TECHNICAL SPECIFICATION

ISO/IEC TS 27570

First edition
2021-01

Privacy protection — Privacy guidelines for smart cities

Reference number
ISO/IEC TS 27570:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The growing integration of ICT technologies (e.g. cloud computing, IoT, big data, mobile networks, artificial intelligence and machine learning) in smart cities will allow for improved data sharing capabilities to achieve better services. But the growing complexity of the ICT infrastructure will also create vulnerabilities at security and privacy level. Security incidents can lead to essential services not operating properly, for instance a massive electricity supply shortage. Likewise, unauthorized access to personal data can lead to major privacy breaches, for instance access to personal health data records.

Ensuring that privacy is properly dealt within smart cities is a challenge. First, a wide variety of public and private stakeholders can be involved such as:

— agencies in charge of managing essential city services for instance administration services;

— business organizations in charge of operating services for instance electricity distribution:

— organizations in supply chains associated with the deployment of related infrastructure for instance transport systems; and

— associations representing the viewpoints of citizens.

Secondly, a wide variety of standards can be used such as:

— privacy standards;

— smart city standards;

— cloud computing standards;

— IoT standards;

— big data standards; and

— IT governance standards.

Figure 1 shows examples of such standards. This document thus focuses on providing guidance on the use of standards, while taking into account the variety of stakeholders in a smart city ecosystem.

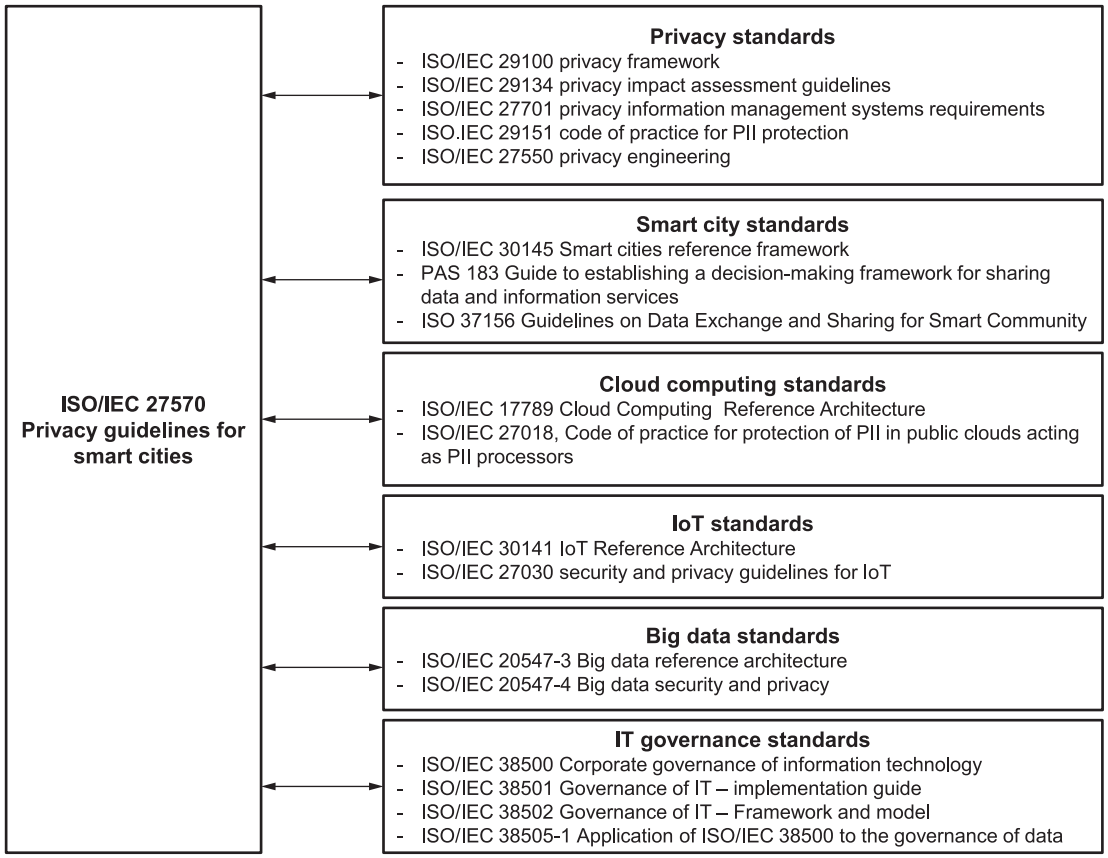

Figure 1 — Examples of standards to reference

Figure 2 summarizes privacy recommendations to smart cities ecosystems in this document, further numbered R6.1, R6.2, R6.3, and R6.4.

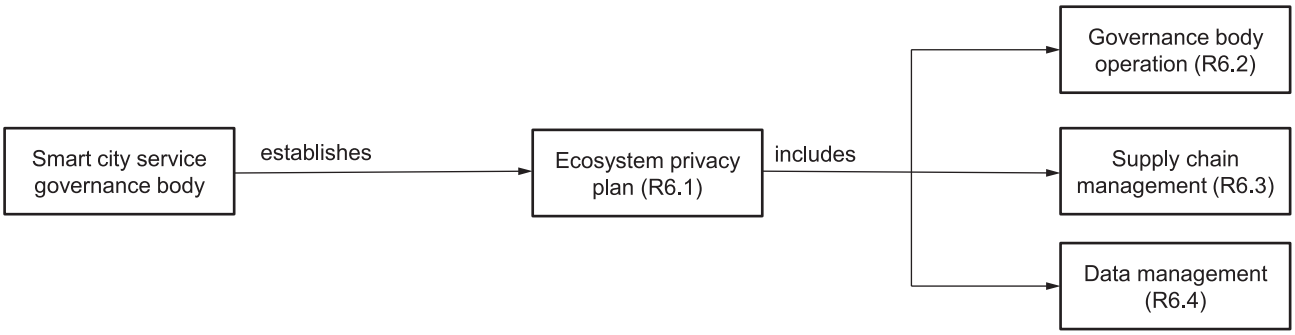

Figure 2 — Ecosystem guidance for privacy

Figure 3 summarizes privacy recommendations to smart cities processes in this document, further numbered R8.2, R8.3, R8.3, R8.4, and R8.5.

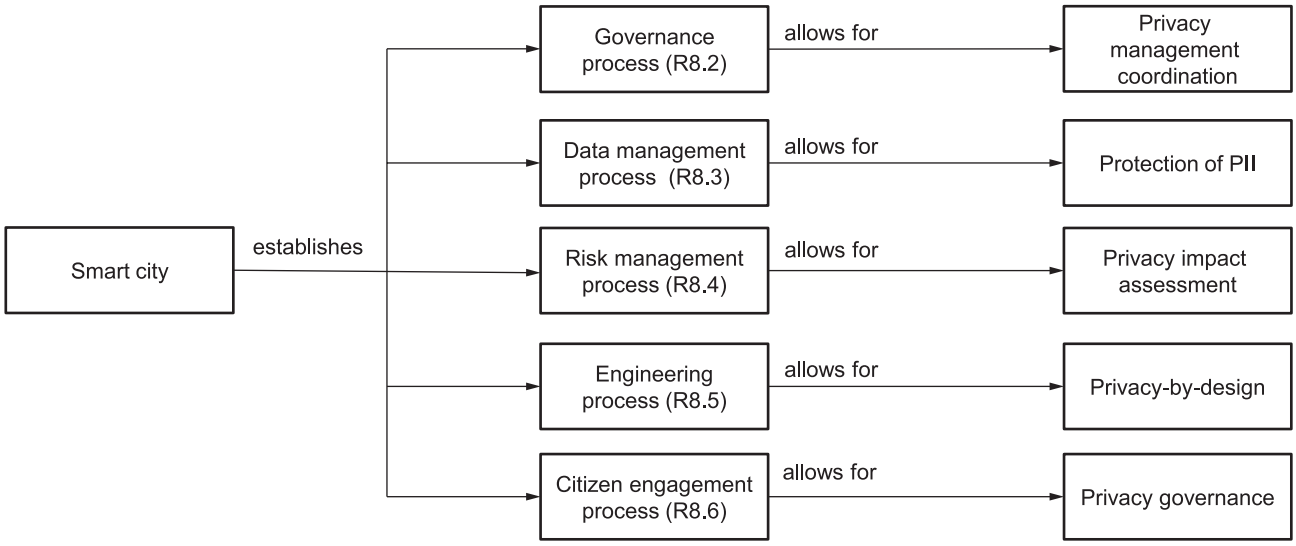

Figure 3 — Process guidance for privacy

It is foreseen that this document will pave the way to future privacy standards for smart cities. Table 1 provides a list of possible future standards.

Table 1 — Examples of possible future standards

Category	Standards
Privacy management to keep track and monitor PII assets that are exploited in smart cities.	Framework for privacy management in smart cities Guidelines for communication between organizations Guidelines for privacy management plans in smart cities Guidelines for privacy policy making in smart cities including data retention Guidelines for privacy impact assessment reports in smart cities Guidelines for consent management in smart cities Guidelines for privacy accountability and transparency management in smart cities Guidelines for privacy breach management in smart cities Guidelines for privacy-by-design of smart city services Guidelines for the integration of privacy concerns in data exchange agreements Smart city services security and privacy assurance
Privacy engineering in smart city ecosystems	Guidelines for privacy engineering[a] in smart cities
Collaboration in smart city ecosystems	Guidelines for citizen engagement Guidelines for communication between organizations (for each type of organization, e.g. administration)
Interoperability to avoid vendor lock-in	Common privacy management information model in smart cities Common privacy impact assessment information in smart cities Common description of privacy capabilities in smart cities Common description of privacy incidents in smart cities

[a] Privacy engineering focuses on the integration of privacy concerns in the engineering of a system.

Privacy protection — Privacy guidelines for smart cities

1 Scope

The document takes a multiple agency as well as a citizen-centric viewpoint.

It provides guidance on:

— smart city ecosystem privacy protection;

— how standards can be used at a global level and at an organizational level for the benefit of citizens; and

— processes for smart city ecosystem privacy protection.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations that provide services in smart city environments.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
activity
set of cohesive *tasks* (3.32) of a *process* (3.25)

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.3]

3.2
agency
organization (3.13) providing a specific service for a city

3.3
availability
property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.4
citizen
inhabitant of a city

3.5
citizen engagement
involvement of *citizens* (3.4) in the decision-making of public policies

3.6
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or *processes* (3.25)

[SOURCE: ISO/IEC 27000:2018, 3.10]

3.7
data protection officer
person appointed by the *PII controller* (3.15) to ensure, in an independent manner, compliance with the privacy law/regulation requirements

3.8
ecosystem
infrastructure and services based on a network of *organizations* (3.13) and stakeholders

Note 1 to entry: Organizations can include public bodies.

3.9
ecosystem privacy plan
planned arrangements for ensuring that privacy is adequately managed in an *ecosystem* (3.8)

3.10
governance
system of directing and controlling

[SOURCE: ISO/IEC 38500:2015, 2.8]

3.11
integrity
property of accuracy and completeness

[SOURCE: ISO/IEC 27000:2018, 3.36]

3.12
intervenability
property that ensures that *PII principals* (3.16), *PII controllers* (3.15), *PII processors* (3.17) and supervisory authorities can intervene in all privacy-relevant data processing

Note 1 to entry: The extent to which any of these stakeholders can intervene in data processing can be limited by relevant legislation or regulation.

[SOURCE: ISO/IEC TR 27550:2019, 3.6]

3.13
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity of institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO 37100:2016, 3.2.3, modified — Note 2 to entry has been omitted.]

3.14
personally identifiable information
PII
any information that a) can be used to identify the *PII principal* (3.16) to whom such information relates, or b) is or might be directly or indirectly linked to a PII principal

Note 1 to entry: To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

[SOURCE: ISO/IEC 29100:2011, 2.9]

3.15
personally identifiable information controller
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information* (3.14) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others [e.g. *PII processors* (3.17)] to process PII on its behalf while the responsibility for the processing remains with the PII controller.

[SOURCE: ISO/IEC 29100:2011, 2.10]

3.16
personally identifiable information principal
PII principal
natural person to whom the *personally identifiable information* (3.14) relates

Note 1 to entry: Depending on the jurisdiction and the particular PII protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

[SOURCE: ISO/IEC 29100:2011, 2.11]

3.17
personally identifiable information processor
PII processor
privacy stakeholder that processes *personally identifiable information* (3.14) on behalf of and in accordance with the instructions of a *PII controller* (3.15)

[SOURCE: ISO/IEC 29100:2011, 2.12]

3.18
policy
intentions and direction of an *organization* (3.13) as formally expressed by its top management

[SOURCE: ISO/IEC 20547-3:2020, 3.11]

3.19
privacy breach
situation where *personally identifiable information* (3.14) is processed in violation of one or more relevant privacy safeguarding requirements

[SOURCE: ISO/IEC 29100:2011, 2.13]

3.21
privacy-by-design
approach in which privacy is considered at the initial design stage and throughout the complete lifecycle of products, processes or services that involve processing *personally identifiable information* (3.14)

3.22
privacy data sharing agreement
clauses for privacy protection in a data sharing agreement

Note 1 to entry: a privacy data sharing agreement can involve data transfer, data processing, and sharing of PII between joint *PII controllers* (3.15) (ISO/IEC 27701:2019 7.2.7)

3.20
privacy principles
set of shared values governing the privacy protection of *personally identifiable information* (3.14) when processed in information and communication technology systems

[SOURCE: ISO/IEC 29100:2011, 2.18]

3.23
privacy risk
effect of uncertainty on privacy

Note 1 to entry: Risk is defined as the "effect of uncertainty on objectives" in ISO Guide 73 and ISO 31000.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

[SOURCE: ISO/IEC 29100:2011, 2.19]

3.24
privacy rule
statement specifying what is allowed or not concerning privacy

3.25
process
set of interrelated or interacting activities which transforms inputs into outputs

[SOURCE: ISO/IEC 27000:2018, 3.54]

3.26
processing of PII
operation or set of operations performed upon *personally identifiable information* (3.14)

Note 1 to entry: Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII.

[SOURCE: ISO/IEC 29100:2011, 2.23]

3.27
smart city
effective integration of physical, digital and human systems in the built environment to deliver a sustainable, prosperous and inclusive future for its *citizens* (3.4)

[SOURCE: BSI PAS 181:2014]

3.28
smart city service governance body
body that acts as a supervisor for privacy recommendations or regulations concerning a *smart city* (3.27) service

3.29
supply chain
network of *organizations* (3.13) that are involved, through upstream and downstream linkages, in the *processes* (3.25) and activities that produce value in the form of products and services in the hands of the ultimate consumer

[SOURCE: ISO/TS 22318:2015, 3.3.5]

3.30
supplier
organization (3.13) of an individual that enters into an agreement with the acquirer for the supply of a product of services

Note 1 to entry: Other terms commonly used for supplier are contractor, producer, seller or vendor.

Note 2 to entry: The acquirer and the supplier sometimes are part of the same organization.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.45]

3.31
system of systems
large system that delivers unique capabilities, formed by integrating independently useful systems

[SOURCE: ISO/IEC/IEEE 24765:2017, 2]

3.32
task
required, recommended, or permissible action, intended to contribute to the achievement of one or more outcomes of a *process* (3.25)

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.50]

3.33
third party
privacy stakeholder other than the *personally identifiable information principal*, the *PII controller* (3.15) and the *PII processor* (3.17), and the natural persons who are authorized to process the data under the direct authority of the PII controller or the PII processor

[SOURCE: ISO/IEC 29100:2011, 2.27]

3.34
transparency
ability to ensure that all privacy-relevant data processing including the legal, technical and organizational setting can be understood and reconstructed

Note 1 to entry: This includes making information on PII processing available to *PII principals* (3.15).

[SOURCE: ISO/IEC TR 27550:2019, 3.24, modified — Note 1 to entry has been added.]

3.35
unlinkability
ability to ensure that a *PII principal* (3.15) may make multiple uses of resources or services without others being able to link these uses together

[SOURCE: ISO/IEC TR 27550:2019, 3.25]

3.36
work product
artifact associated with the execution of a *process* (3.25)

[SOURCE: ISO/IEC/IEEE 42020:2019, 3.26]

4 Abbreviated terms

AI	artificial intelligence
ICT	information and communication technology
IoT	internet of things
LINDDUN	linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness, non-compliance
OASIS	organization for the advancement of structured information standards
PIA	privacy impact assessment
STRIDE	spoofing of user identity, tampering, repudiation, information disclosure, denial of service, elevation of privilege

5 Privacy in smart cities

5.1 General

A smart city aims at the effective integration of physical, digital and human systems in the built environment to deliver a sustainable, prosperous and inclusive future for its citizens. It is a shared vision among city stakeholders to achieve a number of desired outcomes: well-being, transparency, sustainability, economic development, efficiency and resilience, collaboration and innovation. In this vision, economic development and innovation leverage ICT technology (e.g. IoT, big data, AI, cloud computing), and require a system of systems view to enable the integration of sector-specific systems (e.g. energy, transport, health). The integration of privacy is a major concern. Guidance needs to be provided on how smart cities can follow the ISO/IEC 29100 principles:

— consent and choice;

— purpose legitimacy and specification;

— collection limitation;

— data minimization;

— use, retention and disclosure limitation;

— accuracy and quality;

— openness, transparency and access;

— accountability;

— information security; and

— privacy compliance.

5.2 Integration of privacy in the smart city reference framework

5.2.1 Smart city ICT reference framework in the ISO/IEC 30145 series

Figure 4 describes the smart city ICT reference framework in the ISO/IEC 30145 series. It consists of three frameworks:

— a business process framework which specifies the essential processes in the areas of governance, core business and support;

— a knowledge management framework which provides guidance on the modelling and management of knowledge for smart city business and operations; and

— an engineering management framework which provides a set of ICT layers for smart cities operation, i.e. the smart application layer, the data and service supporting layer, the communication and storage layer, the network communication layer and data acquisition layer.

The business process framework includes:

— governance processes, which focus on the establishment of policies, and the continuous monitoring of their proper implementation by governing bodies of a smart city, e.g. local public authorities; and

— core business and support processes, which focus on the running of business processes according to the smart city policies by smart city agencies or delegated business organizations.

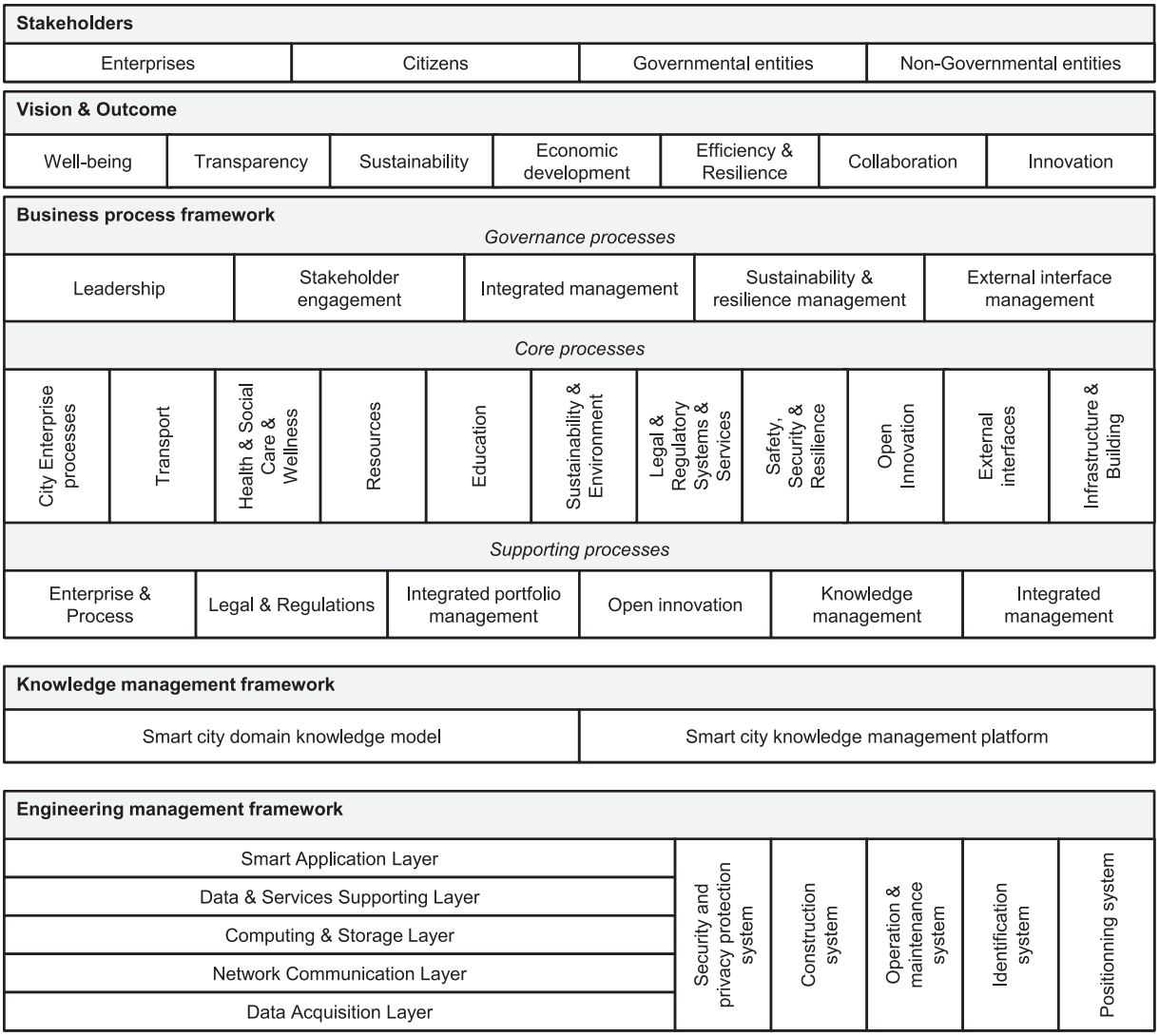

Figure 4 — Smart city ICT reference framework

The engineering management framework is described in Figure 5. This includes:

— the smart application layer focuses on domain applications, smart government, smart transportation, smart education, smart healthcare, smart home and smart campus which all rely on data processing;

— the data and services supporting layer focuses on data sources, data integration and service integration;

— the computing and storage layer focusses on computing, storage and software resources;

— the network communication layer provides communication infrastructure to smart cities with a high-capacity, high-bandwidth and high reliable optical networks and metropolitan wireless broadband network;

— the data acquisition layer provides the capability to sense the world and take actions; and

— vertical systems including the security and privacy protection system, the construction system, the operation and maintenance system, the identification system and the positioning system.

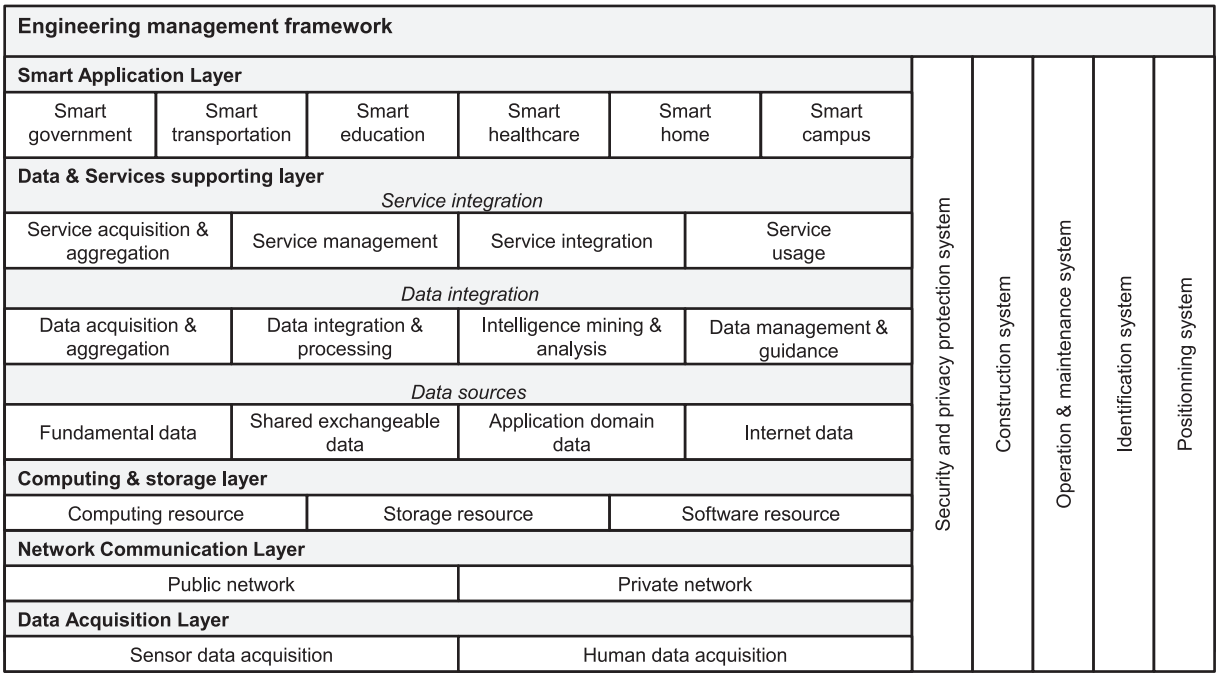

Figure 5 — Smart city engineering management framework

5.2.2 Privacy management activities in the ISO/IEC 30145 series

Processes of the smart city ICT reference framework can include privacy management activities:

— in the business process framework, processes can include additional activities related to PII:

  — the legal and regulatory systems and services process can deal with privacy regulation matters in order to ensure privacy compliance;

  — the safety, security and resilience process can deal with incidents causing privacy breaches;

  — the leadership and direction process can deal with governance of PII;

  — the stakeholder engagement and citizen focus process can deal with citizen queries concerning their PII;

— in the knowledge management framework, the knowledge base can include PII. For instance, knowledge about the provenance of data can provide links between PII principals and data:

— in the engineering management framework, all specified layers, i.e. the smart application layer, the data and services supporting layer, the computing and storage layer, the network communication layer, and the data acquisition layer can involve data leading to PII.

5.3 Actors

Depending on the viewpoints, specific actors should be considered in a smart city vision which leverages ICT technology (e.g. IoT, big data, AI), and which requires a system of systems view to enable the integration of sector-specific systems (e.g. energy, transport, health). Depending on the viewpoints (privacy, smart city, cloud computing, IoT, big data), specific actors should be considered in a smart city environment.

In activities related to privacy, the following actors are defined in ISO/IEC 29100:

— PII principals;

— PII controllers;

— PII processors; and

— third parties.

In activities related to data exchange and sharing for smart community infrastructures, the following roles are defined in ISO 37156:

— data creators, who create, capture, collect or transform data for e.g. a city or services;

— data owners who are the designated actors responsible for the data related to a city service. They define, validate each inherent attribute of the data;

— data custodians who are the custodians of a data for a specific purpose or task related to the provision of a service within the city;

— primary publishers who perform the publication for all data across the data spectrum;

— secondary publishers who create additional value from the city data that has been published; and

— users, e.g. city organizations, third sector organizations, business users, citizens, academic organizations or other cities.

In activities related to the cloud, the following actors are defined in ISO/IEC 17789:

— cloud service customers;

— cloud services partners; and

— cloud service providers.

The cloud service customer uses cloud services for the purpose of a business relationship. The cloud service provider makes cloud services available. The cloud service partner is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer.

In activities related to IoT, the following actors are defined in ISO/IEC 30141:

— IoT users;

— IoT service providers; and

— IoT service developers.

The role of IoT users is to administer and consume IoT services. The role of IoT service providers is to manage and operate IoT services. The role of IoT service developers is to implement, test and integrate IoT services.

In activities related to big data, the following actors are defined in ISO/IEC 20547-3:

— big data consumers;

— big data providers;

— big data application providers;

— big data framework providers; and

— big data service partners.

The role of big data consumers is to consume the value output of big data systems. The role of big data providers is to make data available. The role of big data application providers is to execute the manipulations of the data lifecycle. The role of big data framework providers is to provide a big data infrastructure, a big data platform, and big data processing. The role of big data service partners it to support big data application providers, big data providers and big data consumer.

	Individuals	Smart city governance bodies	Operators of business processes	Suppliers	Customers
Privacy ISO/IEC 29100	PII principal	PII controller	PII controller PII processor		Third parties
Smart city ISO/IEC 30145	Citizen	Agency	Primary and secondary publisher Data creator, owner, curator, custodian		Agency Business organisation
Cloud ISO/IEC 17789			Cloud service provider	Cloud service partner	Cloud service customer
IoT ISO/IEC 30141	IoT User	Agency Business organisation	IoT service provider	IoT service developer	IoT User
Big data ISO/IEC 20547	Big data consumer	Agency Business organisation	Big data provider Big data application provider Big data framework provider	Big data service partner	Big data consumer

Figure 6 — Stakeholders in smart cities and their relationship with those defined in other relevant standards

Figure 6 shows five categories of stakeholders: individuals, smart city governance bodies, operators of business processes, suppliers and customers. For each category, examples of actors and roles are provided, taking a privacy viewpoint (ISO/IEC 29100), a smart city viewpoint (ISO/IEC 30145 series), a cloud viewpoint (ISO/IEC 17789) an IoT viewpoint (ISO/IEC 30141) and a big data viewpoint (ISO/IEC 20547-3):

— individuals can be:

  — PII principals who are impacted by privacy breaches;

  — citizens belonging to or visiting a smart city;

  — cloud service customers;

  — IoT users of an IoT service; and

  — big data consumers;

— smart city governance bodies can be:

  — PII controllers who determine the purposes and means for processing of PII;

  — agencies who perform overall governance duties;

  — agencies or business organizations who perform governance duties on cloud services;

  - agencies or business organizations who perform governance duties on IoT services;
  - agencies or business organizations who perform governance duties on big data services;
- operators of business processes can be:
  - PII controllers or PII processors;
  - stakeholders involved in data exchange and sharing with roles such as primary and secondary publisher, data creator, owner, curator, custodian;
  - cloud service providers;
  - IoT service providers; and
  - big data providers, big data application providers or big data framework providers;
- suppliers can be:
  - network or infrastructure operators;
  - cloud service partners;
  - IoT service developers;
  - big data service partners; and
- customers can be:
  - citizens or third parties;
  - government organizations or agencies;
  - non-government organizations;
  - business organizations;
  - cloud service customers;
  - IoT users; and
  - big data consumers.

5.4 Challenges

Figure 7 illustrates integration problems in smart cities:

- IoT and big data are technology ecosystems which have to be integrated in the smart city ecosystem. Many smart cities applications are big data applications[1)]. Many smart cities ICT systems are IoT systems. As stated by Andrea Zanella,[29] the Iot has the capability "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";
- integration between different domains, such as smart grids, health, transport; and
- maintaining trust in services where the integration of multiple concerns such as security, privacy, safety and resilience is needed. For instance, the increasing combination of data points can raise the risk of creating PII.

1) For instance in Amsterdam (https://data.amsterdam.nl/), Berlin (https://daten.berlin.de/), London (https://data.london.gov.uk/) or Paris (https://opendata.paris.fr)

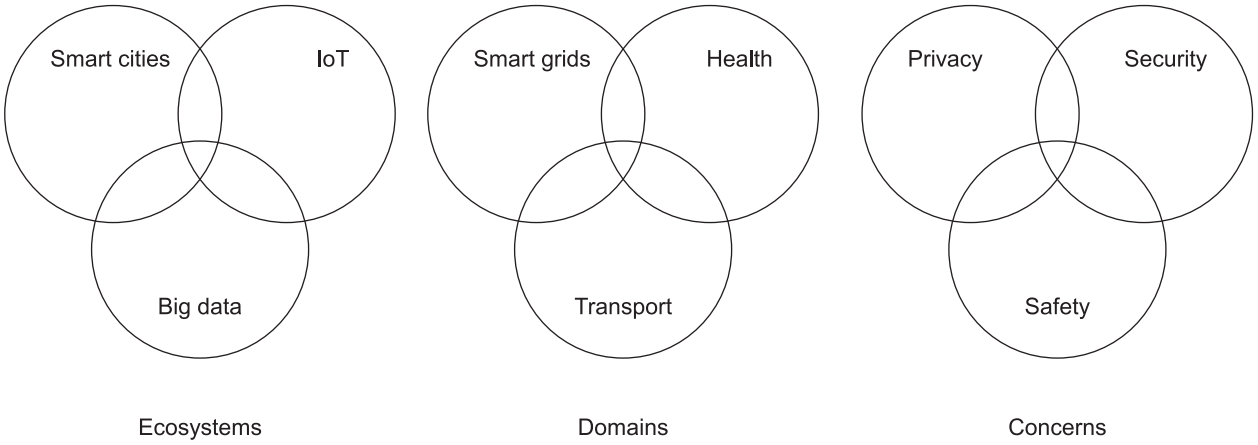

Figure 7 — Examples of ecosystems, domains and concerns

The need to integrate privacy has on impact on the following:

— the governance approach that is associated with concerns such as safety, security and privacy. For instance, a data protection authority might provide high-level rules (i.e. statement about what to do concerning privacy) and policies which, in turn, are used by smart city governance bodies to ensure specific compliance measures. These ensure proper rules and policies within the smart city ecosystem;

— the supply chain that is associated with the harvesting, collection, aggregation and transport of data in a smart city. For instance, data collected by a smart meter and further aggregated for data analysis involve a number of organizations (e.g. the manufacturer of a smart meter, the smart grid utility, the data analysts); and

— the data sharing ecosystem that is associated with data analysis in a smart city. For instance, multiple organizations can be involved in sharing energy data to improve its usage in different domains (e.g. transport, health, public infrastructures).

The following issues should be taken into account.

— In the governance approach, tracking the list of PII controllers and PII processors in order to address the accountability principle. For instance, the occurrence of a privacy incident can necessitate an action that impacts a specific stakeholder.

— In the supply chain, identifying how suppliers support privacy and communicating with them in order to enforce rules and policies. ICT technology includes a variety of products, end products such as sensors, devices, smart devices, cloud solutions or component products such as electronics, security modules, operating systems, middleware. Suppliers should provide appropriate privacy technical and organizational measures. For instance, a manufacturer of a storage system can include controls that would help PII controllers or PII processors.

— In the data sharing ecosystem, enforcing explicit privacy data sharing agreements when PII is processed and exchanged.

— The need to take into account individuals expectations including the right to be informed, to inform, correct, redress, restore and recover.

Table 2 shows examples of business vulnerabilities in smart cities.

Table 2 — Examples of business vulnerabilities in smart cities

Business aspect	Vulnerabilities
Governance	Smart city service governing body is not able to track all PII controllers or PII processors. For instance, it is not able to identify the PII controllers or PII processors that caused a breach.
	Smart city governing body has not defined clear rules and policies for privacy. It is not able to enforce privacy policies amongst PII controllers and PII processors.
Supply chain	Privacy impact assessments provided by suppliers are incomplete or inaccurate. For instance, they can be unaware of some privacy risks.
	PII controllers or PII processors rely on suppliers of components that do not support some desired privacy controls. For instance, a storage system does not include automated deletion capabilities.
Data sharing ecosystem	A stakeholder in the data sharing ecosystem is negligent on the enforcement of obligations. For instance, a stakeholder provides PII to another stakeholder without informing him about its obligations.
	Wrong assessment from a stakeholder that it is not a PII controller or PII processor. For instance, publishing open data that is not properly anonymized, or combining two datasets which do not contain PII into a dataset which contains PII.

6 Guidance on smart city ecosystems privacy protection

6.1 Ecosystem privacy plan

6.1.1 Recommendation R6.1

The smart city governance body should establish an ecosystem privacy plan.

6.1.2 Explanations

Figure 8 describes the relationships between organizations, processes and a smart city ICT reference framework as described in 5.1:

— an organization is a part of an ecosystem which follows the smart ICT reference framework;

— the smart ICT reference framework describes governance and integration processes as well as business and operation processes

— an organization implements processes that are related to roles, activities and functional components. For instance, an organization can be in charge of the big data application provider role; and

— an organization implements processes focusing on security and privacy. They are applied to protect assets in the smart city ICT reference frameworks against vulnerabilities. Some assets are specific to an organization, e.g. commercially sensitive information while others are shared within the ecosystems, e.g. open data. The organization can appoint a data protection officer in charge of ensuring, in an independent manner, compliance with the processes.

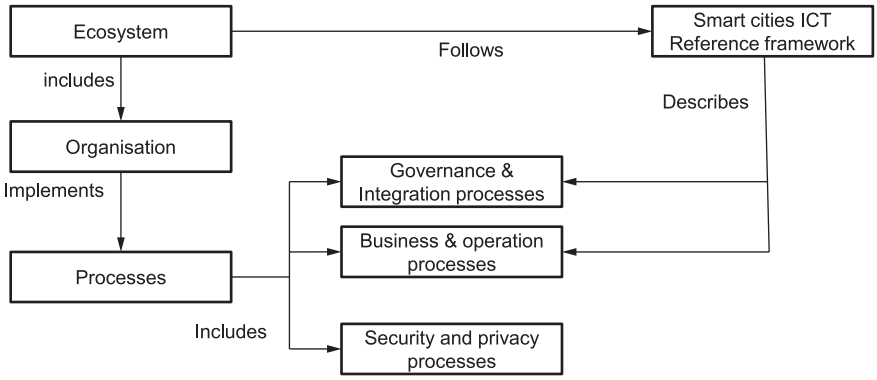

Figure 8 — Organizations in smart city ecosystems

There is a need to coordinate the processes of the organizations in a smart city ecosystem, as showed in Figure 9:

— an overall coordination by the smart city service governing body ensures consistency of each individual process; and

— each organization carries out its processes;

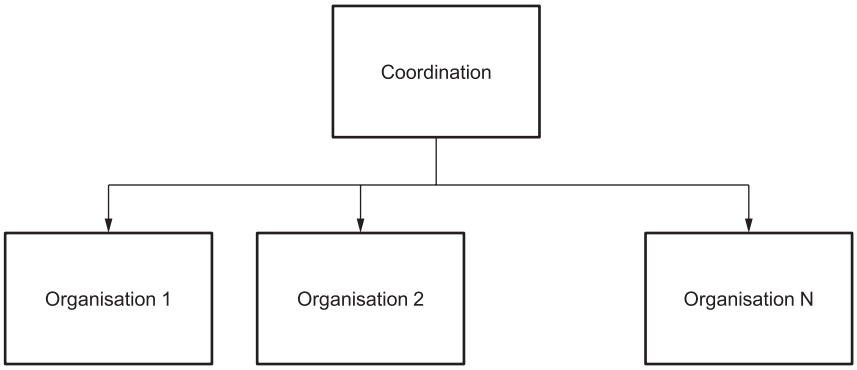

Figure 9 — Ecosystem coordination of organizations

6.1.3 Work product

The coordination is established through a smart city ecosystem privacy plan. Annex A provides an example of ecosystem privacy plan structure.

6.2 Governance

6.2.1 Recommendation R6.2

The ecosystem privacy plan should specify the governance body operation.

6.2.2 Explanations

The coordination of privacy in smart city ecosystems is managed by a governing body. The governing body can take different forms, e.g. a public authority, a dedicated organization, an alliance. They can be dedicated to specific domains. For instance:

— organizations involved in smart traffic management apply security and privacy processes that are coordinated by a city transport agency;

— organizations involved in healthcare big data apply security and privacy processes that are coordinated by a city health agency; and

— organizations involved in energy grid service apply security and privacy processes that are coordinated by an ad-hoc working group in coordination with a city energy grid agency.

The coordination can involve data protection officers from the governing body and from the organizations of the ecosystem.

6.2.3 Work product

The smart city ecosystem privacy plan describes the governance body and its rules and procedures.

6.3 Supply chain

6.3.1 Recommendation R6.3

The ecosystem privacy plan should include supply chain management.

6.3.2 Explanations

The supply chain management ensures that contractual arrangements on privacy are sufficient. It ensures the following:

— PII controllers and PII processors in the supply chain are aware of the privacy rules and policies in the smart city ecosystem;

— PII processors receive proper instruction by PII controllers (e.g. through privacy data sharing agreements); and

— suppliers to the PII controllers and PII processors take into account those privacy rules and policies. (transmitted, for example, through contractual requirements).

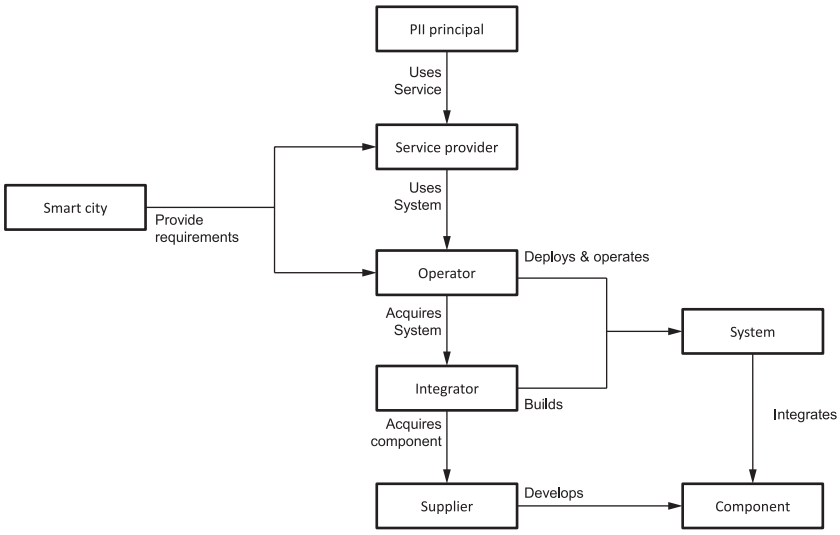

Figure 10 — Example of smart city supply chain

Figure 10 provides an example of supply chain for the creation of a system. It involves the following stakeholders:

— suppliers who provide the components making up a system, e.g. a sensor, a smart device, a cloud system;

— integrators who build the system, integrating the various components acquired from suppliers;

— operators who deploy, operate and maintain the system acquired from integrators;

— service providers who use the system to provide a service to end users;

— smart city authorities who provide requirements to application providers and operators concerning a service; and

— PII principals who use a service provided by the service provider.

Here is an example for a smart transport application providing real-time traffic advice to citizens. PII principals are the inhabitants of a city. The service provider is the city transport agency. The operator is a local SME associated with a major international cloud operator. The integrator is a very large company with experience in building complex systems. The suppliers are local producers of devices (e.g. a display system), an external start-up providing features for real-time advice, and a major operating system provider.

The supply chain is modified as showed in Figure 11 when privacy concerns are integrated:

— suppliers provide components that implement privacy controls that meet the requirements of the PII controllers and PII processors (e.g. de-identification techniques);

— integrators should provide the overall privacy controls integrating those provided by suppliers;

— PII controllers and PII processors carry out privacy management related operations (e.g. consent management, privacy breach management);

— data protection authorities and the smart city local authorities provide specific rules and policies to PII controllers and PII processors, for instance some specific privacy impact analysis guidelines;

— service providers get privacy guidelines from the data protection authorities;

— PII principals using the service are properly protected according to the rules and policies for privacy.

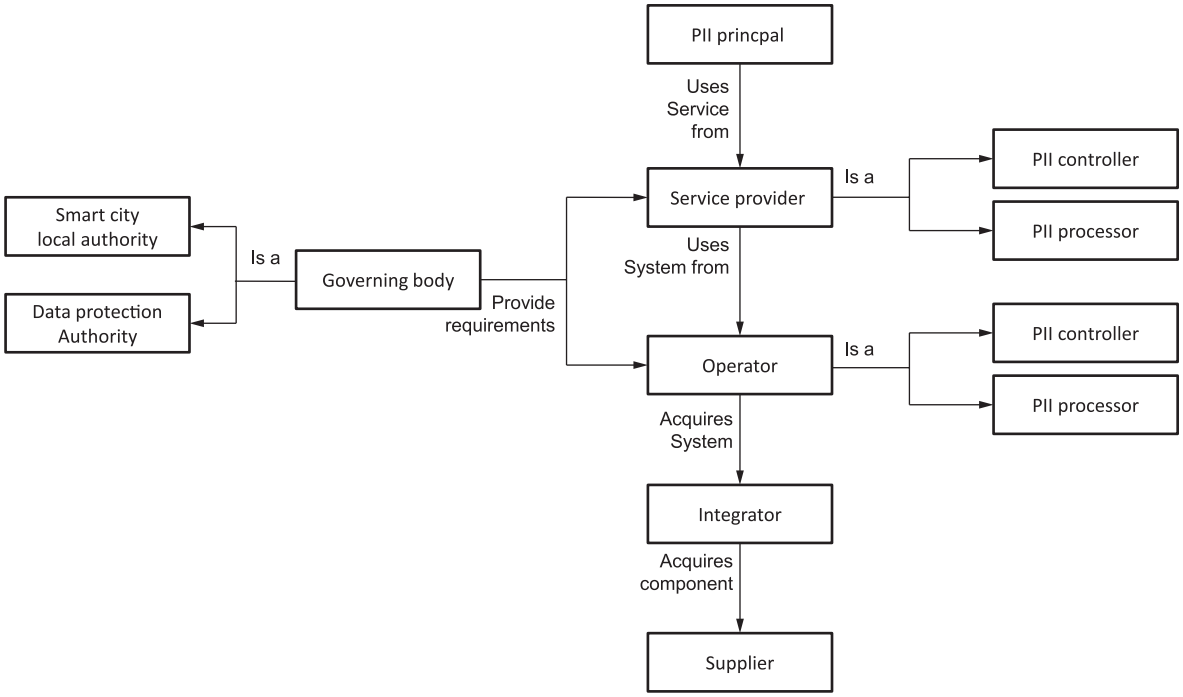

Figure 11 — Example of smart city supply chain integrating privacy

6.3.3 Work product

The smart city ecosystem privacy plan describes supply chain coordination.

6.4 Data management

6.4.1 Recommendation R6.4

The ecosystem privacy plan should include data management.

6.4.2 Explanations

Data processing stakeholders are further involved in a data sharing ecosystem. The integration of security and privacy in this value chain is depicted by Figure 12:

— two data processing stakeholders A and B negotiates a privacy data sharing agreement, where:

  — A is a PII controller and provides data to B which is a PII processor or a PII controller (scenario A); or

  — A and B are joint controllers (scenario B);

— the privacy data sharing agreement sets out obligations on data processing security and privacy capabilities provided by each stakeholder.

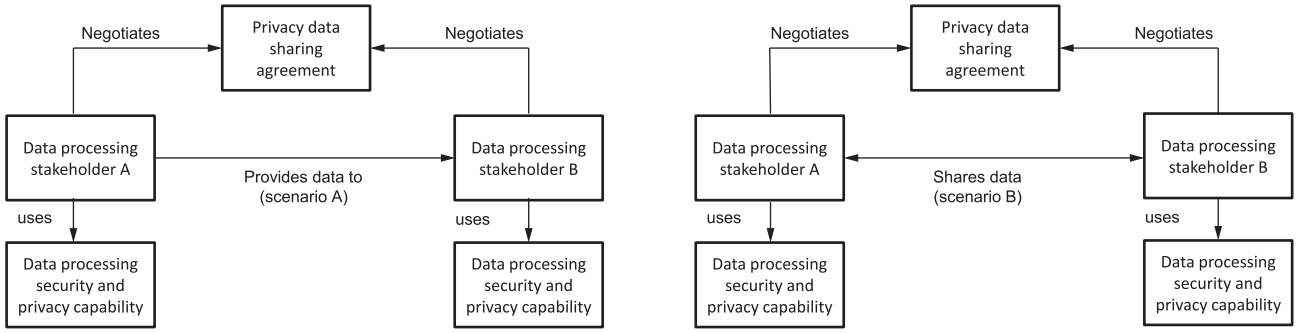

Figure 12 — Data sharing agreement from a security and privacy viewpoint

The coordination of privacy in data management ensures that:

— PII controllers and PII processors in the supply chain are aware of the privacy rules and policies in the smart city ecosystem;

— PII processors receive proper instruction by PII controllers (e.g. through privacy data sharing agreements);

— Suppliers to the PII controllers and PII processors take into account those privacy rules and policies; and

— if compliance verification is required by the governance process, determine the auditing stakeholders in charge of compliance.

For instance, an IoT system operator collects data that is provided as a dataset to a service provider which in turn combines it with other sources of data and provides it to a data consumer. As showed in Figure 13:

— an overall coordination of each organization's data management processes to ensure that they follow compatible privacy rules and policies; and

— each organization carries out its own data management process.

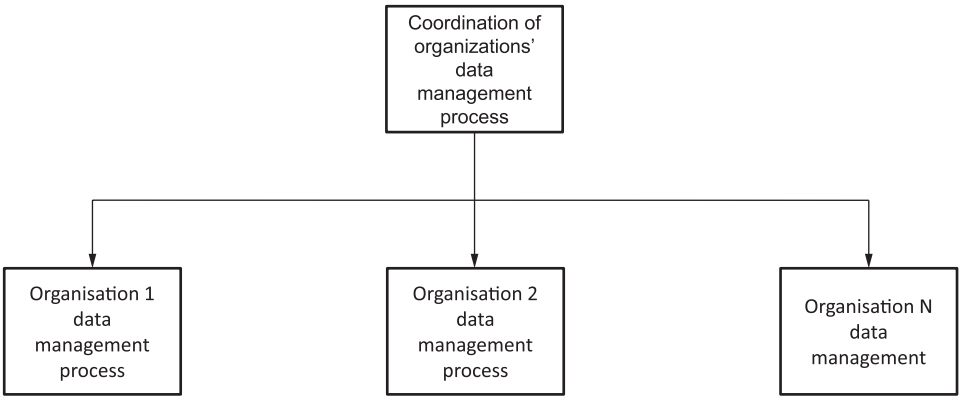

Figure 13 — Smart city management of data sharing ecosystem

6.4.3 Work product

The smart city ecosystem privacy plan describes data management coordination.

7 Guidance on standards for smart city ecosystems privacy protection

7.1 General

Figure 14 shows the various standards that can be used to guide organizations in the support of security and privacy. They cover the standards for:

— the governance process (8.2);

— the risk management process (8.4); and

— the engineering process (8.5).

NOTE These standards can be completed with further guidance documents (e.g. local standards).

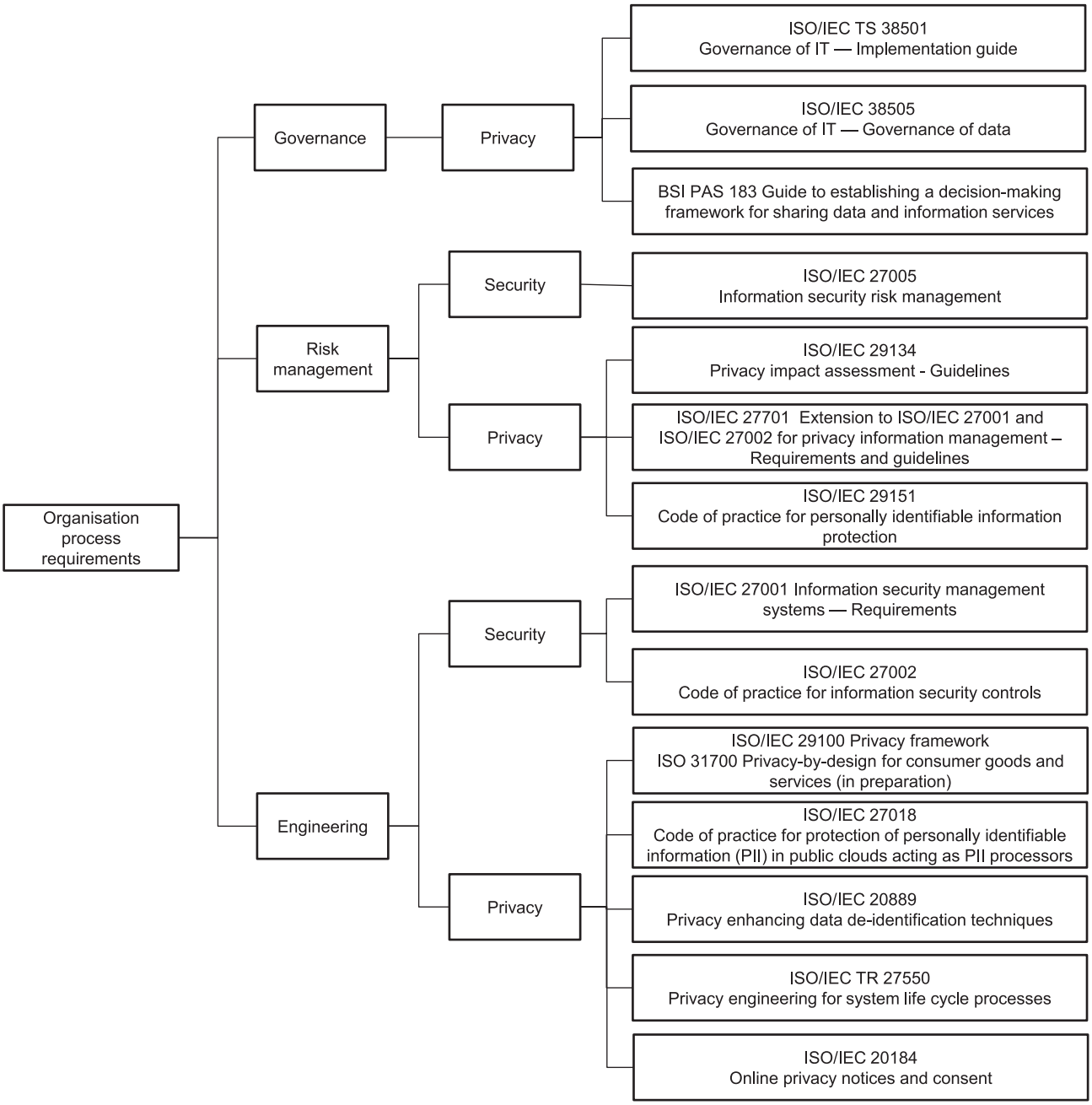

Figure 14 — Standards for organizations' privacy processes

7.2 Privacy governance

Smart city privacy processes dealing with governance can follow the following standards:

— implementation guide for IT governance as described in ISO/IEC TS 38501;

— IT governance for data as described in ISO/IEC 38505 (all parts);

— guide to establishing a decision-making framework for sharing data and information services as described in BSI PAS 183; and

— ecosystem coordination as described in this document.

7.3 Privacy risk management

Smart city privacy processes dealing with risk management can follow the following standards:

— information security risk management as described in ISO/IEC 27005;

— privacy impact assessment guidelines as described in ISO/IEC 29134;

— privacy requirements of smart city information systems as described in ISO/IEC 27701;

— code of practice for PII protection as described in ISO/IEC 29151; and

— ecosystem coordination as described in this document.

7.4 Privacy engineering

Smart city privacy processes dealing with engineering can follow the following lifecycle standards:

— security requirements of smart city information systems as described in ISO/IEC 27001;

— code of practice for information security controls as described in ISO/IEC 27002;

— privacy requirements of smart city systems resulting from the use of privacy principles as described in ISO/IEC 29100;

— code of practice for protection of PII in public clouds acting as PII processors as described in ISO/IEC 27018;

— privacy enhancing data de-identification techniques as described in ISO/IEC 20889;

— privacy engineering as described in ISO/IEC TR 27550;

— online privacy notices and consent as described in ISO/IEC 29184; and

— ecosystem coordination as described in this document.

8 Guidance on processes for smart city ecosystem privacy protection

8.1 General

This clause provides privacy guidelines for the creation, design, deployment and operation of a smart city service, focusing on the following processes:

— governance;

— data management;

— risk management;

— engineering; and

— citizen engagement.

Guidelines for each process are provided with the following content:

— a recommendation;

— an explanation of the activities at a global ecosystem level;

— guidelines for ecosystem coordination (carried out the smart city governance body);

— guidelines for organizations;

— standards and methods that can be used;

— examples; and

— the work product which describes the process.

8.2 Governance process

8.2.1 Recommendation R8.2

A governance process should be established by the smart city service governance body to ensure privacy management coordination of smart city ecosystems.

8.2.2 Explanations

The governance process focuses on the establishment of privacy policies, and the continuous monitoring of their proper implementation in a smart city service. These activities are carried out by the governing bodies of a smart city, as well as by the organizations in the ecosystem which implement the privacy policies, as shown in Figure 15.

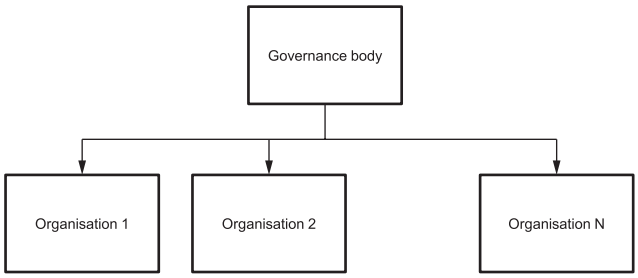

Figure 15 — Governance process stakeholders

8.2.3 Guidance on ecosystem coordination

The following guidance is provided at the ecosystem level:

— assess whether the creation of a smart city service requires specific privacy governance. In this case:

  — specify the rules and policies of the new privacy governance;

  — specify a privacy governance describing supervision requirements, and the resulting supervision activity;

  NOTE 1 Rules and policies includes guidelines for data retention policies between organizations sharing data.

— assess whether a privacy competence program (regulation, technical and organizational) should be implemented and include the outcome from the assessment in the governance, risk management, data management, privacy engineering and citizen engagement processes.

  NOTE 2 An example of regulation in Europe is GDPR.

— identify the supervised organizations for privacy governance and their responsibilities (e.g. PII controllers, PII processors, integrators or suppliers);

— establish and implement a communication and supervision activity, ensure that rules and policies are well communicated to organizations and implemented and if appropriate interact with specific organizations in the ecosystem (e.g. citizen complaints, privacy breach incidents); and

— establish and implement appropriate procedures for the protection of citizens' rights and interact throughout the process with data protection authorities.

NOTE 3 The communication activity includes requirements on information exchanged, agreement on controls applied and auditing capabilities.

8.2.4 Guidance for organizations

The following guidance is provided at the organization level:

— request the creation of privacy governance to the smart city governance body or, if governance already exists, request participation to the governance process;

— participate in the competence program;

— participate in the communication and supervision activity:

— implement the measures that meet the rules and policies associated with the privacy governance and, if appropriate, interact with the governance bodies (e.g. citizen complaints, privacy breach incidents); and

— interact with the governance body to provide information required for supervision.

8.2.5 Standards and methods

The following standards and methods can be used:

— ISO/IEC 30145 series is used as an overall framework;

— ISO/IEC 38500 is used by the governing body to govern the use of IT through three tasks: evaluate, direct and monitor;

— ISO/IEC TS 38501 is used to support the implementation of the governance process, through a cycle of three activities: establish and sustain enabling environment, govern IT and continual review;

— ISO/IEC TR 38502 is used to build a governance framework. This includes the following: principles for good governance, strategies and policies for the use of IT, business planning for IT, management systems for IT, the organization's use of IT, accountabilities and risk management; and

— ISO/IEC 38505-1 and ISO/IEC TR 38505-2 are used to build a data specific governance.

EXAMPLE A smart city deploys sensors to collect weather data, traffic data or energy usage data. Two services, a smart traffic application and an energy resource management are implemented. The first service is operated directly by a city agency (A). The other service is operated by a private organization (B). The whole program includes an ecosystem of organizations (C, D, E) collecting, treating and analysing data. Some data contain PII, for instance data collected by sensors in vehicles. Consequently, the city establishes a governance process according to this document: it identifies a supervising agency (A), and supervised organizations: A and B are PII controllers, C, D are PII processors, and E is a supplier of sensors. City agency A implements a communication and supervision activity addressing agreements on data management. This includes rules for public information (e.g. documentations associated with sensors being installed in vehicles). It also includes rules and policies for data retention. The activity requires periodic annual meetings and reviews leading to continual improvement decisions. The meetings and reviews are organized by city agency A.

8.2.6 Work product

The ecosystem privacy plan describes the governance process.

8.3 Data management process

8.3.1 Recommendation R8.3

A data management process should be established by the smart city service governance body to ensure protection of PII.

8.3.2 Explanations

The data management process focuses on the management of privacy in the creating, capturing, collecting, transforming, publishing, accessing, transferring and archiving of data within a smart city service. Actors can be smart city agencies or businesses. These activities are carried out by the governing bodies of a smart city, as well as by the organizations in the ecosystem as showed in Figure 16. A prerequisite to this process is the synchronization with the governance, risk management and engineering processes.

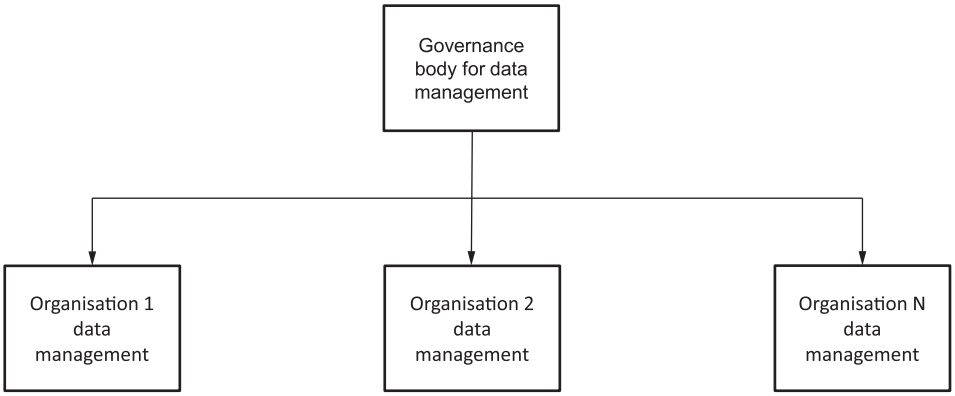

Figure 16 — Data management process stakeholders

8.3.3 Guidance on ecosystem coordination

The following guidance is provided at the ecosystem level:

— initiate the governance process and demonstrate that the data sharing purpose is compliant with policies and regulations;

— initiate the risk management process as required;

— initiate the engineering process as required;

— specify the privacy impact assessment and sharing agreement templates to use; and

— establish and implement coordination schemes in the ecosystem, concerning:

  — the participation of new organizations to a data sharing community;

  — the extension of data sharing to new applications:

  — the compliance of data sharing applications with agreed policies as well as regulation; and

  — assurance and audit of practice.

8.3.4 Guidance for organizations

The following guidance is provided at the organization level:

— initiate the governance process as required;

— initiate the risk management process as required;

— initiate the engineering process as required,

— use the privacy impact assessment and sharing agreement templates recommended at coordination level; and

— carry out data sharing activities in accordance with the ecosystem coordination scheme.

8.3.5 Standards and methods

The following standards and methods can be used:

— BSI PAS 183 is used to implement a transparent approach to making decisions and creating specific data sharing agreements;

— ISO 37156 provides a framework for data exchange and sharing to entities having authority to develop and operate community infrastructure; and

— ISO/IEC 29184 provides controls, which shape the content and the structure of online privacy notice as well as the process of asking consent to collect and process PII from PII principals.

EXAMPLE 1 A city agency operates an infrastructure to collect smart meters data in order to optimize its overall energy resources. Data is collected with the consent of the inhabitants for the purpose of energy study uniquely. The collected data is made available to a number of data analytics companies through a data sharing agreement which explicitly forbids organizations in the data sharing ecosystem to use the data for another purpose than energy study, and states that transmitted data is removed after analysis. The city agency establishes a data management process according to this document. This includes a reporting mechanism. Organizations in the data sharing ecosystem report annually providing information such as PIA annual report update, the list of processing carried out and the PII removal actions.

EXAMPLE 2 A private energy agency deploys a service for energy management optimization in an eco-district consisting of multiple smart buildings. Consent is provided by inhabitants for the collection and analysis of data provided by the various smart meters and HVAC devices installed in the buildings by different suppliers. The agency establishes a data management process according to this document. This includes a contractual agreement specifying the purpose for collecting and processing data signed by the stakeholders authorized to access data. Data management activities are deployed in accordance with the ecosystem coordination scheme. A new application provider wants to access to data in order to provide marketing services. As the new application does not comply with the smart city policy, it is not allowed to access collected data.

8.3.6 Work product

The smart city ecosystem privacy plan describes the data management process.

8.4 Risk management process

8.4.1 Recommendation R8.4

A risk management process should be established by the smart city service governance body to assess privacy impact.

8.4.2 Explanations

The risk management process deals with the analysis and the treatment of risks to the privacy on PII principals in a smart city service. The activities are carried out by the governing bodies of a smart city, as well as by the organizations in the ecosystem as showed in Figure 17. A prerequisite to this process is the synchronization with the governance process.

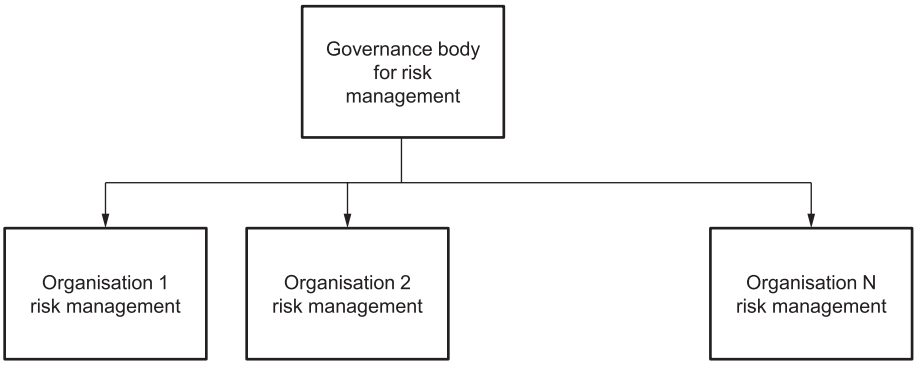

Figure 17 — Privacy risk management process stakeholders

8.4.3 Guidance for ecosystem coordination

The following guidance is provided at the ecosystem level:

— initiate the privacy governance process if it is not in place yet;

— establish and implement specific risk management coordination schemes in the ecosystem. This includes:

  — a mapping of the system of systems to the organizations of the ecosystem, and the specification of their roles in the risk management process;

  — the coordination of the risk management activities including the system of systems risk analysis and monitoring, compliance, assurance and audits of practice;

— establish and implement the risk management process of the smart city service viewed as a system of systems. This includes:

  — the identification of the vulnerabilities and threats to privacy in the system of systems;

  — the identification of the potential risks and breaches in the system of systems;

  — the evaluation of the potential impact to the PII principal;

  — the identification of controls to treat the risks of the system of systems;

  — the risk treatment implementations by the organizations of the ecosystem; and

  — the implementation of continual improvement and the related communications of improvements to the ecosystem.

NOTE 1 The system of systems risk management process is carried out under the responsibility of the smart city service PII controller who can be different from the organization in charge of ecosystem coordination.

NOTE 2 The risk assessment includes the identification of relevant legislation and contracts applicable.

8.4.4 Guidance for organizations

The following guidance is provided at the organization level:

— establish and implement a risk analysis process of the system(s) the organization is responsible for. The process includes:

  — the identification of the vulnerabilities and threats of the system(s) which the organization is responsible for;

- the identification of process owners, risks owners and individuals that are involved in the processing;
- the identification of the risks and breaches of the system(s);
- the evaluation of the potential impact to the PII principal;
- the identification of proposed controls to treat the risks of the system(s);
- the risk treatment implementations; and
- the implementation of continual improvement.

— establish and implement a risk management process in accordance with the specific ecosystem coordination schemes and the governance process described in 8.2. This can include the implementation of an information security and privacy risk impact assessment method.

NOTE 1 The information security and privacy risk impact assessment method includes the following steps: context establishment, risk assessment, risk treatment, risk acceptance, risk communication and consultation, risk monitoring and review.

NOTE 2 If the application of the risk assessment step provides sufficient information to effectively determine the actions required to modify the risks to an acceptable level, then the task is complete and the risk treatment follows. if the information is insufficient, another iteration of the risk assessment with revised context (e.g. risk evaluation criteria, risk acceptance criteria or impact criteria) is conducted, corresponding to the plan–do–check–act (PDCA) cycle.

8.4.5 Standards and methods

The following standards and methods should be used:

— ISO/IEC 29134 to support privacy risk analysis;

— ISO/IEC 27701 is used to support the identification activity of privacy controls to treat the risks of the system.

Classifications such as STRIDE or LINDDUN[27][28] can be used to support the activity of identifying threats.

EXAMPLE A smart city transportation agency deploys a service for intersection collision warning. The service is based on connected vehicles capabilities to broadcast at a high frequency cooperative awareness messages,[30] or information about their position, direction or speed. These messages are received by other vehicles as well by road side units deployed in intersections, analysed in real-time to detect case of potential collisions in order to trigger collision avoidance actions. There is a lapse of time when consecutive cooperative messages from the same vehicle are received. The vehicle cannot be tracked because messages are transmitted with pseudonyms. In order to ensure authentication of messages, all pseudonyms are signed sent with a public key certificate.[31] The ecosystem includes the following organizations: multiple operators of connected vehicle capabilities, multiple operators of road side units, multiple public key certificate providers and multiple operators of the service.

8.4.6 Work product

The smart city ecosystem privacy plan describes the risk management process.

8.5 Engineering process

8.5.1 Recommendation R8.5

An engineering process should be established by the smart city service governance body to take in consideration, whenever possible, a privacy-by-design approach.

8.5.2 Explanations

The engineering process is a set of activities related to the lifecycle of a smart city service. These activities are carried out by the governing bodies of a smart city, as well as by the organizations in the ecosystem concerned with the delivery, the use of the availability of a smart city service, as showed in Figure 18. A prerequisite to this process is the synchronization with the governance and the risk management processes.

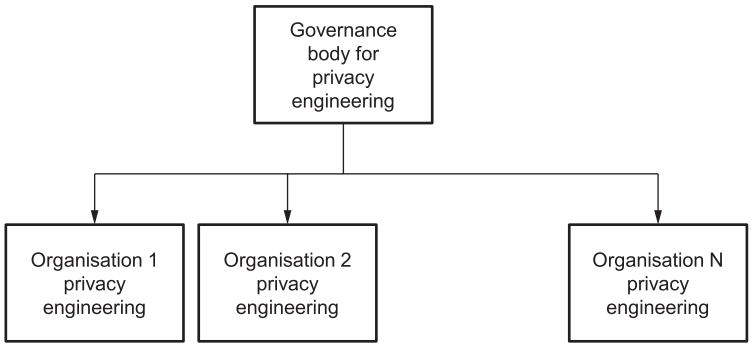

Figure 18 — Privacy engineering process stakeholders.

8.5.3 Guidance for ecosystem coordination

The following guidance is provided at the ecosystem level:

— initiate the privacy governance process if not in place;

— initiate the privacy risk management process if not in place;

— establish and implement specific privacy engineering coordination schemes in the ecosystem. This includes:

  — a mapping of the system of systems to the organizations of the ecosystem and the specification of their roles in the privacy engineering process;

  — the coordination of the privacy engineering lifecycle activities that will lead to the design of appropriate system of systems privacy controls; and

  — the coordination of the privacy engineering lifecycle activities related to assurance, compliance approach, or audit;

— establish and implement the privacy engineering process for the smart city service viewed as a system of systems. This includes:

  — a specification of the data model of the system of systems, focusing on data assets, data flows and processing of PII;

  — a risk management process of the system of systems as described in 8.4;

  — the activities in the privacy engineering systems of system lifecycle that will lead to the specification of privacy policies, conformance criteria, privacy technical requirements, privacy controls and privacy service and functions of the systems of system and their mapping to the organizations of the ecosystem;

  — the activities for continual improvement involving a periodic review of requirements and measures and their mapping to the organizations of the ecosystem.

NOTE 1 The activities in the privacy engineering process can include the resolution of conflict scenarios and the identification of resulting privacy policies. The goal in the engineering of a smart city product or service is to find a balance between the constraints and the needs of all the organizations and stakeholders, and the individual's privacy rights in the design phase, operational phase, maintenance phase, registration phase of the individuals (if any) and deregistration phase of the individuals (if any).

NOTE 2 PII processing related to data assets and data flows can include collection, retention/logging, generation/transformation, disclosure/transfer and/or disposal. Other terms used are data at rest, data in motion.

8.5.4 Guidance for organizations

The following guidance is provided at the organization level:

— establish and implement a privacy engineering process of the system(s) the organization is responsible for, including:

  — the specification of the data model;

  — the risk analysis;

  — the activities of the system(s) lifecycle;

  — and the definition of continual improvement;

— establish and implement a privacy engineering process in accordance with the specific ecosystem coordination schemes and the governance process described in 8.2, including the design phase, the usage phase, and the customer relationship management phase.

NOTE 1 The activities concerned by the customer relationship management (CRM) can include the acquisition of a product and/or the subscription to a service, the delivery of a product or a service, the support, service, maintenance and assistance for a product or a service, the marketing of the evolutions of the product or of the service or news related to the products or the services, and the recycling or disposal of a product or de-registration to a service.

NOTE 2 Smart city services are often added on top of other existing services. In such a case, privacy-by-design takes into account that existing infrastructure.

8.5.5 Standards and methods

ISO/IEC 29100 should be used.

It provides the principles to apply: consent and choice; purpose legitimacy and specification; collection limitation; data minimization; use, retention and disclosure limitation; accuracy and quality; openness, transparency and access; accountability; information security; and privacy compliance.

The following standards and methods can be used:

— the model and methodology provided by OASIS PMRM[32] is used to support the system of systems privacy engineering process. It is used to describe data assets and data flows and provide a picture of all domains, systems, and processes in which PII is used; to specify privacy policies and conformance criteria; to conduct a privacy analysis leading to the identification of requirement; to specify the privacy controls associated with PII, including internal privacy controls created within the domain/sub domain, but also privacy controls inherited and exported to/from other domains/subdomains; and finally to define privacy services and functions to be implemented in technical privacy mechanisms for data chains within an ecosystem;

— ISO/IEC TR 27550 is used to support the system of systems privacy engineering process. It identifies security and privacy properties that are used in the process such as confidentiality, integrity, availability, unlinkability, transparency or intervenability. It identifies privacy engineering design properties that are used in the process: data-oriented strategies (minimize, separate, abstract, hide) and process oriented strategies (inform, control, enforce, demonstrate);

— ISO/IEC 27701 is used to support the identification activity of privacy controls to treat the risks of the system; and

— ISO/IEC 20889 is used to specify terminology, a classification of de-identification techniques according to their characteristics and their applicability for reducing the risk of re-identification.

EXAMPLE A smart city deploys a smart city service to collect a variety of environment data such as weather conditions or road maintenance status. It takes advantage of the existence of an open ecosystem for provisioning vehicle data where citizens install a data collecting capability on their vehicles and trade collected data through personal data vaults: diagnosis data are provided to car manufacturers, meteorological data are provided to a local weather forecast organization and road conditions data are provided to the road maintenance organization. [33] The ecosystem includes the following organizations: multiple personal data vaults service providers, market place operators, global and local service providers. The city establishes an overall coordination scheme covering governance, risk management, data sharing, privacy engineering and citizen engagement according to this document. The ecosystem privacy engineering process includes the periodic assessment of privacy principles for minimizing data transfer from personal data vaults to service providers. The privacy engineering coordination involves the personal data vaults service providers, the market place operators, and the service providers, it identifies the suitability to switch to a new de-identification technique, synchronizing with the privacy engineering activities of each organization.

8.5.6 Work product

The smart city ecosystem privacy plan describes the engineering process.

8.6 Citizen engagement process

8.6.1 Recommendation R8.6

A citizen engagement process that integrates privacy should be established by the smart city service governance body.

8.6.2 Explanations

The citizen engagement process focuses on consultation with smart city citizens on rules and policies at governance level, and on the support on the enforcement of these rules and policies concerning the privacy of a smart city service. These activities are carried out by the governing bodies of a smart city, as well as by the organizations in the ecosystem as showed in Figure 19.

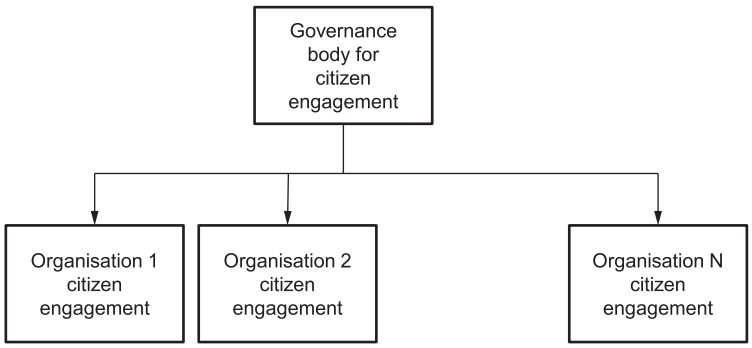

Figure 19 — Privacy citizen engagement process stakeholders

8.6.3 Guidance for ecosystem coordination

The following guidance is provided at the ecosystem level:

— establish a citizen dialogue and co-decision process for the establishment of smart city rules and policies for privacy, in accordance with the governance process described in 8.2. Examples of topics

are smart city policies for consent notice or transparency of information on smart city services PII processing;

— establish a citizen interaction activity, including for instance information events, enquiries and complaints;

— for each service to be deployed, determine whether a citizen consultation is needed that will review service purpose, ethics and privacy;

— for each service to be deployed, foster the creation of enablers to facilitate citizens engagement (e.g. privacy apps);

— carry out periodic citizen review of services and provide recommendations for amendment when appropriate;

— carry out periodic citizen review of the smart city rules and policies;

— establish citizen dialogue and co-decision requirements that organizations of the ecosystem should meet; and

— establish coordination schemes in the ecosystem for organizations that have citizen concertation requirements.

NOTE The activities in the citizen engagement process can include conflict scenarios resolutions which are addressed when defining privacy policies.

8.6.4 Guidance for organizations

The following guidance is provided at the organization level:

— identify whether citizen dialogue and co-decision requirements should be met by the organization;

— if appropriate, implement citizen dialogue and co-decision requirements;

— if appropriate, participate in periodic citizen review of services; and

— implement amendments.

EXAMPLE 1 A smart city develops a smart city service that aims at recommending citizens and visitors where to go at what time, based on different data sources including weather, traffic but also personal profiles (e.g. demographical data, consumption patterns, location history). Because processing PII will make the recommendations better, and to avoid bad publicity, they decide to engage with citizens to understand their privacy concerns and to establish appropriate privacy policies in a citizen engagement process, which is instigated from the very beginning of the development process. This allows the city and citizens to understand and integrate privacy concerns and service needs, and to assess what they are willing to share in order to get what in return. Essential parts of the dialogue process are frequent reports established in the coordination scheme, which foster transparency, keep the public up to date, manage expectations and create trust.

This attention on the project also led to review policies for consent, and approaches for data minimization. The outcome of the review of consent policies is twofold. First, a decision to provide a higher score to services where the PII controller is part of the ecosystem coordination scheme. Second, the recommendation that in public spaces in cities consent is, in many cases, not the right legal ground for processing. Regarding data minimisation approaches, the most important outcome was that any data collection needs to be tightly linked to clear and specific purposes defined a priori.

EXAMPLE 2 A smart city installs video cameras with the objective of identifying vehicle license plates to enable automated tool collection. Consent is not given by the individuals but by the governance of the city. A citizen engagement process is applied in order to agree on the procedures for informing individuals on the treatments that are made, and on the modalities for periodic audit of the system video cameras operation. Annex B provides further considerations on the use of video cameras in smart cities.

8.6.5 Work product

The smart city ecosystem privacy plan describes the citizen engagement process.

Annex A
(informative)

Example of ecosystem privacy plan structure

Table A.1 provides an example of an ecosystem privacy plan structure.

Table A.1 — Example of an ecosystem privacy plan structure

Section	Subsection	Description or content
Identification	Smart city name	Unique name of smart city ecosystem
	Responsibility	Name and signature of person responsible for ecosystem privacy plan
	History	Lists the reviews and evolutions of the privacy plan. Also includes a calendar for update plans.
	Confidentiality	Express the confidentiality of the plan, or of some of its section. Plan is structured so that there are sections that are public, and others that confidential but accessible for control by identified stakeholders.
	Information repository	URL to repository of information on smart city ecosystem. Can include a public part, as well as a private part.
Description of smart city service	General service description	Description of the service Description of the operational environment of the service (stakeholders, systems) Description of applicable laws and regulation, description of application standards
	General ecosystem description	Description of business chains (governance, supply chain, data management)
	Stakeholders	List of organizations in ecosystems and roles
Description of smart city ecosystem	Governance body	Description of governance scheme and objectives, description of governance body Description of rules and procedures: nomination of members of the governance body, operations Members of the governance body
	Supply chain management	Description of supply chain Description of management objectives Description of coordination procedures, information exchanged, access rights and monitoring approach Identification of stakeholders in supply chain that have an influence on privacy (e.g. PII controllers and processors, suppliers of privacy controls)
	Data management	Description of data flow in ecosystem Description of management objectives Description of coordination procedures, information exchanged and monitoring approach Identification of stakeholders in data sharing ecosystem that have an influence on privacy (e.g. PII controllers and processors)

Table A.1 *(continued)*

Section	Subsection	Description or content
Privacy management plan	Governance process	Description of how the governance process (8.2) is applied and reassessed for continual improvement Rules and policies for privacy governance Supervision requirements and activity Competence program Communication and supervision activity, dashboard requirements Procedures for the protection of citizens' rights Interaction activity with data protection authorities
	Data management process	Description of how the data management process (8.3) is applied and reassessed for continual improvement Privacy impact assessment templates, sharing agreement templates, standards to be used Coordination of data management in ecosystem and dashboard operation Measures for compliance assurance and audit of practice
	Risk management process	Description of how the risk management process (8.4) is applied and reassessed for continual improvement Practices to be applied, standards to be used Coordination of risk management in ecosystem and dashboard operation Measures for compliance assurance and audit of practice
	Engineering process	Description of how the engineering process (8.5) is applied and reassessed for continual improvement Practices to be applied, standards to be used Coordination of privacy engineering lifecycle activities in ecosystem and dashboard operation Measures for compliance assurance and audit of practice
	Citizen engagement process	Description of how the citizen engagement process (8.6) is applied and reassessed for continual improvement Practices to be applied, standards to be used Coordination of citizen engagement activities in ecosystem and dashboard operation (e.g. on co-decisions) Measures for compliance assurance and audit of practice

Annex B
(informative)

Using video cameras in smart cities

B.1 Data flow treatment of video cameras

Video cameras are sensors that transmit video data and optionally sound data. Video data can be in transmitted in the visible spectrum and/or in the infra-red spectrum. They can then be analysed, aggregated with other data and used in order to extrapolate information.

Cities or its stakeholders can be interested in using this information for multiple objectives like traffic management, energy reduction or crime detection. For instance, information about accidents and traffic jams can be used to alert the police or to reroute traffic.

The challenge is that cameras produce, as soon as they observe human activities, privacy sensitive information, the management of which is often covered by strict national or regional regulations.

Typically, installation and operation of a camera in areas open to the public is subject to an authorization for a designated purpose and the owner of the camera is also the owner of the data produced and as such liable on their usage.

The provisions below should accordingly be considered as generic. The implementer of smart city cameras should identify applicable regulations which, in some cases, can prohibit any camera sharing between applications.

B.2 Privacy concerns

Privacy concerns arise when collected data, possibly aggregated from multiple information sources can be used to identify an individual or to indirectly identify an individual, e.g. by collecting vehicle license plate numbers. Treatments made on raw video data can enable the recognition of individuals or/and vehicle license plate numbers. Further, captured images can be kept for unknown duration.

B.3 Intended purpose

The intended purpose of data collection and data aggregation should always be clearly identified. A balance between the advantages for the city or its stakeholders and the drawbacks for the citizens, if any, should be established. Once a proper balance has been agreed, the intended purpose should be advertised. These activities can be supported by the governance process (8.2), the risk management process (8.4) and the citizen engagement process (8.6) described in this document.

Further, the intended purpose of data collection and data aggregation should be established before a system is designed. In addition, accountability measures should be specified during the design phase to increase confidence that only the intended purpose is being addressed. These activities can be supported by the data management process (8.3) and the engineering process (8.5) described in this document.

B.4 Non-intended purposes

Raw data from video cameras is often transmitted to a data centre to perform a treatment corresponding to an intended purpose. But the data centre can also be in a position to perform non-intended treatments. Such additional treatments should be scrutinized. A balance between the advantages for

the city or its stakeholders and the drawbacks for the citizens, if any, should be established and proper balance should be agreed concerning:

— human beings (cameras can simply be used to count the number of people or to identify the citizen faces);

— vehicles (cameras can simply count the number of vehicles or track their owners and count the number of people sitting in the front seats); or

— areas (cameras can simply be used to monitor air pollution or to record the movement of vehicles and people in case an incident happens in an area).

One problem is to get confidence that the specific purpose for which cameras were initially installed is not diverted later to another purpose that has not been disclosed (and approved).

B.5 Unlawfully data sharing with third parties

Treatments that can be made of video captures are usually under the responsibility of the city or of the police of the city. When smart city technology is outsourced to private corporations, there are risks that PII can be unlawfully shared with third parties. Some of the equipment provided to achieve the intended purpose can contain backdoors which can be activated during a software update. If the data flows that are used correspond to published data flows, then they can be analysed and even filtered to make sure that they only transmit the intended data. Otherwise, full confidence needs to be placed in the equipment manufacturer.

B.6 User consent

User consent is one of the major privacy principles. However, in the case of video cameras, individual user consent is not possible. Consent is not given directly by individuals but by the governance of the cities or of the governments of the countries where the cameras are installed. It is generally recommended that individuals who think that their image has been recorded be given access and possibility to get the relevant data masked or erased. Some consumer groups can be invited through the citizen engagement process (8.6) to appreciate the balance between the benefits for the city or its stakeholders and the drawbacks for the individuals. Measures for informing individuals on the treatments that are made by these cameras should be implemented.

Bibliography

[1] ISO/IEC 17788:2014, *Information technology — Cloud computing — Overview and vocabulary*

[2] ISO/IEC 17789:2014, *Information technology — Cloud computing — Reference architecture*

[3] ISO/IEC 20889:2018, *Privacy enhancing data de-identification terminology and classification of techniques*

[4] ISO/IEC 20547-3, *Information technology — Big data reference architecture — Part 3: Reference architecture*

[5] ISO/IEC 20547-4, *Information technology — Big data reference architecture — Part 4: Security and privacy*

[6] ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[7] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

[8] ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

[9] ISO/IEC 27018:2019, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[10] ISO/IEC TR 27550:2019, *Information technology — Security techniques — Privacy engineering for system life cycle processes*

[11] ISO/IEC 27701:2019, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

[12] ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

[13] ISO/IEC 29134:2017, *Information technology — Security techniques — Guidelines for privacy impact assessment*

[14] ISO/IEC 29151:2017, *Information technology — Security techniques — Code of practice for personally identifiable information protection*

[15] ISO/IEC 29184:2020, *Information technology — Online privacy notices and consent*

[16] ISO/IEC 29190:2015, *Information technology — Security techniques — Privacy capability assessment model*

[17] ISO/IEC 30141:2018, *Internet of Things (loT) — Reference Architecture*

[18] ISO/IEC 30145 (all parts), *Information technology — Smart City ICT reference framework*

[19] ISO/IEC 30182:2017, *Smart city concept model — Guidance for establishing a model for data interoperability*

[20] ISO 37156, *Smart community infrastructures — Guidelines on data exchange and sharing for smart community infrastructures*

[21] ISO/IEC 38500:2015, *Information technology — Governance of IT for the organization*

[22] ISO/IEC TS 38501:2015, *Information technology — Governance of IT — Implementation guide*

[23] ISO/IEC TR 38502:2017, *Information technology — Governance of IT — Framework and model*

[24] ISO/IEC 38505 (all parts), *Information technology — Governance of IT — Governance of data*

[25] BSI PAS 183:2017, *Smart cities — Guide to establishing a decision-making framework for sharing data and information services*

[26] ISO/IEC/IEEE 15288, *Systems and software engineering — System life cycle processes*

[27] The STRIDE threat model[2], https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[28] LINDDUN privacy threat analysis methodology, https://www.linddun.org/

[29] Zanella A., Bui N., Castellani A., Vangelista L., Zorzi M., IEEE Internet of Things for Smart Cities. IEEE Internet of things journal. Vol.1, N°1, February 2014. https://ieeexplore.ieee.org/document/6740844/

[30] Systems I.T., (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service. ETSI TS 102 637-2 V1.2.1 (2011-03), https://www.etsi.org/deliver/etsi_ts/102600_102699/10263702/01.02.01_60/ts_10263702v010201p.pdf

[31] Systems I.T., (ITS); Security; Pre-standardization study on pseudonym change management ETSI TR 103 415 V1.1.1 (2018-04), https://www.etsi.org/deliver/etsi_tr/103400_103499/103415/01.01.01_60/tr_103415v010101p.pdf

[32] Organization for the Advancement of Structured Information Standards (OASIS) *Privacy Management Reference Model and Methodology (PMRM),* Version 1.0. July 2013, updated May 2016. http://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.pdf

[33] Full prototype of cross-sectorial vehicle data services. AutoMat H2020 projects deliverable D5.3. January 2018. https://www.automat-project.eu/sites/default/files/automat/public/content-files/articles/AutoMat%20D5%203_Full%20Prototype%20of%20Cross-Sectorial%20Vehicle%20Data%20Services_final.pdf

2) The page states the following: "This documentation is archived and is not being maintained".

ICS 35.030

Price based on 37 pages