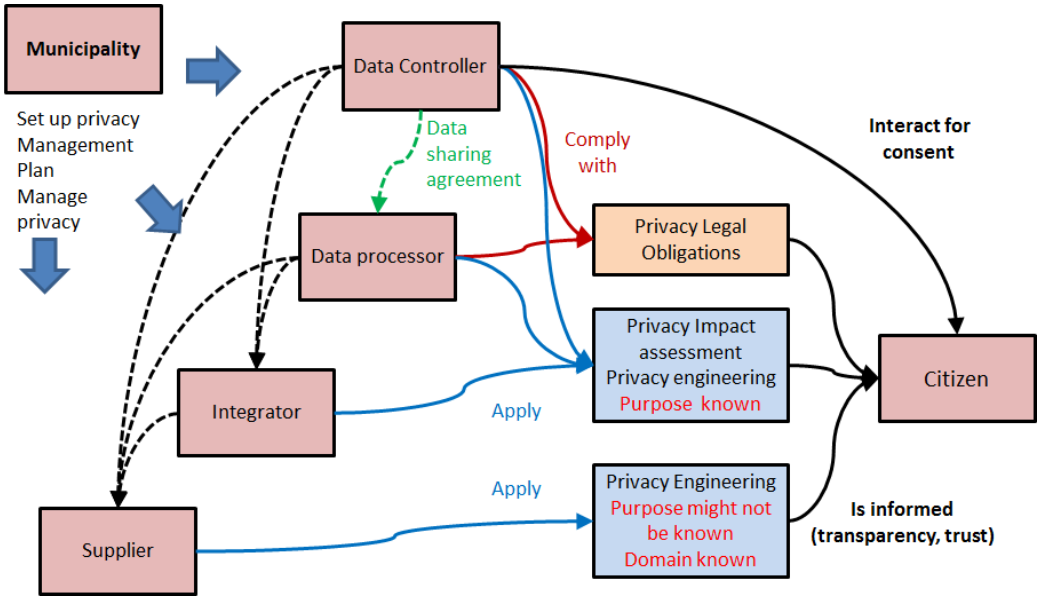

Figure 2: Privacy management in smart cities

3 Need for Privacy Management in Smart Cities

Privacy was discussed during a two-day workshop [2] organised by the H2020 SharingCities project. SharingCities is a large scale project involving three lighthouse cities (London, Milan, Lisbon) and three followers cities (Bordeaux, Burgas, Warsaw) with the objective of developing, experimenting and replicating a variety of applications (energy management, building retrofit, e-mobility, smart lamp post).

The following conclusions were drawn during the workshop, which we believe could be applied to most big smart city undertakings:

- **Need for global privacy management:** in parallel to the building, experimentation and replication of ICT assets within the cities, a global privacy management is needed to keep track and monitor the personal data assets that are exploited.
- **Need for interoperability of privacy management information**: privacy impact assessment and privacy engineering are processes that need to be carried out in so that some of their outcome will inform the global privacy management system.
- **Need for reusability of privacy management information**: when an ICT application that has already been deployed in a city A is replicated in another city B, it would be of interest to assess if the management information associated with the privacy impact assessment and privacy engineering carried out in the city A can be reused in city B.

We conclude that there is a need for privacy management standards for smart cities.

Table 2 provide examples of such standards.

Category of Standard	Example of possible standards
Global privacy management	Framework for privacy management in smart cities Guidelines for practice management practice • Creation of privacy management plans • Privacy policy making • Managing acceptance of privacy impact assessments • Global management of personal data assets • Accountability management • Transparency management • Breach reporting management • …
Interoperability of privacy management information	Common privacy management information model • Privacy impact assessment information (contact points, description of collected personal data, description of processing purpose, description of risks and measures, description of auditing agreements…)
Reusability of privacy management information	Guidelines for privacy management information replication

Table 2: Examples of smart city privacy management standards

4 Need for a Consistent Set of Privacy Standards in Smart Cities

As a matter of fact, smart cities ecosystems will involve IoT and Big data. Figure 1 shows a Venn diagram with three ICT ecosystems, smart cities, big data and IoT. The three ecosystems are related as follows:

- Many smart cities applications are big data applications, for instance in Amsterdam[2], Berlin[3], London[4] or Paris[5].
- Many smart cities ICT systems are IOT systems. As stated in [5], *the Internet of Things (IoT) shall be able to incorporate transparently and seamlessly a large number of different and heterogeneous end systems, while providing open access to selected subsets of data for the development of a plethora of digital services*.

There is therefore a need to provide a consistent set of privacy standards. A possible focus distribution that would ensure consistency would be the following:

- privacy standards for smart cities focus on privacy management,
- privacy standards for IoT focus on privacy capability in things (as explained in [4]),
- privacy standards for big data sent focus on datasets privacy management.

Table 3 shows examples of standards based on this focus distribution.

Ecosystems	Standard focus
Smart cities	Privacy management • Global privacy management • Interoperability of privacy management information • Reusability of privacy management information
IoT	Privacy capabilities in things • guidelines to design privacy capabilities in things • privacy level agreements in things for interoperability • IoT application privacy-by-design using things with privacy capabilities
Big data	Datasets privacy management • Privacy guidelines for datasets constructions (e.g. using IoT standards) • Datasets exchange agreements • Privacy guidelines for datasets analytics

Table 3: Ecosystems standard focus

[2] http://data.amsterdam.nl/
[3] https://daten.berlin.de/
[4] https://data.london.gov.uk/
[5] https://opendata.paris.fr

Figure 3 shows the relationships between these standards as well as the existing standards.

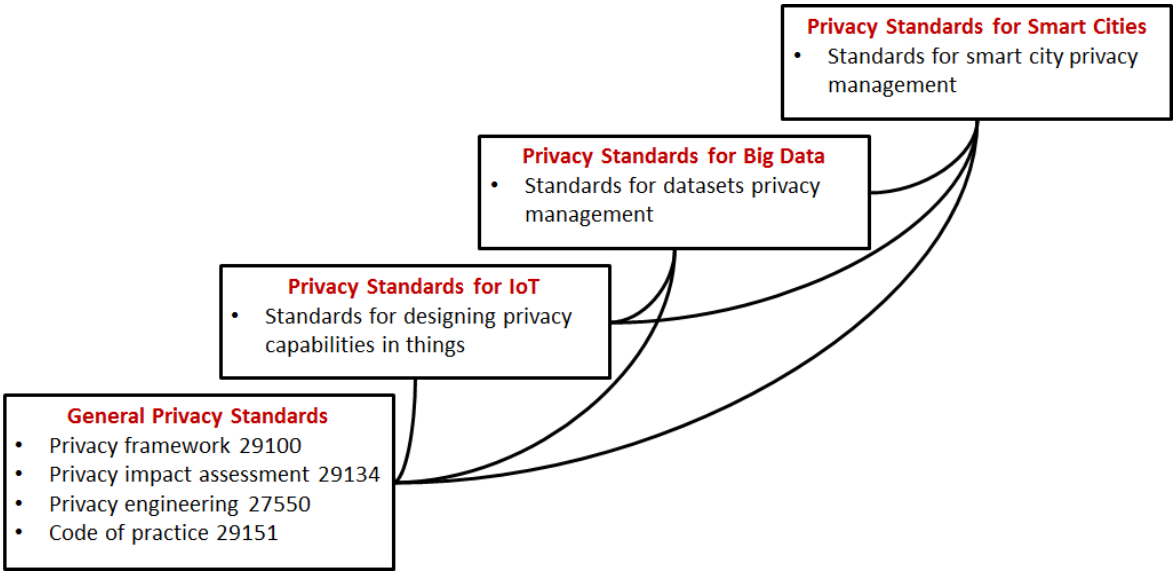

Figure 3: Consistent set of privacy standards

5 Proposal for Further Work in SP Privacy in Smart Cities

We suggest to extend the SP privacy in smart cities for another six-month. The objective would be to discuss whether a consensus can be reached on future courses of actions concerning privacy standards for smart cities, in particular

- refine the needs for privacy management standards and propose a roadmap.
- agree on the focus for privacy standards in big data and IoT. This would also benefit from some coordination between SC27, WG9 Big data, WG10 Smart Cities and SC41 IoT

6 References

[1] PRIPARE Recommendations for smart cities. ISO-IECJTC1-SC27-WG5_N0477_PRIPARE_contr_2nd_CfC_SP_Smart_Ci (Dubai, Oct 2016) or https://eu-smartcities.eu/sites/all/files/PRIPARE%20recommendations%20for%20Smart%20cities.pdf.

[2] Sharing Cities workshop on Privacy Complance.London, March 7-8th 2017. A report on the workshop is under preparation that will be published soon (http://www.sharingcities.eu/)

[3] PRIPARE Contribution to SP Privacy in Smart Cities (Dubai, Oct 2016). WG5_N0400 or https://eu-smartcities.eu/sites/all/files/PRIPARE%20recommendations%20for%20Smart%20cities.pdf.

[4] PRIPARE Contribution to SP Security guidelines for the IoT and SP Privacy guidelines for the IoT (Hamilton April 2017). ISO-IECJTC1-SC27-WG5_N0718_PRIPARE_contr_to_SP_Privacy_guidelines_for_IoT.

[5] Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, Michele Zorzi, IEEE Internet of Things for Smart Cities. IEEE Internet of things journal. Vol.1, N°1, February 2014. http://ieeexplore.ieee.org/document/6740844/