INTERNATIONAL STANDARD

ISO/IEC 27556

First edition
2022-10

Information security, cybersecurity and privacy protection — User-centric privacy preferences management framework

Sécurité de l'information, cybersécurité et protection de la vie privée — Cadre centré sur l'utilisateur pour le traitement des données à caractère personnel basé sur des préférences relatives au respect de la vie privée

Reference number
ISO/IEC 27556:2022(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 or www.iec.ch/members_experts/refdocs).

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 https://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. In the IEC, see www.iec.ch/understanding-standards.

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 and www.iec.ch/national-committees.

Introduction

This document describes a user-centric framework for handling personally identifiable information (PII), based on privacy preferences and privacy preference administration within information and communication technology (ICT) systems. ICT systems which handle PII implement privacy control mechanisms. To ensure these mechanisms are implemented effectively in ICT systems, PII is controlled using privacy preferences which are set (directly or indirectly) by the relevant PII principal, including consent information. When PII is processed based upon authorities other than consent, ICT systems can, where appropriate, incorporate mechanisms to improve transparency and adjust PII processing in accordance with the preferences of the PII principal. PII principals can make informed use of a system only when they understand the scope of its privacy implications, which is improved when the actionable privacy control options align in an intuitive way with PII processing undertaken in the ICT system.

Mechanisms that incorporate a PII principal's privacy preferences into machine-readable settings for each PII handling system can be useful. Moreover, such collected PII may be shared or transferred among other service providers according to the PII principal's preferences.

The framework is intended to help organizations include user-centric PII handling mechanisms in their systems following privacy-by-design principles and realize PII handling based on privacy preferences of PII principals. The framework includes components designed to manage privacy preference information, and sub-components that are implemented within that component are defined in this document. However, this document does not specify the content and format of privacy preference information.

This document can be used to:

— design and implement ICT systems that handle PII, or transfer PII between organizations;

— develop PII exchange platforms based on privacy preferences;

— provide privacy preference management services.

Information security, cybersecurity and privacy protection — User-centric privacy preferences management framework

1 Scope

This document provides a user-centric framework for handling personally identifiable information (PII), based on privacy preferences.

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 terminology databases for use in standardization at the following addresses:

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

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

3.1
personally identifiable information
PII
information that (a) can be used to identify the *PII principal* (3.2) to whom such information relates, or (b) is or may 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, modified — The word “any” has been removed, “might” has been replaced by “may”.]

3.2
PII principal
natural person to whom the *personally identifiable information* (3.1) relates

Note 1 to entry: Depending on the jurisdiction and the particular data 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]

3.3
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information* (3.1) other than natural persons who use data for personal purposes

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

Note 2 to entry: A *PII principal* (3.2) may sometimes be the "controller" of their own information where information and communication technology (ICT) systems are designed to enable direct control by the PII principal. In such cases the ICT system would be the PII processer responding to the PII controller who is also the PII subject.

[SOURCE: ISO/IEC 29100:2011, 2.10 — Note 2 to entry has been added.]

3.4
PII processor
privacy stakeholder that processes *personally identifiable information* (3.1) on behalf of and in accordance with the instructions of a *PII controller* (3.3)

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

3.5
third party
privacy stakeholder other than the *personally identifiable information (PII) principal* (3.2), the *PII controller* (3.3) and the *PII processor* (3.4), 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]

3.6
privacy stakeholder
natural or legal person, public authority, agency or any other body that can affect, be affected by, or perceive themselves to be affected by a decision or activity related to *personally identifiable information* (3.1) processing

[SOURCE: ISO/IEC 29100:2011, 2.22]

3.7
identifying attribute
attribute in a dataset that is able to contribute to uniquely identifying a *PII principal* (3.2) within a specific operational context

Note 1 to entry: ISO/IEC 20889:2018 uses a term "data principal" that is broader than "PII principal". However, this document focuses on data sets related to PII principals.

[SOURCE: ISO/IEC 20889:2018, 3.14, modified — The word "data principal" has been changed to "PII principal" and Note 1 to entry added.]

3.8
control
measure that is modifying risk

Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk.

Note 2 to entry: It is possible that controls do not always achieve the intended or assumed modifying effect.

[SOURCE: ISO Guide 73:2009, 3.8.1.1, modified — Note 2 to entry has been changed.]

3.9
data transformation
process which creates new data from an original source

EXAMPLE The process of migrating into a different format, or by creating a subset, by selection or query, to create newly derived results, such as for publication.

[SOURCE: ISO 5127:2017, 3.1.11.06]

3.10
de-identification technique
method for transforming a dataset with the objective of reducing the extent to which information is able to be associated with the *PII principal* (3.2)

Note 1 to entry: ISO/IEC 20889:2018 uses a term "data principal" that is broader than "PII principal". However, this document focuses on data sets related to PII principals.

[SOURCE: ISO/IEC 20889:2018, 3.7, modified — The word "data principal" has been changed to "PII principal" and Note 1 to entry added.]

3.11
re-identification
process of associating data in a de-identified data set with the *PII principal* (3.2)

Note 1 to entry: A process that establishes the presence of a particular data principal in a dataset is included in this definition.

Note 2 to entry: ISO/IEC 20889:2018 uses a term "data principal" that is broader than "PII principal. However, this document focuses on datasets related to PII principals.

[SOURCE: ISO/IEC 20889:2018, 3.31, modified — The word "data principal" has been changed to "PII principal" and Note 2 to entry added.]

3.12
redaction
removal of a field such that it results in the irreversible and permanent removal of information contained within that field from the message

Note 1 to entry: The removal of a field only removes the information contained within that field. Information that can be derived from other fields of the message or from other sources is not removed.

[SOURCE: ISO/IEC 23264-1:2021, 3.21]

3.13
unlinkability
property that ensures that a *PII principal* (3.2) 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]

3.14
intervenability
property that ensures that *PII principals* (3.2), *PII controllers* (3.3), *PII processors* (3.4) 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 may be limited by relevant legislation or regulation.

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

3.15
transparency
property that ensures that all privacy-relevant data processing including the legal, technical and organizational setting can be understood and reconstructed

[SOURCE: ISO/IEC TR 27550:2019, 3.24]

3.16
privacy preferences
specific choices made by a *personally identifiable information (PII) principal* (3.2) about how their *PII* (3.1) should be processed for a particular purpose

[SOURCE: ISO/IEC 29100:2011, 2.17]

3.17
privacy preference manager
PPM
component providing a capability allowing *PII principals* (3.2) to express *privacy preferences* (3.16) and a capability to monitor PII processing according to these privacy preferences

3.18
privacy preference administrator
PPA
privacy stakeholder which administrates a *privacy preference manager* (3.17)

4 Symbols and abbreviated terms

For the purposes of this document, the following abbreviations apply:

EHR electronic health record

ICT information and communications technology

PIA privacy impact assessment

PII personally identifiable information

PPA privacy preference administrator

PPM privacy preference manager

5 User-centric framework for handling PII

5.1 General

Privacy preference handling is the key enabler for the construction of a user-centric PII handling framework based on privacy preferences. As shown in Figure 1, such a framework can be used as a technical reference for developers of ICT systems that process PII. Use cases of PII handling based on privacy preferences are introduced in Annex A.

The framework consists of actors and components.

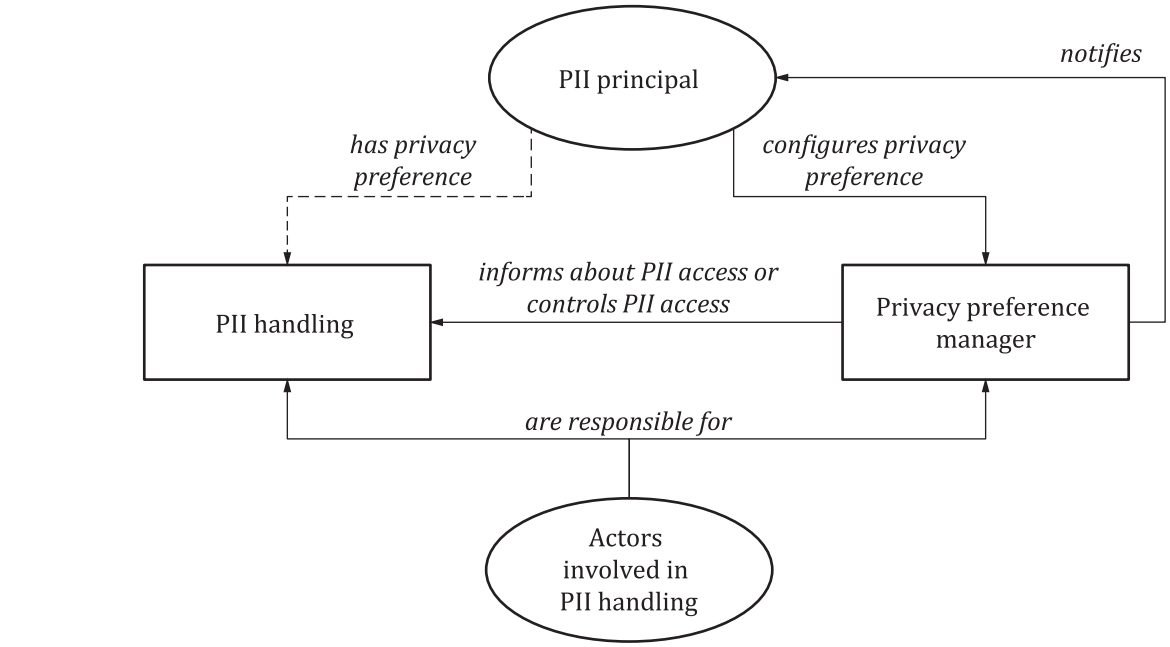

Figure 1 — User-centric framework for handling PII

The privacy preference manager (PPM) provides the following capabilities:

— the management of privacy preferences of PII principals;

— the management of privacy notices;

— the management of consent information where applicable;

— generation of information for handling PII processing in IT systems at a granularity level corresponding to the preferences;

— the implementation of control mechanisms to enforce these preferences during PII processing, including in the case of PII transfer.

As shown in Figure 1, the privacy preference manager acts as a proxy for the PII principal(s) in order to realize privacy preference-based handling. From the point of view of PII principals, PII should be processed appropriately by service providers (PII controllers or PII processors) based on the PII principal's privacy preferences. In this case, a PII principal should specify their privacy preferences, such as the type of PII that can be collected, how their PII shall and shall not be processed and with which entities, if any, their PII may be shared. In a complex service environment, the preference of PII principals for PII usage should be configured flexibly. To this end, privacy preference handling enables the following functionalities.

— PII principals can configure their PII privacy preferences. These preferences may include the list of PII that a PII principal allows to be collected, and the service providers that the PII principal allows to access the collected PII. A default setting of privacy preferences includes no PII list as a privacy by default setting.

— The delivery of PII to a service provider is controlled by the privacy preferences which are made by the PII principal in the context of a particular operation performed with that service provider.

— PII principals have access to a summary showing when their PII has been shared with other service providers.

NOTE A third party is a recipient of PII, and the third party becomes either PII controller, PII processor, or PII sub-processor once it has received the PII.

5.2 Actors

The actors in the user-centric PII handling framework are the following:

— the PII principals;

— PII controllers (including a third party);

— the PII processors;

— the privacy preference administrators (PPAs).

5.3 Roles of actors in user-centric PII handling frameworks

5.3.1 Roles of PII principals

PII principals give consent, where applicable, and determine their preferences for how their PII should be collected and processed, and provide the privacy preferences to the PPM.

NOTE Consent and preferences can be provided indirectly by an authorized third party, who gives consent and indicates privacy preferences on behalf of other PII principals. Examples of PII providers are employees that provide information on their family members to an employer, or a job applicant that provides a contact number of an ex-employer when applying for a new job.

5.3.2 Roles of PII controllers

A PII controller can, where appropriate:

— implement control mechanisms as required to protect the PII of the PII principal;

— process PII, respecting the preferences of the PII principal, e.g. as recorded in the PPM;

— implement mechanisms to allow the PII principal direct access and/or control to some or all of their own PII;

— decide to have all or part of the processing operations carried out by a different privacy stakeholder on its behalf (using a PII processor) where the PII principal has authorized this implicitly or explicitly, e.g. via a preference stored in the PPM;

— transfer PII to another controller. The PII principal's preferences, e.g. as reflected in the PPM, continue to be respected when the new controller processes the PII.

A PII controller should provide appropriate privacy notices to PII principals.

NOTE ISO/IEC 29184 provides guidance on the structure and content of privacy notices.

5.3.3 Roles of PII processors

A PII processor can:

— implement control mechanisms as required to protect the PII principal's PII, potentially including additional controls as required by the PII controller;

— process PII as instructed by the PII controller, respecting the PII principal's preferences, as recorded in the PPM.

5.3.4 Roles of privacy preference administrators

Privacy preference administrators (PPAs) are privacy stakeholders that administrate the PPM and handle its contents. The purpose is to inform the PII processors and PII controllers on their actions.

NOTE 1 The provision of information can take place in real time.

NOTE 2 The PPA is a controller and processor of privacy preferences. The PPA is a specific role in the organizational structure of a PII controller or a PII processor.

5.4 Components in the user-centric PII handling framework

5.4.1 Overview

Figure 2 shows the components in the user-centric PII handling framework that can have an influence on the privacy preference manager.

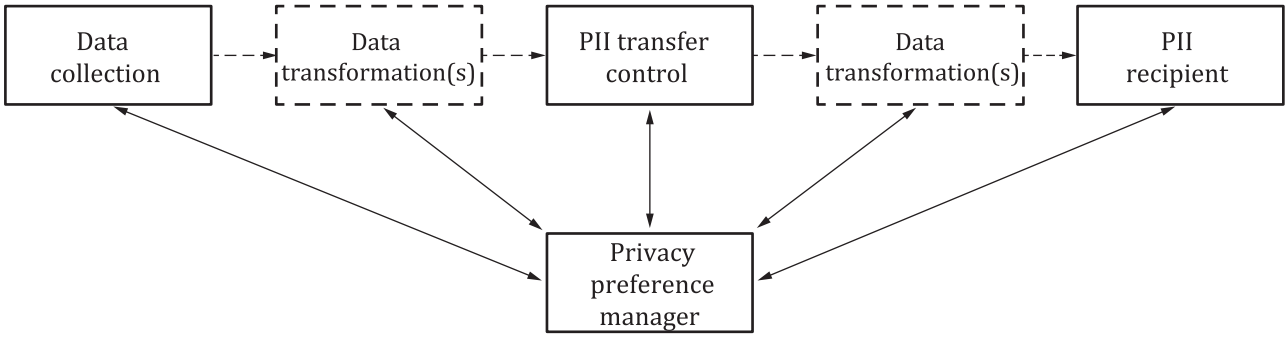

Figure 2 — Components in the user-centric PII handling framework

5.4.2 Data collection

The data collection component collects PII from data sources. Data sources are individuals, devices, databases, or systems that provide information including PII for data processing.

5.4.3 Data transformation(s)

The data transformation component provides an optional process. A typical example of a transformation applied to data are de-identification and redaction. PII may be de-identified before or after PII transfer control according to a privacy preference.

NOTE 1 An additional category of preference is de-identification policies. ISO/IEC 20889 specifies terminology, a classification of de-identification techniques according to their characteristics, and their applicability for reducing the risk of re-identification. These techniques include suppression, generalization, and randomization techniques. Data sets can undergo redaction before or after transfer, which can reduce identifying attributes.

NOTE 2 ISO/IEC 27038 specifies the redaction of digital documents.

NOTE 3 ISO/IEC 23264-1 specifies properties of cryptographic mechanisms to redact authentic data (i.e. data with associated attestations).

5.4.4 PII transfer control

The PII transfer control component handles PII transfer from data source(s) to PII recipient(s). The PII transfer control component involves the use of control mechanisms to enforce privacy preferences.

NOTE 1 ISO/IEC 27701 can be used as guidance on controls that can be used by PII controllers and PII processors.

NOTE 2 PII transfer is allowed only into controlled and authorized processors' systems.

5.4.5 PII recipient

The PII recipient component receives PII and executes operations according to the PII principal's privacy preferences.

5.4.6 Privacy preference manager

The privacy preference manager (PPM) component includes the following sub-components, as shown in Figure 3.

— Consent information administration: this sub-component is optional. It provides an interface for storing, updating and accessing consent information, and securely maintains the stored consent information (providing confidentiality, integrity and availability). A receipt of consent can be provided to PII principals based on the stored consent information. The consent information administration sub-component may also provide a mechanism for obtaining the consent of the PII principal.

— Privacy preference administration: this sub-component securely collects privacy preference information and provides a mechanism for input, modification and deletion of privacy preferences related to actions performed on a service provider. Privacy preferences should be configured so that all choices are disabled by default and it should be able to be updated or modified by the PII principals at any time. Annex C provides examples on the configuration of privacy preferences.

— Control rule generation: this sub-component provides data flow control rules to the PII transfer control component. Data flow control rules are generated according to consent information and privacy preferences chosen by PII principals. The rules are used for access control to PII by the PII transfer control component.

— Transparency administration: this sub-component provides for logging and log inspection; the logging involves logging PII transfer receipts and the associated transfer times. The log inspection allows each PII principal to check the logs, where appropriate, using the log inspection.

NOTE 1 The PPM, itself being operated by a data controller or processor, can maintain records of processing.

NOTE 2 This subcomponent can also include mechanisms for collecting, holding, and displaying consent and data use receipts.

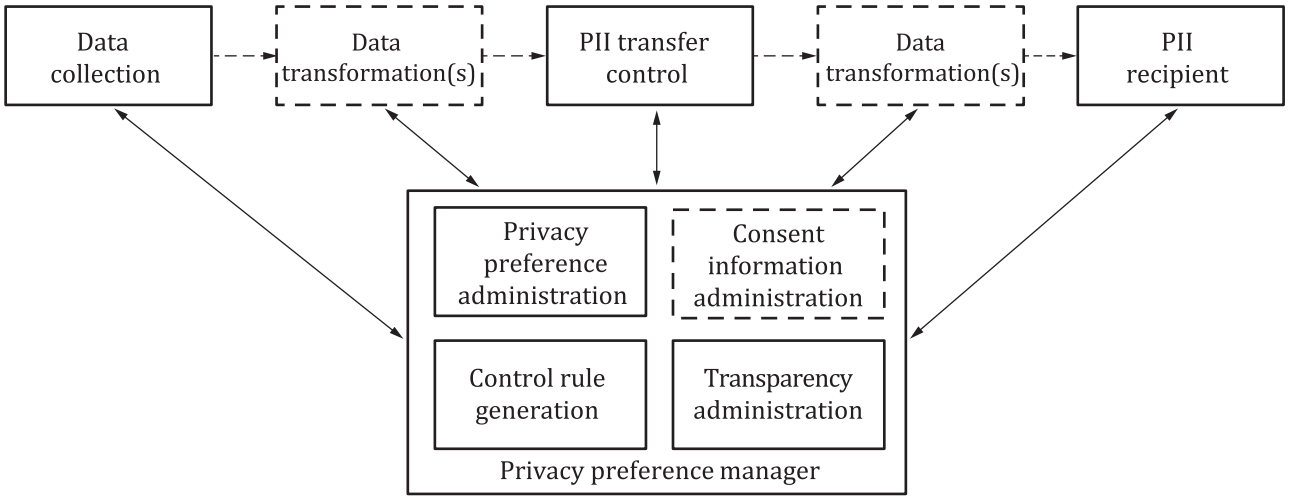

Figure 3 — Structure of the privacy preference manager

5.5 Relationship between actors and components

Figure 4 illustrates the relationships between the actors and the components:

— the PII principal interacts with the PPM;

— the privacy preference administrator operates the PPM;

— the PII controllers and PII processors handle PII.

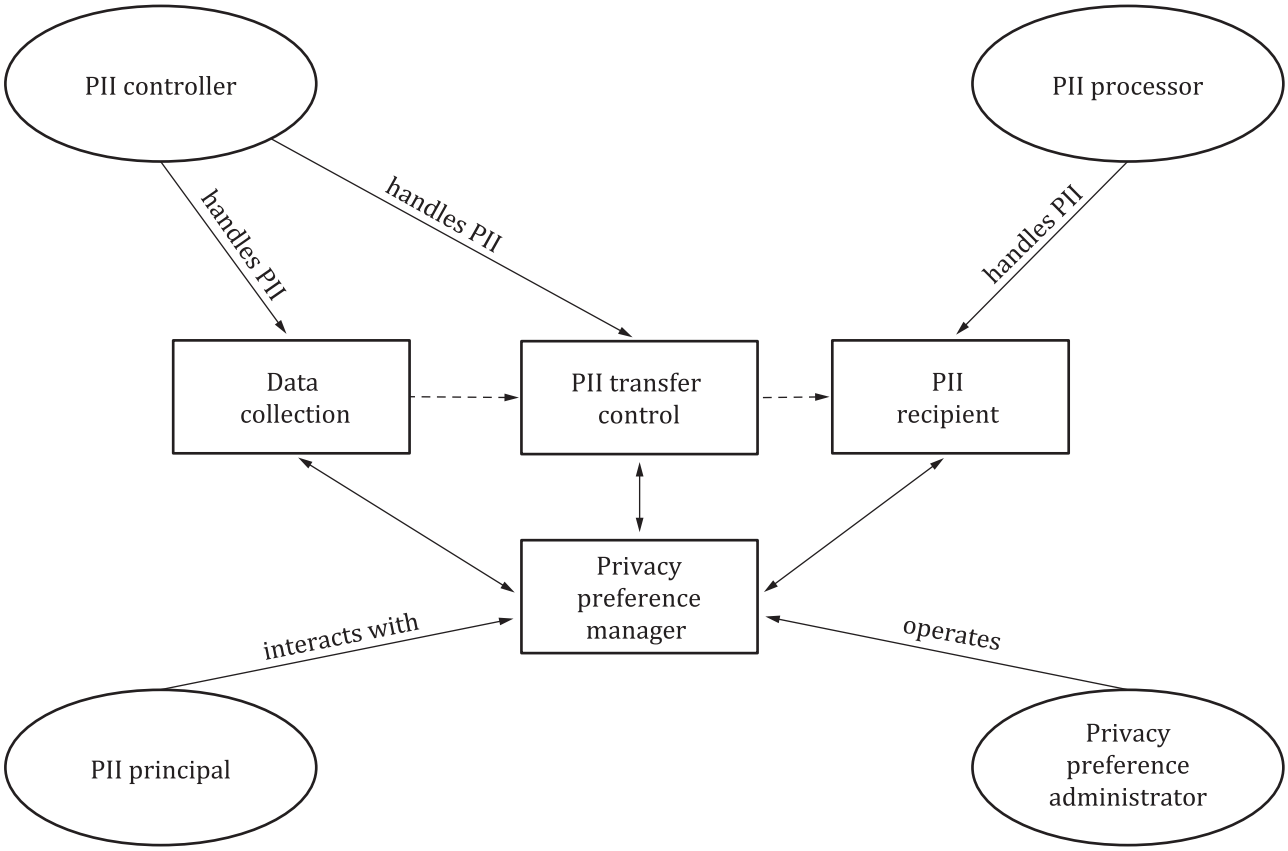

Figure 4 — Relationships between the actors and the components

Figure 5 shows an example of a PII controller managing a platform involving the distribution of PII:

— the PII controller provides a privacy notice to PII principals;

— the PII principal provides consent information and privacy preferences to the PPM;

— the privacy preference administrators may provide a privacy notice to PII principals;

— the privacy preference administrators define data flow control rules and distribute them to PII controllers;

— the PII controllers handle PII in data collection and PII recipient components, and PII processors handle PII in the PII recipient component;

— the PII processors receive PII via the platform managed by a PII controller;

— the PII controller/processor processes PII;

— the PII controller/processor can issue a receipt for the collection or use of the PII.

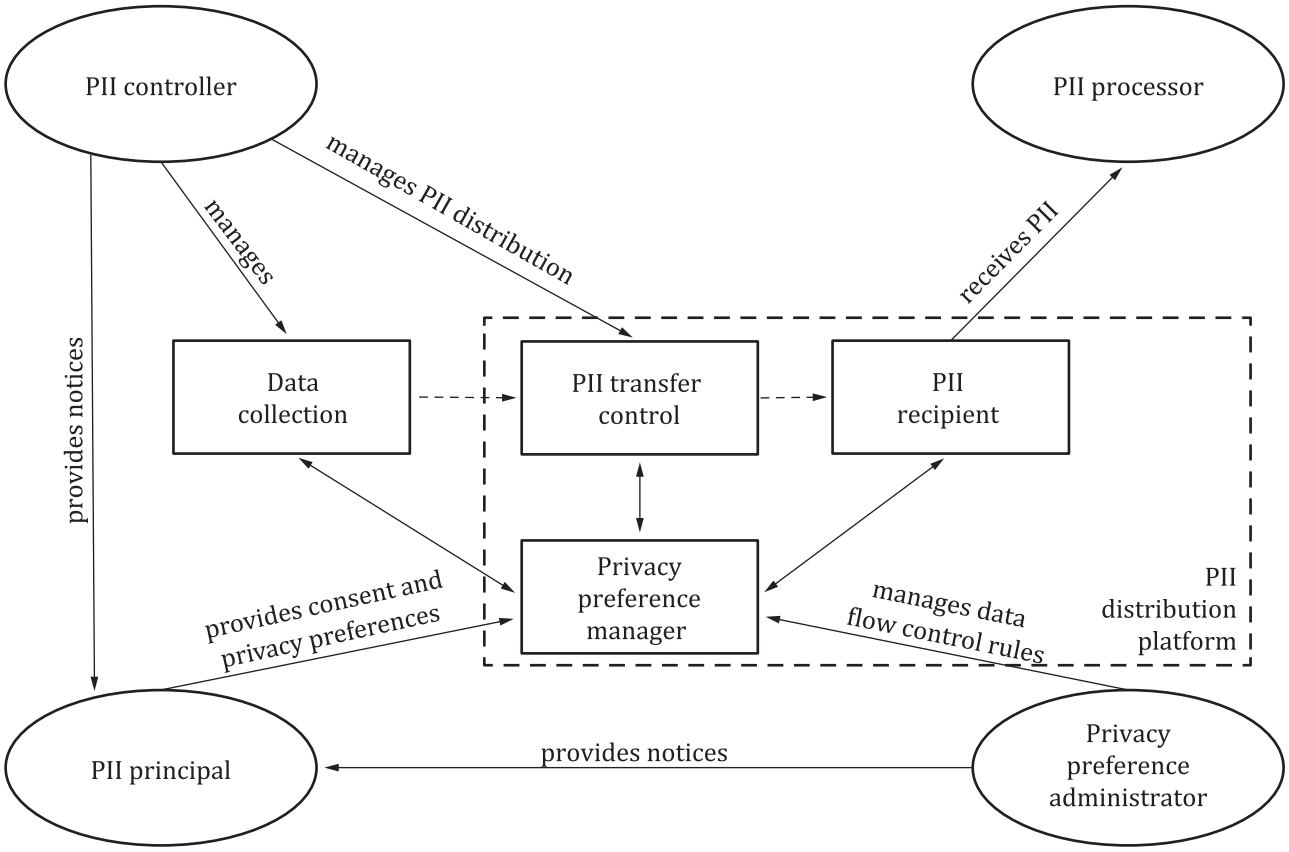

Figure 5 — Example of a platform involving the distribution of PII

The roles of actors in use-cases are introduced in Annex B.

6 Requirements and recommendations for the privacy preference manager

6.1 Overview

The PPM acts as a proxy system for PII principals. It is a useful function for user-centric PII handling based on privacy preferences. In order to realize data flow control based on consent information and privacy preferences, a PPM managing them should be implemented in the system, and a mechanism, for example a user interface, allowing PII principals to input their consent information and privacy preferences should be provided as a part of the component. The PPM shall be designed and operated according to the following requirements and recommendations.

6.2 Privacy impact assessment

A privacy impact assessment (PIA) shall be carried out on the platform (see Figure 5 and 5.5).

NOTE An example of a PIA is described in ISO/IEC 29134.

6.3 Functional recommendations

The PPM should meet the following functional recommendations.

a) Protection of privacy preferences and, where present, consent information: Data protection should be considered, including any risks identified through the privacy impact assessment. Regulatory requirements can be applicable. For example, all privacy preferences and consent information in the PPM should be securely collected, including use of encryption at rest and in transit.

b) Access control: The PPM should be operated with proper access controls. All PII principals and administrators of the PPM should be identified and authenticated, and all their operations should be performed under proper access control policies.

c) Interaction with PII principals: They should be periodically reminded that privacy preferences can be updated, to reflect their current preferences for handling PII.

d) Logging: Operations on the PPM should be recorded in a log including creator, date, type of information, type of operation, and operators.

6.4 Requirements for life cycle management of privacy preferences

Privacy preferences shall be managed according to the following requirements.

a) Generation: Privacy preferences shall be collected, stored and applied to PII handling in a timely manner, once PII principals define them.

b) Update: The privacy preferences shall be collected, stored and applied to PII handling in a timely manner, once they are updated. They can be manually updated by the PPA or automatically updated, whenever the PII principal modifies them. The PPM records the revision history of privacy preferences.

c) Removal: Privacy preferences of a PII principal shall be removed from the PPM in accordance with a principled deletion process (e.g. see ISO/IEC 27555), when the PII principal terminates use of the PPM.

d) Retention: Privacy preferences of a PII principal shall have a retention period after which they are automatically deleted or removed from the PPM (e.g. see ISO/IEC 27555).

7 Further considerations for the PPM in a privacy information management system

When the PPM is used in the context of a privacy information management system (PIMS) for processing PII concerning multiple PII principals, the principles of ISO/IEC 29100 are followed:

— 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;

— privacy compliance.

To this end, the following properties may be of interest:

— confidentiality of privacy preference data;

— integrity of privacy preference data;

— availability of privacy preference data;

— unlinkability of privacy preference data;

— transparency of privacy preference management;

— intervenability of privacy preference management.

Proportionality of privacy preference management efforts should be balanced against the potential privacy implications of the product and service functionality.

Annex D provides examples of PPM capabilities that help meet these properties.

Annex A
(informative)

Use cases of PII handling based on privacy preferences

A.1 Internet-of-Things use case with multiple service providers

This Internet-of-Things (IoT) use case is described in Recommendation ITU-T X.1363[12].

Figure A.1 shows a technical framework in which an IoT service platform that is composed of multiple service providers uses the user preferences stored in privacy preference manager (PPM).

In this case, the common user preferences for any services are stored in a PPM that is accessible through a privacy preference management portal. Specific preferences for each service are stored in another PPM managed by each data service provider. When a user starts to subscribe to a service, data service provider's PPM retrieves common user preferences with the PPM on the privacy preference management portal. The components in the service, such as IoT devices, data storage, and application/service, control the PII based on the preferences in the PPM.

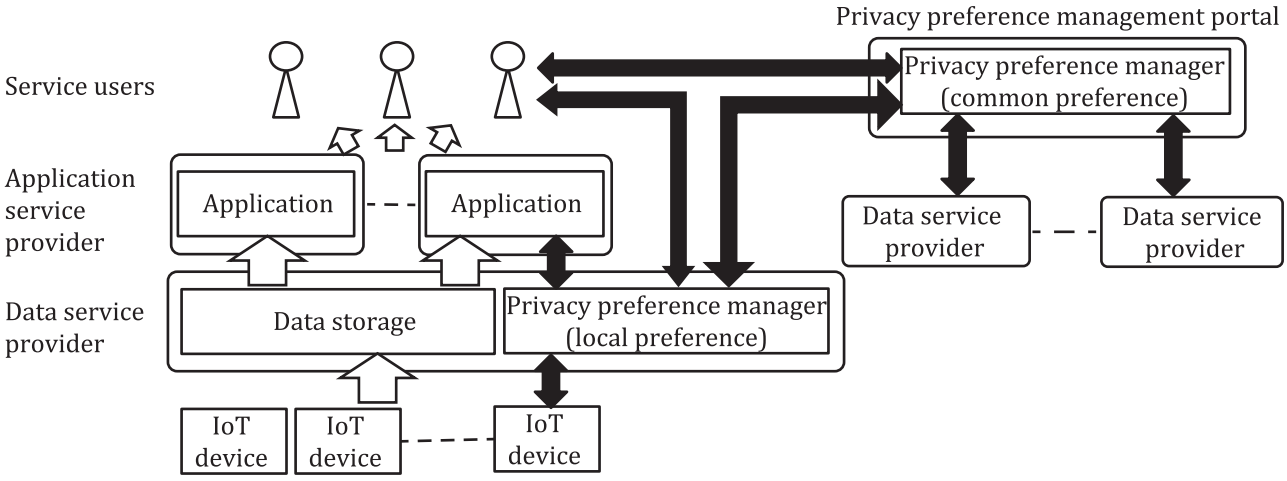

Figure A.1 — Technical framework for handling PII on IoT services by multiple providers with a common privacy preference

A.2 Handling of electronic healthcare records

The electronic health record (EHR) is a set of digital data and documents originated from the interaction of the patients with the healthcare system and generated by present and past clinical events, relating to the patient.

Patients have full control over their data (i.e. patient privacy centric). They have the freedom and rights to decide clinical events, documents and specific data that should be accessed only by concerned/specific health professionals who are directly related with the treatment of the concerned patient. Patients can also decide which data are accessible to other health professionals (e.g. general practitioners, paediatricians, pharmacists, doctors, physicians).

The health professionals who care for the patient can access the clinical data archived in the EHR, except for those data that are subject to obscuration. Health professionals are not expected to be aware of the fact that the patient has obscured such data (i.e. ignorance of data obscuration by patients).

The PPM should be installed to the healthcare system in order to user-centric EHRs handling as Figure A.2.

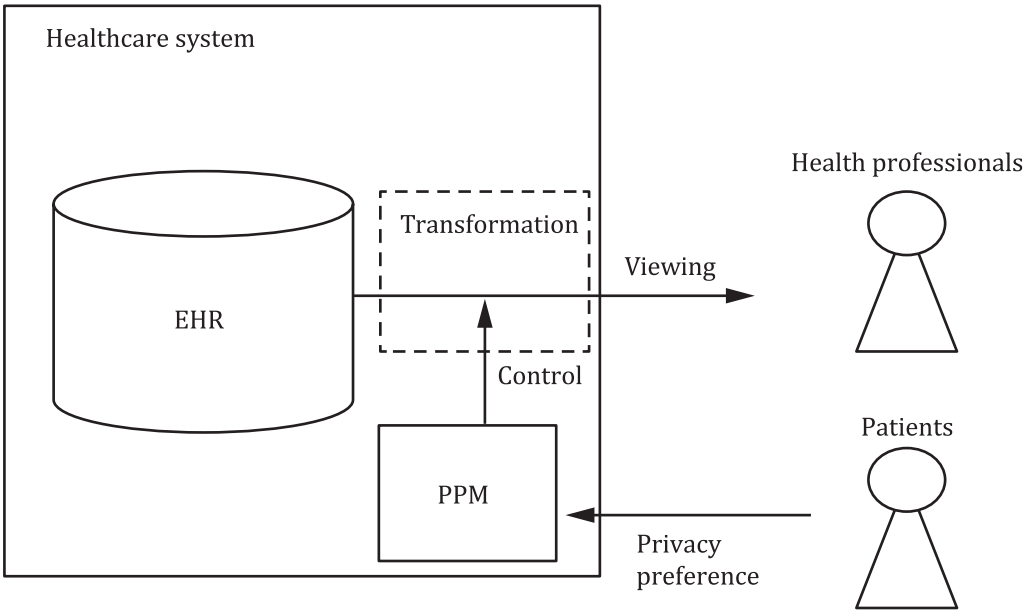

Figure A.2 — Handling of EHR

A.3 Handling of financial data

The financial data sharing platform based on PPM, MyData service, is designed to share financial data of PII principals from different organizations. This is a new, innovative financial business model that offers integrated management of financial data such as banking transactions or credit card records.

For example, the credit rating company receives the financial data as a data receiver to provide a credit rating of a PII principal. The PPM should be installed to the MyData sharing platform to meet a user-centric financial data handling[13].

The purpose of the MyData service is to empower PII principals with the means for improving their right to self-determination regarding their financial data. The objective of the MyData service is to provide innovative, data-driven financial services and bring new benefits to consumers' financial portfolios, including credit and asset management, spending as well as savings.

Figure A.3 describes the concept of a financial data sharing platform of financial data according to PPM configured by the PII principals:

— PII principals provide consent information and configure their privacy preferences in the PPM;

— PII processors receive financial data via the platform;

— the shared data are processed in the data recipient as a PII processor;

— the PII controller/processor provides the custom service, such as the credit rating service of the PII principals.

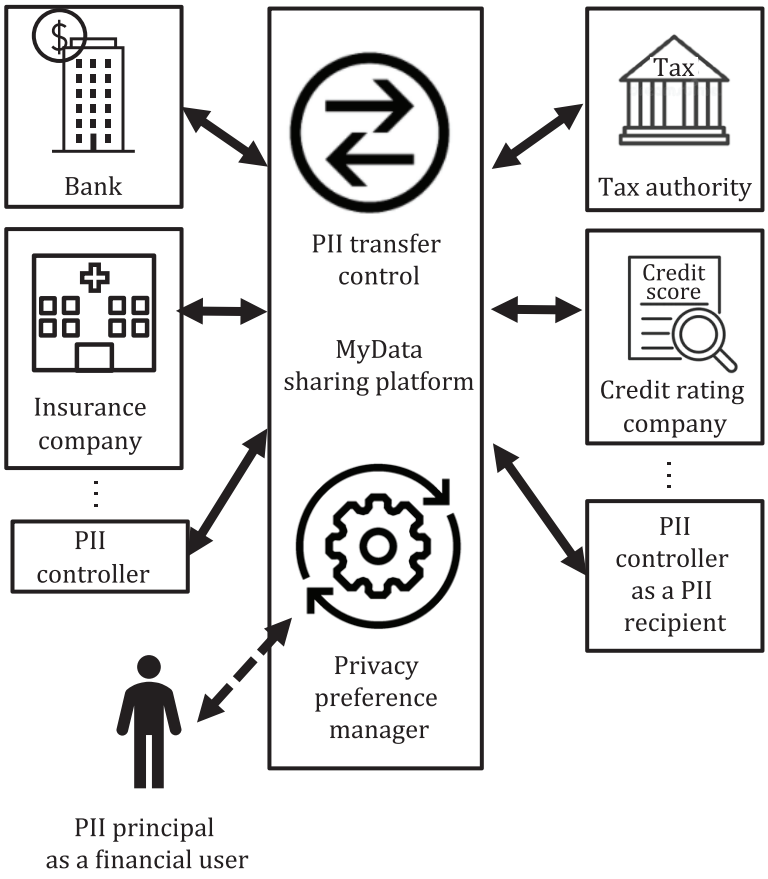

Figure A.3 — Handling of financial data

Annex B
(informative)

Identifying an actor serving as a component for each example service

Table B.1 explains roles between actors and components in some use-cases.

Table B.1 — Roles between actors and components

Example services	Data collection	Privacy preference manager	PII transfer Control	PII recipient	Data transformation(s)	References
Internet of Things (IoT)	IoT devices	Privacy preference management portal	Data service provider	Application service provider /data service provider	Data service provider	A.1
EHR	Health professional	Healthcare system	Healthcare system	Health professionals/ healthcare system	Healthcare system	A.2
Financial data (MyData)	PII principal	MyData	MyData	Service provider	MyData	A.3

Annex C
(informative)

Guidance on configuration of privacy preferences management

C.1 Principles for user interfaces

Annex C provides guidance on the configuration of privacy preferences including design criteria of user interfaces.

User interfaces should be configured to ensure the following:

— ease of access for PII principals;

EXAMPLE The first screen of a personalized web-based service includes a link to the privacy preference user interface.

— comprehensive and clear interface design;

EXAMPLE Example criteria of user interface design are provided in C.2.

— identifiable by each PII principal;

EXAMPLE The PPM provides information about user account of accessing the PII principal on the interface.

— common formats are followed.

EXAMPLE The PPM can provide consent record information following a common format.

C.2 Example criteria of user interface design

Example criteria of the user interface design include:

— The PPM provides an interface through which the PII principal configures common privacy preferences for all PII handling cases. The common privacy preference is used as initial settings of individual privacy preferences for each PII handling case.

— The PPM provides an interface through which the PII principal customizes individual privacy preferences for each PII handling case.

— PII handling cases are categorized into groups and sub-groups. The PPM provide an interface through which PII principal configures individual privacy preferences for each group and each sub-group, in order to reduce PII principal's burden of the configuration for all PII handling cases.

— Differences between common privacy preferences and PII handling cases (use of PII) are indicated on the interface for configuring individual privacy preferences. This information is helpful to configure each individual privacy preference.

— All interfaces are designed as clear and plain descriptions in order to avoid misunderstanding or misconfiguration of privacy preference settings.

C.3 Privacy preference configuration

Table C.1 shows an example scenario for the configuration of privacy preferences. It assumes two capabilities:

— the presentation of privacy preference options, and

— the provision, modification and removal of privacy preference parameters.

Table C.1 — Example of privacy preference scenario

Agents in scenario	User (PII principal), client, e.g. a smart phone, and server, e.g. a cloud server.
Objective of scenario	User requests a function to the server, using the client. This function may involve the use of different PII (attributes or identifying attributes) by the server.
Scenario for privacy preference configuration	Action 1: Client requests a function to the server. Action 2: Server determines the PII attributes that are needed to allow the function to be performed. Server provides the user with information about the PII controller's policies, procedures and practices with respect to the processing of PII. Action 3: Server indicates to the client which attributes are needed to allow the function to be performed, the location where these attributes may be obtained as well as other conditions, if they exist, that may apply to the transfer of these attributes to third parties. Client displays that information to the user. Action 4: Client indicates to the user which attributes are needed to allow the function to be performed and other conditions that may apply to the transfer of these attributes to third parties. Action 5: User indicates to the client whether the client accepts or denies the provision of these attributes to server. If case of acceptance, the client determines from which locations these attributes may be obtained and then fetches these attributes. Action 6: Client releases these attributes to the server. Action 7: Server receives these attributes and check whether they conform to its request and whether they are valid. If the server has indicated that the received attributes are transferred to a third party, it can inform the user by returning a message to the client ("third party receives privacy information").
Scenario for distributed configuration	User (PII principal) has already expressed preferences. User would like this to remembered so that the next time he/she can just confirm. If a cache of the previous preferences is maintained on a laptop or a smart phone, that cache should be synchronized with authoritative records maintained by PPM. Since these choices are PII, they should not be shared with any third party. As the copy in the cache is maintained by a third party, that copy is encrypted.

Annex D
(informative)

Supporting the design of a privacy preference management

Table D.1 provides examples of privacy and security threats which a privacy preference management should take into account. Annex D uses the STRIDE and LINDDUN security and privacy threat classification.

Table D.1 — Example of threats for privacy preference management

Security threats	
Spoofing	Spoofing the privacy preference management components to apply different policies
Tampering	Privacy preference data are changed
Repudiation	A PII principal denies having changed its privacy preferences
Information disclosure	Disclosing privacy preference data
Denial of service	Changing privacy preference to deny services to PII principals Preventing access to the PPM to create denial of service
Elevation of privilege	Changing privilege to enable unauthorized access to the PPM
Privacy threats	
Linkability	Linking privacy preference management activities with other PII principal activities
Identifiability	Identifying a PII principal by monitoring privacy preference management activities
Non-repudiation	PII principal cannot deny having performed an action that has an impact on his/her privacy because of PPM data disclosure
Detectability	Detecting PII principal activities by monitoring privacy preference management components
Disclosure of information	Disclosing PII through privacy preference modification Disclosing privacy preference management activities ending up being PII
Unawareness	PII principal not aware of its privacy preference leading to unwanted PII disclosure
Non-compliance	No compliance of privacy preference management

Examples of capabilities to be provided include the following.

— Consent management: The PPM provides user-interfaces for obtaining consent from PII principals where consent is the legal basis for processing, and manages the consent information. The process to obtain consent from PII principals should follow guidelines in ISO/IEC 29184.

— Access right management: The PPM generates information for PII transfer according to the consent information and privacy preferences of PII principal, and provides it to PII transfer control mechanisms.

Table D.2 and Table D.3 provide examples of PPM capabilities in the case of a PII controller and of a PII processor respectively. The first two columns list controls from ISO/IEC 27701.

Table D.2 — Capabilities for PII controllers supported by PPM

Category	Controls for PII controllers in ISO/IEC 27701	Controls supported by PPM
Conditions for collection and processing	Identify and document purpose	
	Identify legal basis	
	Determine when and how consent should be obtained	
	Obtain and record consent	Managing consent
	Privacy impact assessment	-
	Contracts with PII processors	Managing exchange of privacy preference data
	Joint PII processor	Managing integrity of privacy preference in case of joint PII processing
	Records related to processing PII	Logging privacy preference modifications
Obligations to PII principals	Determining and fulfilling obligations to PII principals	Ensuring that privacy notices provide information on privacy preference management Ensuring that privacy preference management supports PII principals to assert rights that are relevant to a given legislation
	Determining information for PII principals	Ensuring that privacy notices provide clear information on privacy preference management Specifying range of privacy preferences available to PII principals
	Providing information to PII principals	Providing privacy preferences management activities to PII principals
	Provide mechanism to modify or withdraw consent	Managing evidence of modification of consent status
	Provide mechanism to object to PII processing	Providing mechanism to object to processing
	Access, correction and/or erasure	When appropriate, this control should follow PII principal's preferences. For instance, preference on the characteristics of third party PII processors such as location, purpose, impact of processing, related safeguards in place can be considered as preference parameters.
	PII controllers' obligations to inform third parties	
	Providing copy of PII processed	
	Handling requests	
	Automated decision taking	
Privacy-by-design and by-default	Limit collection	When appropriate, these controls should follow PII principal's preferences
	Limit processing	
	Accuracy and quality	
	PII minimization objectives	
	PII de-identification and deletion at the end of processing	
	Temporary files	
	Retention	
	Disposal	
	PII transmission controls	

Table D.2 *(continued)*

Category	Controls for PII controllers in ISO/IEC 27701	Controls supported by PPM
PII sharing, transfer and disclosure	Identify basis for PII transfer between jurisdictions	When appropriate, these controls should follow PII principal's preferences
	Countries and organizations to which PII can be transferred	
	Records of transfer of PII	
	Records of PII disclosure to third parties	

Table D.3 — Capabilities for PII processors supported by PPM

Category	Controls for PII processors	Controls supported by PPM
Conditions for collection and processing	Customer agreement	Obtain agreement on privacy preference management requirements
	Organization's purposes	Verifying that the data processor processes according to PII principal's privacy preferences
	Marketing and advertising use	
	Infringing instruction	
	Customer obligations	
	Records related to processing PII	Logging privacy preference modifications
Obligations to PII principals	Obligations to PII principals	
Privacy-by-design and by-default	Temporary files	When appropriate, these controls should follow PII principal's preferences
	Return transfer or disposal of PII	
	PII transmission controls	
PII sharing, transfer and disclosure	Basis for PII transfer between jurisdiction	When appropriate, these controls should follow PII principal's preferences. For instance, a PII principal can have some preferences on subcontracting.
	Countries and international organizations to which PII may be transferred	
	Records of PII disclosure to third parties	
	Notification of PII disclosure requests	
	Legally binding PII disclosures	
	Disclosure of subcontractors used to process PII	
	Engagement of a subcontractor to process PII	
	Change of subcontractor to process PII	

Bibliography

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

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

[3] ISO Guide 73:2009, *Risk management — Vocabulary*

[4] ISO 5127:2017, *Information and documentation — Foundation and vocabulary*

[5] ISO/IEC 23264-1:2021, *Information security — Redaction of authentic data — Part 1: General*

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

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

[8] ISO/IEC 27038, *Information technology — Security techniques — Specification for digital redaction*

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

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

[11] ISO/IEC 27555, *Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion*

[12] ITU-T X.1363: *Technical framework of personally identifiable information handling system in Internet of things environment*

[13] Guidelines on MyData services in the financial sectors, February 2021, Financial Services Commission (FSC Korea)

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

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

[16] ISO/IEC 27002, *Information security, cybersecurity and privacy protection — Information security controls*

ICS 35.030

Price based on 22 pages