FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
29100**

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2023-06-20

Voting terminates on:
2023-08-15

Information technology — Security techniques — Privacy framework

Technologies de l'information — Techniques de sécurité — Cadre privé

Reference number
ISO/IEC FDIS 29100:2023(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).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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*.

This second edition cancels and replaces the first edition (ISO/IEC 29100:2011), of which it constitutes a minor revision. It also incorporates the Amendment ISO/IEC 29100:2011/Amd 1:2018.

The main changes are as follows:

— Clause 2 (normative references) has been added and cross-references have been updated throughout the document;

— replaced the term "secondary use" with “secondary purpose” in Clause 3;

— bibliography has been updated.

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 provides a high-level framework for the protection of personally identifiable information (PII) within information and communication technology (ICT) systems. It is general in nature and places organizational, technical, and procedural aspects in an overall privacy framework.

The privacy framework is intended to help organizations define their privacy safeguarding requirements related to PII within an ICT environment by:

— specifying a common privacy terminology;

— defining the actors and their roles in processing PII;

— describing privacy safeguarding requirements; and

— referencing known privacy principles.

Due to the increasing number of information and communication technologies that process PII, it is important to have international information security standards that provide a common understanding for the protection of PII. This document is intended to enhance existing security standards by adding a focus relevant to the processing of PII.

The increasing commercial use and value of PII, the sharing of PII across jurisdictions, and the growing complexity of ICT systems, can make it difficult for an organization to ensure privacy and to achieve compliance with the various applicable laws. Privacy stakeholders can prevent uncertainty and distrust from arising by handling privacy matters properly and avoiding cases of PII misuse.

Use of this document will:

— aid in the design, implementation, operation, and maintenance of ICT systems that handle and protect PII;

— spur innovative solutions to enable the protection of PII within ICT systems; and

— improve organizations' privacy programs through the use of best practices.

The privacy framework provided within this document can serve as a basis for additional privacy standardization initiatives, such as for:

— a technical reference architecture;

— the implementation and use of specific privacy technologies and overall privacy management;

— privacy controls for outsourced data processes;

— privacy risk assessments; or

— specific engineering specifications.

Information technology — Security techniques — Privacy framework

1 Scope

This document provides a privacy framework which:

— specifies a common privacy terminology;

— defines the actors and their roles in processing personally identifiable information (PII);

— describes privacy safeguarding considerations;

— provides references to known privacy principles for information technology.

This document is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.

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
anonymity
characteristic of information that does not permit a *personally identifiable information principal* (3.9) to be identified directly or indirectly

3.2
anonymization
process by which *personally identifiable information (PII)* (3.7) is irreversibly altered in such a way that a *PII principal* (3.9) can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party

3.3
anonymized data
data that has been produced as the output of a *personally identifiable information* (3.7) *anonymization* (3.2) process

3.4
consent
personally identifiable information (PII) principal's (3.9) freely given, specific and informed agreement to the processing of their PII

3.5
identifiability
condition which results in a *personally identifiable information (PII) principal* (3.9) being identified, directly or indirectly, on the basis of a given set of PII

3.6
opt-in
process or type of policy whereby the *personally identifiable information (PII) principal* (3.9) is required to take an action to express explicit, prior *consent* (3.4) for their PII to be processed for a particular purpose

Note 1 to entry: A different term that is often used with the privacy principle "consent and choice" is “opt-out”. It describes a process or type of policy whereby the PII principal is required to take a separate action in order to withhold or withdraw consent, or oppose a specific type of processing. The use of an opt-out policy presumes that the PII controller has the right to process the PII in the intended way. This right can be implied by some action of the PII principal different from consent (e.g. placing an order in an online shop).

3.7
personally identifiable information
PII
information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or might be directly or indirectly linked to a natural person

Note 1 to entry: The “natural person” in the definition is the *PII principal* (3.9). 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 establish the link between the set of PII and the natural person.

3.8
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information (PII)* (3.7) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others [e.g. *PII processors* (3.10)] to process PII on its behalf while the responsibility for the processing remains with the PII controller.

3.9
PII principal
data subject
natural person to whom the *personally identifiable information (PII)* (3.7) relates

3.10
PII processor
privacy stakeholder that processes *personally identifiable information (PII)* (3.7) on behalf of and in accordance with the instructions of a *PII controller* (3.8)

3.11
privacy breach
situation where *personally identifiable information* (3.7) is processed in violation of one or more relevant privacy safeguarding requirements

3.12
privacy control
measure that treats privacy risks by reducing their likelihood or their consequences

Note 1 to entry: Privacy controls include organizational, physical and technical measures, e.g. policies, procedures, guidelines, legal contracts, management practices or organizational structures.

Note 2 to entry: Control is also used as a synonym for safeguard or countermeasure.

3.13
privacy enhancing technology
PET
privacy control (3.12), consisting of information and communication technology (ICT) measures, products, or services that protect privacy by eliminating or reducing *personally identifiable information (PII)* (3.7) or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system

Note 1 to entry: Examples of PETs include, but are not limited to, *anonymization* (3.2) and *pseudonymization* (3.22) tools that eliminate, reduce, mask, or de-identify PII or that prevent unnecessary, unauthorized and/or undesirable processing of PII.

Note 2 to entry: Masking is the process of obscuring elements of PII.

3.14
privacy policy
overall intention and direction, rules and commitment, as formally expressed by the *personally identifiable information (PII) controller* (3.8) related to the processing of *PII* (3.7) in a particular setting

3.15
privacy preference
specific choices made by a *personally identifiable information (PII) principal* (3.9) about how their *PII* (3.7) should be processed for a particular purpose

3.16
privacy principle
shared value governing the privacy protection of *personally identifiable information (PII)* (3.7) when processed in information and communication technology systems

3.17
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.

3.18
privacy impact assessment
privacy risk assessment
overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of *personally identifiable information* (3.7), framed within an organization's broader risk management framework

3.19
privacy safeguarding requirement
requirement that an organization takes into account when processing *personally identifiable information (PII)* (3.7) with respect to the privacy protection of PII

3.20
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 (PII)* (3.7) processing

3.21
processing of PII
operation or set of operations performed upon *personally identifiable information (PII)* (3.7)

Note 1 to entry: Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, *anonymization* (3.2), *pseudonymization* (3.22), dissemination or otherwise making available, deletion or destruction of PII.

3.22
pseudonymization
process applied to *personally identifiable information (PII)* (3.7) which replaces identifying information with an alias

Note 1 to entry: Pseudonymization can be performed either by *PII principals* (3.9) themselves or by *PII controllers* (3.8). Pseudonymization can be used by PII principals to consistently use a resource or service without disclosing their identity to this resource or service (or between services), while still being held accountable for that use.

Note 2 to entry: Pseudonymization does not rule out the possibility that there can be (a restricted set of) *privacy stakeholders* (3.20) other than the PII controller of the pseudonymized data which are able to determine the PII principal's identity based on the alias and data linked to it.

3.23
sensitive PII
category of *personally identifiable information (PII)* (3.7), either whose nature is sensitive, such as those that relate to the *PII principal's* (3.9) most intimate sphere, or that can have a significant impact on the PII principal

Note 1 to entry: In some jurisdictions or in specific contexts, sensitive PII is defined in reference to the nature of the PII and can consist of PII revealing the racial origin, political opinions or religious or other beliefs, personal data on health, sex life or criminal convictions, as well as other PII that can be defined as sensitive.

3.24
third party

privacy stakeholder (3.20) other than the *personally identifiable information (PII) principal* (3.9), the *PII controller* (3.8) and the *PII processor* (3.10), and the natural persons who are authorized to process the data under the direct authority of the PII controller or the PII processor

4 Abbreviated terms

ICT information and communication technology

PET privacy enhancing technology

PII personally identifiable information

5 Basic elements of the privacy framework

5.1 Overview of the privacy framework

The following components relate to privacy and the processing of PII in ICT systems and make up the privacy framework described in this document:

— actors and roles;

— interactions;

— recognizing PII;

— privacy safeguarding requirements;

— privacy policies;

— privacy controls.

For the development of this privacy framework, concepts, definitions and recommendations from other official sources have been taken into consideration. These sources can be found in Reference [3].

NOTE In order to make it easier to use ISO/IEC 27000 and related international standards concerning ISMS [4]-[25] in the specific context of privacy and to integrate privacy concepts in the ISO/IEC 27000 context, Table A.1 shows how the concepts from References [4] to [25] correspond with the concepts used in this document.

5.2 Actors and roles

5.2.1 General

For the purposes of this document, it is important to identify the actors involved in the processing of PII. There are four types of actors who can be involved in the processing of PII: PII principals, PII controllers, PII processors and third parties.

5.2.2 PII principals

PII principals provide their PII for processing to PII controllers and PII processors and, when it is not otherwise provided by applicable law, they give consent and determine their privacy preferences for how their PII should be processed. PII principals can include, for example, an employee listed in the human resources system of a company, the consumer mentioned in a credit report, and a patient listed in an electronic health record. It is not always necessary that the respective natural person is identified directly by name in order to be considered a PII principal. If the natural person to whom the PII relates can be identified indirectly (e.g. through an account identifier, social security number, or even through the combination of available attributes), he or she is considered to be the PII principal for that PII set.

5.2.3 PII controllers

A PII controller determines why (purpose) and how (means) the processing of PII takes place. The PII controller should ensure adherence to the privacy principles in this framework during the processing of PII under its control (e.g. by implementing the necessary privacy controls). There can be more than one PII controller for the same PII set or set of operations performed upon PII (for the same or different legitimate purposes). In this case, the different PII controllers shall work together and make the necessary arrangements to ensure the privacy principles are adhered to during the processing of PII. A PII controller can also decide to have all or part of the processing operations carried out by a different privacy stakeholder on its behalf. It is expected that PII controllers carefully assess whether or not they are processing sensitive PII and implement reasonable and appropriate privacy and security controls, as well as any potential adverse effects for PII principals as identified during a privacy risk assessment.

NOTE Legal requirements can apply.

5.2.4 PII processors

A PII processor carries out the processing of PII on behalf of a PII controller, acts on behalf of, or in accordance with the instructions of the PII controller, observes the stipulated privacy requirements and implements the corresponding privacy controls.

NOTE In some jurisdictions, the PII processor is bound by a contract.

5.2.5 Third parties

A third party can receive PII from a PII controller or a PII processor. A third party does not process PII on behalf of the PII controller. Generally, the third party will become a PII controller in its own right once it has received the PII in question.

5.3 Interactions

The actors identified in 5.2 can interact with each other in a variety of ways. As far as the possible flows of PII among the PII principal, the PII controller and the PII processor are concerned, the following scenarios can be identified:

a) the PII principal provides PII to a PII controller (e.g. when registering for a service provided by the PII controller);

b) the PII controller provides PII to a PII processor which processes that PII on behalf of the PII controller (e.g. as part of an outsourcing agreement);

c) the PII principal provides PII to a PII processor which processes that PII on behalf of the PII controller;

d) the PII controller provides the PII principal with PII which is related to the PII principal (e.g. pursuant to a request made by the PII principal);

e) the PII processor provides PII to the PII principal (e.g. as directed by the PII controller);

f) the PII processor provides PII to the PII controller (e.g. after having performed the service for which it was appointed).

The roles of the PII principal, PII controller, PII processor and a third party in these scenarios are illustrated in Table 1.

There is a need to distinguish between PII processors and third parties because the legal control of the PII remains with the original PII controller when it is sent over to the PII processor, whereas a third party can become a PII controller in its own right once it has received the PII in question. For instance, where a third party makes the decision to transfer PII it has received from a PII controller to yet another party, it will be acting as a PII controller in its own right and will therefore no longer be considered a third party.

As far as the possible flows of PII among the PII controllers and PII processors on the one hand, and third parties on the other hand are concerned, the following scenarios can be identified:

g) the PII controller provides PII to a third party (e.g. in the context of a business agreement); and

h) the PII processor provides PII to a third party (e.g. as directed by the PII controller).

The roles of the PII controller and a third party in these scenarios are also illustrated in Table 1.

Table 1 — Possible flows of PII among the PII principal, PII controller, PII processor and a third party and their roles

	PII principal	PII controller	PII processor	Third party
Scenario a)	PII provider	PII recipient	—	—
Scenario b)	—	PII provider	PII recipient	—
Scenario c)	PII provider	—	PII recipient	—
Scenario d)	PII recipient	PII provider	—	—
Scenario e)	PII recipient	—	PII provider	—
Scenario f)	—	PII recipient	PII provider	—
Scenario g)	—	PII provider	—	PII recipient
Scenario h)	—	—	PII provider	PII recipient

