International Standard

ISO/IEC 29100

Information technology — Security techniques — Privacy framework

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

Second edition
2024-02

Reference number
ISO/IEC 29100:2024(en)

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