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/IEC 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **6**
5 Privacy in smart cities **6**
5.1 General 6
5.2 Integration of privacy in the smart city reference framework 6
5.2.1 Smart city ICT reference framework in the ISO/IEC 30145 series 6
5.2.2 Privacy management activities in the ISO/IEC 30145 series 8
5.3 Actors 9
5.4 Challenges 11
6 Guidance on smart city ecosystems privacy protection **13**
6.1 Ecosystem privacy plan 13
6.1.1 Recommendation R6.1 13
6.1.2 Explanations 13
6.1.3 Work product 14
6.2 Governance 14
6.2.1 Recommendation R6.2 14
6.2.2 Explanations 14
6.2.3 Work product 15
6.3 Supply chain 15
6.3.1 Recommendation R6.3 15
6.3.2 Explanations 15
6.3.3 Work product 17
6.4 Data management 17
6.4.1 Recommendation R6.4 17
6.4.2 Explanations 17
6.4.3 Work product 18
7 Guidance on standards for smart city ecosystems privacy protection **18**
7.1 General 18
7.2 Privacy governance 19
7.3 Privacy risk management 20
7.4 Privacy engineering 20
8 Guidance on processes for smart city ecosystem privacy protection **20**
8.1 General 20
8.2 Governance process 21
8.2.1 Recommendation R8.2 21
8.2.2 Explanations 21
8.2.3 Guidance on ecosystem coordination 21
8.2.4 Guidance for organizations 22
8.2.5 Standards and methods 22
8.2.6 Work product 22
8.3 Data management process 23
8.3.1 Recommendation R8.3 23
8.3.2 Explanations 23
8.3.3 Guidance on ecosystem coordination 23
8.3.4 Guidance for organizations 23
8.3.5 Standards and methods 24
8.3.6 Work product 24

© ISO/IEC 2021 – All rights reserved

8.4 Risk management process 24
8.4.1 Recommendation R8.4 24
8.4.2 Explanations 24
8.4.3 Guidance for ecosystem coordination 25
8.4.4 Guidance for organizations 25
8.4.5 Standards and methods 26
8.4.6 Work product 26
8.5 Engineering process 26
8.5.1 Recommendation R8.5 26
8.5.2 Explanations 27
8.5.3 Guidance for ecosystem coordination 27
8.5.4 Guidance for organizations 28
8.5.5 Standards and methods 28
8.5.6 Work product 29
8.6 Citizen engagement process 29
8.6.1 Recommendation R8.6 29
8.6.2 Explanations 29
8.6.3 Guidance for ecosystem coordination 29
8.6.4 Guidance for organizations 30
8.6.5 Work product 31
Annex A (informative) **Example of ecosystem privacy plan structure** **32**
Annex B (informative) **Using video cameras in smart cities** **34**
Bibliography **36**

 © ISO/IEC 2021 – All rights reserved

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.

© ISO/IEC 2021 – All rights reserved

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.

© ISO/IEC 2021 – All rights reserved

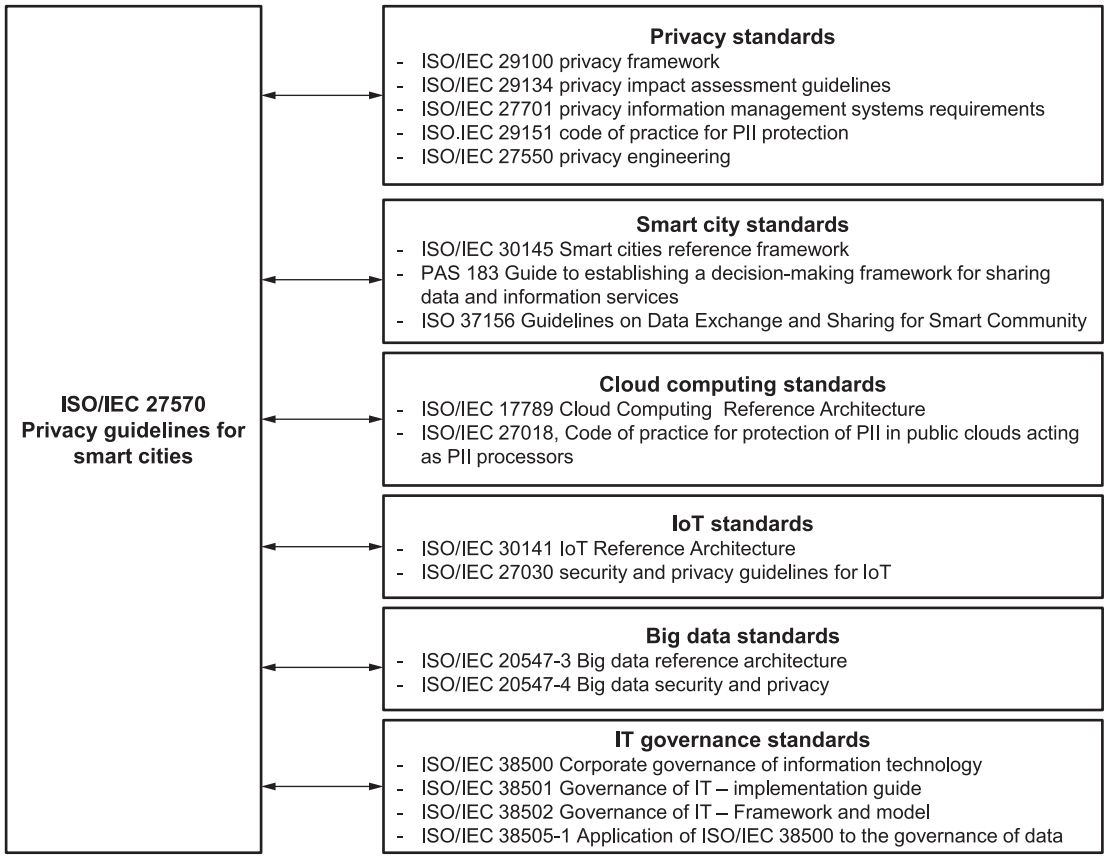


Figure 1 — Examples of standards to reference

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

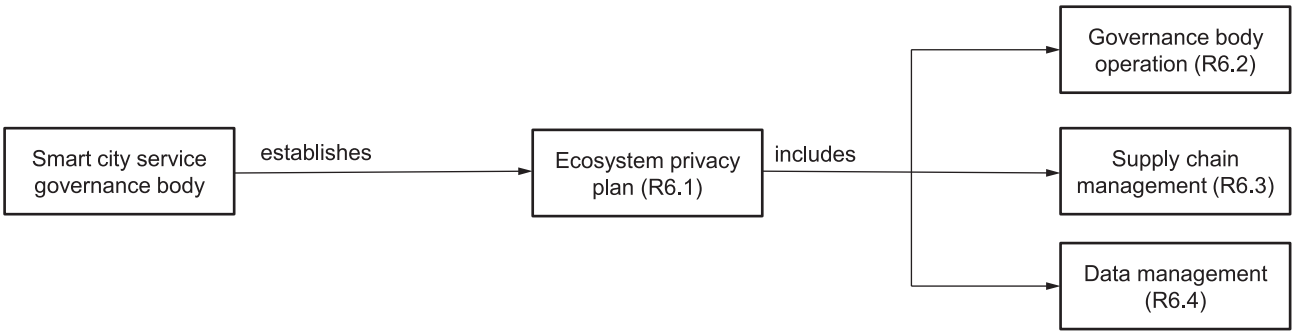


Figure 2 — Ecosystem guidance for privacy

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.

© ISO/IEC 2021 – All rights reserved

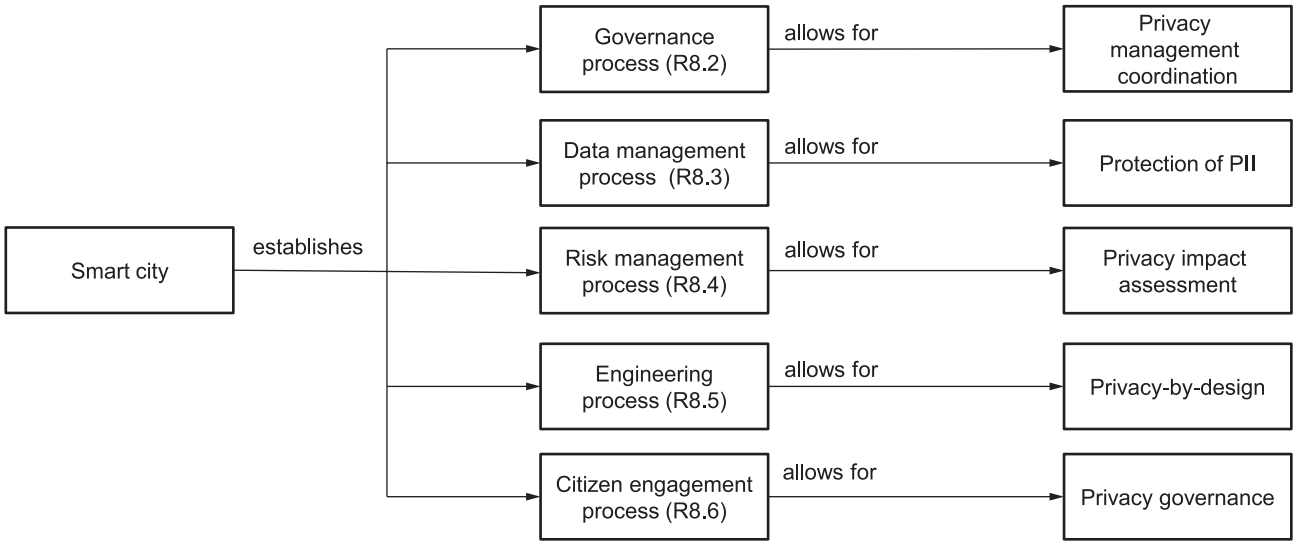


Figure 3 — Process guidance for privacy

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.

© ISO/IEC 2021 – All rights reserved

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

© ISO/IEC 2021 – All rights reserved

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.]

© ISO/IEC 2021 – All rights reserved

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)

© ISO/IEC 2021 – All rights reserved

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

© ISO/IEC 2021 – All rights reserved

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]

© ISO/IEC 2021 – All rights reserved