SLOVENSKI STANDARD
oSIST prEN ISO/IEC 29100:2020

01-april-2020

Informacijska tehnologija - Varnostne tehnike - Zasebni okvir (ISO/IEC 29100:2011, vključno z dopolnilom A1:2018)

Information technology - Security techniques - Privacy framework (ISO/IEC 29100:2011, including Amd 1:2018)

Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Datenschutz (ISO/IEC 29100:2011, einschließlich Amd 1:2018)

Technologies de l'information - Techniques de sécurité - Cadre privé (ISO/IEC 29100:2011, y compris Amd 1:2018)

Ta slovenski standard je istoveten z: **prEN ISO/IEC 29100**

ICS:

35.030	Informacijska varnost	IT Security

oSIST prEN ISO/IEC 29100:2020 **en,fr,de**

INTERNATIONAL STANDARD

ISO/IEC 29100

First edition
2011-12-15

Information technology — Security techniques — Privacy framework

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

Reference number
ISO/IEC 29100:2011(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Figures

Tables

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 29100 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

This International Standard 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.

In some jurisdictions, this International Standard's references to privacy safeguarding requirements might be understood as being complementary to legal requirements for the protection of PII. 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 International Standard 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 legal 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 International Standard 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 International Standard 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.

Some jurisdictions might require compliance with one or more of the documents referenced in ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 (WG 5 SD2) — *Official Privacy Documents References* [3] or with other applicable laws and regulations, but this International Standard is not intended to be a global model policy, nor a legislative framework.

Information technology — Security techniques — Privacy framework

1 Scope

This International Standard 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; and
- provides references to known privacy principles for information technology.

This International Standard 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 Terms and definitions

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

NOTE In order to make it easier to use the ISO/IEC 27000 family of International Standards in the specific context of privacy and to integrate privacy concepts in the ISO/IEC 27000 context, the table in Annex A provides the ISO/IEC 27000 concepts that correspond with the ISO/IEC 29100 concepts used in this International Standard.

2.1
anonymity
characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly

2.2
anonymization
process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party

2.3
anonymized data
data that has been produced as the output of a personally identifiable information anonymization process

2.4
consent
personally identifiable information (PII) principal’s freely given, specific and informed agreement to the processing of their PII

2.5
identifiability
condition which results in a personally identifiable information (PII) principal being identified, directly or indirectly, on the basis of a given set of PII

2.6
identify
establish the link between a personally identifiable information (PII) principal and PII or a set of PII

2.7
identity
set of attributes which make it possible to identify the personally identifiable information principal

2.8
opt-in
process or type of policy whereby the personally identifiable information (PII) principal is required to take an action to express explicit, prior consent for their PII to be processed for a particular purpose

NOTE 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).

2.9
personally identifiable information
PII
any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

NOTE 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.

2.10
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes

NOTE A PII controller sometimes instructs others (e.g., PII processors) to process PII on its behalf while the responsibility for the processing remains with the PII controller.

2.11
PII principal
natural person to whom the personally identifiable information (PII) relates

NOTE 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”.

2.12
PII processor
privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller

2.13
privacy breach
situation where personally identifiable information is processed in violation of one or more relevant privacy safeguarding requirements

2.14
privacy controls
measures that treat privacy risks by reducing their likelihood or their consequences

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

NOTE 2 Control is also used as a synonym for safeguard or countermeasure.

2.15
privacy enhancing technology
PET
privacy control, consisting of information and communication technology (ICT) measures, products, or services that protect privacy by eliminating or reducing personally identifiable information (PII) or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system

NOTE 1 Examples of PETs include, but are not limited to, anonymization and pseudonymization tools that eliminate, reduce, mask, or de-identify PII or that prevent unnecessary, unauthorized and/or undesirable processing of PII.

NOTE 2 Masking is the process of obscuring elements of PII.

2.16
privacy policy
overall intention and direction, rules and commitment, as formally expressed by the personally identifiable information (PII) controller related to the processing of PII in a particular setting

2.17
privacy preferences
specific choices made by a personally identifiable information (PII) principal about how their PII should be processed for a particular purpose

2.18
privacy principles
set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems

2.19
privacy risk
effect of uncertainty on privacy

NOTE 1 Risk is defined as the “effect of uncertainty on objectives” in ISO Guide 73 and ISO 31000.

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

2.20
privacy risk assessment
overall process of risk identification, risk analysis and risk evaluation with regard to the processing of personally identifiable information (PII)

NOTE This process is also known as a privacy impact assessment.

2.21
privacy safeguarding requirements
set of requirements an organization has to take into account when processing personally identifiable information (PII) with respect to the privacy protection of PII

2.22
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) processing