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

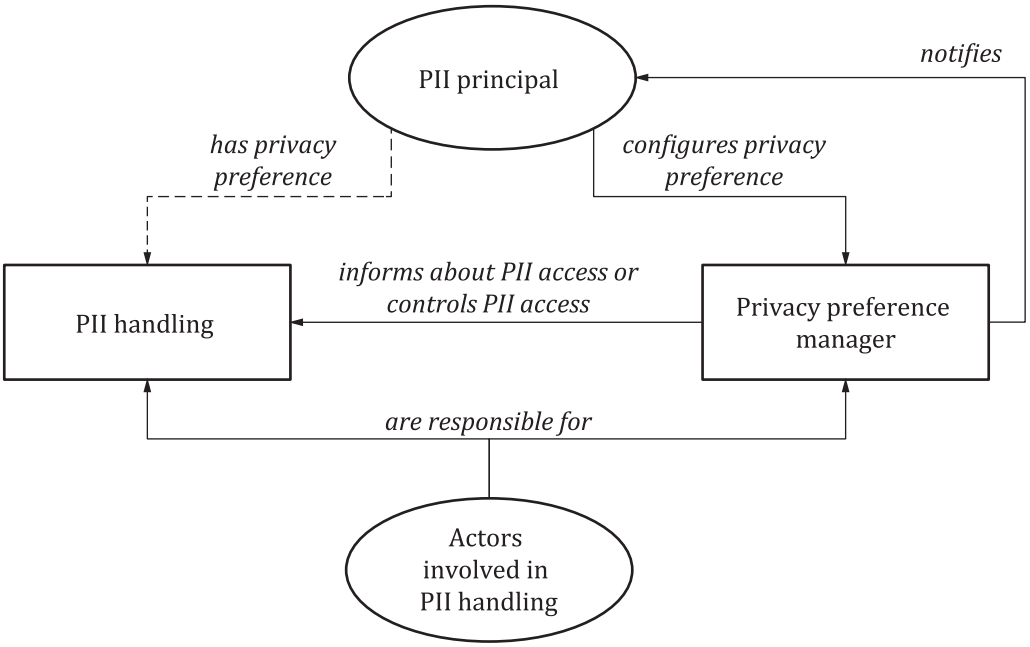
PPM privacy preference manager

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.



Key

actor

component

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.

