International Standard

ISO/IEC 27701

Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la protection de la vie privée — Exigences et recommandations

Second edition
2025-10

Reference number
ISO/IEC 27701:2025(en)

© ISO/IEC 2025



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms, definitions and abbreviations **1**

4 Context of the organization **4**
4.1 Understanding the organization and its context 4
4.2 Understanding the needs and expectations of interested parties 5
4.3 Determining the scope of the privacy information management system 5
4.4 Privacy information management system 6

5 Leadership **6**
5.1 Leadership and commitment 6
5.2 Privacy policy 6
5.3 Roles, responsibilities and authorities 7

6 Planning **7**
6.1 Actions to address risks and opportunities 7
6.1.1 General 7
6.1.2 Privacy risk assessment 7
6.1.3 Privacy risk treatment 8
6.2 Privacy objectives and planning to achieve them 9
6.3 Planning of changes 10

7 Support **10**
7.1 Resources 10
7.2 Competence 10
7.3 Awareness 10
7.4 Communication 10
7.5 Documented information 11
7.5.1 General 11
7.5.2 Creating and updating documented information 11
7.5.3 Control of documented information 11

8 Operation **12**
8.1 Operational planning and control 12
8.2 Privacy risk assessment 12
8.3 Privacy risk treatment 12

9 Performance evaluation **12**
9.1 Monitoring, measurement, analysis and evaluation 12
9.2 Internal audit 13
9.2.1 General 13
9.2.2 Internal audit programme 13
9.3 Management review 13
9.3.1 General 13
9.3.2 Management review inputs 13
9.3.3 Management review results 14

10 Improvement **14**
10.1 Continual improvement 14
10.2 Nonconformity and corrective action 14

11 Further information on annexes **14**

Annex A (normative) **PIMS reference control objectives and controls for PII controllers and PII processors** **15**

© ISO/IEC 2025 – All rights reserved

Annex B (normative) **Implementation guidance for PII controllers and PII processors** **21**
Annex C (informative) **Mapping to ISO/IEC 29100** **51**
Annex D (informative) **Mapping to the General Data Protection Regulation** **53**
Annex E (informative) **Mapping to ISO/IEC 27018 and ISO/IEC 29151** **56**
Annex F (informative) **Correspondence with ISO/IEC 27701:2019** **58**
Bibliography **64**

© ISO/IEC 2025 – All rights reserved

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*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/CLC/JTC 13, *Cybersecurity and data protection*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This second edition cancels and replaces the first edition (ISO/IEC 27701:2019), which has been technically revised.

The main changes are as follows:

— the document has been redrafted as a stand-alone management system standard.

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.

© ISO/IEC 2025 – All rights reserved

Introduction

0.1 General

Almost every organization processes personally identifiable information (PII). Further, the quantity and types of PII processed are increasing, as are the number of situations where an organization needs to cooperate with other organizations regarding the processing of PII. Protection of privacy in the context of the processing of PII is a societal need, as well as the topic of dedicated legal requirements worldwide.

This document includes mapping to:

— the privacy framework and principles defined in ISO/IEC 29100;

— ISO/IEC 27018;

— ISO/IEC 29151;

— the EU General Data Protection Regulation.

NOTE These mappings can be interpreted to take into account local legal requirements.

This document can be used by PII controllers (including those that are joint PII controllers) and PII processors (including those using subcontracted PII processors and those processing PII as subcontractors to PII processors).

By complying with the requirements in this document, an organization can generate evidence of how it handles the processing of PII. Such evidence can be used to facilitate agreements with business partners where the processing of PII is mutually relevant. This can also assist in relationships with other interested parties. The use of this document can provide independent verification of this evidence.

0.2 Compatibility with other management system standards

This document applies the framework developed by ISO to improve alignment among its management system standards.

This document enables an organization to align or integrate its privacy information management system (PIMS) with the requirements of other management system standards, and in particular with the information security management system specified in ISO/IEC 27001.

© ISO/IEC 2025 – All rights reserved

Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

1 Scope

This document specifies requirements for establishing, implementing, maintaining and continually improving a privacy information management system (PIMS).

Guidance is also provided to assist in the implementation of the requirements in this document.

This document is intended for personally identifiable information (PII) controllers and PII processors holding responsibility and accountability for PII processing.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

3 Terms, definitions and abbreviations

For the purposes of this document, the terms and definitions given in ISO/IEC 29100 and the following 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
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.6)

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: If the organization is part of a larger entity, the term “organization” refers only to the part of the larger entity that is within the scope of the *privacy informationmanagement system* (3.23).

3.2
interested party
person or *organization* (3.1) that can affect, be affected by, or perceive itself to be affected by a decision or activity

© ISO/IEC 2025 – All rights reserved

3.3
top management
person or group of people who directs and controls an *organization* (3.1) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: If the scope of the *management system* (3.4) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

3.4
management system
set of interrelated or interacting elements of an *organization* (3.1) to establish *policies* (3.5) and *objectives* (3.6), as well as *processes* (3.8) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The management system elements include the organization's structure, roles and responsibilities, planning and operation.

3.5
policy
intentions and direction of an *organization* (3.1) as formally expressed by its *top management* (3.3)

3.6
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as finance, health and safety, and environment). They can be, for example, organization-wide or specific to a project, product or *process* (3.8).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended result, as a purpose, as an operational criterion, as a privacy objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of *privacy information management systems* (3.23), privacy objectives are set by the *organization* (3.1), consistent with the privacy *policy* (3.5), to achieve specific results.

3.7
risk
effect of uncertainty

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

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.

Note 3 to entry: Risk is often characterized by reference to potential events and consequences, or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

3.8
process
set of interrelated or interacting activities that uses or transforms inputs to deliver a result

Note 1 to entry: Whether the result of a process is called an output, a product or a service depends on the context of the reference.

3.9
competence
ability to apply knowledge and skills to achieve intended results

© ISO/IEC 2025 – All rights reserved

3.10
documented information
information required to be controlled and maintained by an *organization* (3.1) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media and from any source.

Note 2 to entry: Documented information can refer to:

— the *management system* (3.4), including related *processes* (3.8);

— information created in order for the organization to operate (documentation);

— evidence of results achieved (records).

3.11
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to managing activities, *processes* (3.8), products, services, systems or *organizations* (3.1).

3.12
continual improvement
recurring activity to enhance *performance* (3.11)

3.13
effectiveness
extent to which planned activities are realized and planned results are achieved

3.14
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the *organization* (3.1) and *interested parties* (3.2) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, e.g. in *documented information* (3.10).

3.15
conformity
fulfilment of a *requirement* (3.14)

3.16
nonconformity
non-fulfilment of a *requirement* (3.14)

3.17
corrective action
action to eliminate the cause(s) of a *nonconformity* (3.16) and to prevent recurrence

3.18
audit
systematic and independent *process* (3.8) for obtaining evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: An internal audit is conducted by the *organization* (3.1) itself, or by an external party on its behalf.

Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

© ISO/IEC 2025 – All rights reserved

3.19
measurement
process (3.8) to determine a value

3.20
monitoring
determining the status of a system, a *process* (3.8) or an activity

Note 1 to entry: To determine the status, there can be a need to check, supervise or critically observe.

3.21
joint PII controller
personally identifiable information (PII) controller that determines the purposes and means of the processing of PII jointly with one or more other PII controllers

3.22
customer
person or *organization* (3.1) that can or does receive a product or a service that is intended for or required by this person or organization

EXAMPLE Consumer, client, end-user, retailer, receiver of product or service from an internal *process* (3.8), beneficiary and purchaser.

Note 1 to entry: A customer can be internal or external to the organization.

Note 2 to entry: A customer can be an organization that has a contract with a PII controller, a PII controller who has a contract with a PII processor or a PII processor that has a contract with a subcontractor for PII processing.

3.23
privacy information management system
PIMS
management system (3.4) which addresses the protection of privacy as potentially affected by the processing of personally identifiable information

3.24
information security programme
set of *policies* (3.5), *objectives* (3.6) and *processes* (3.8) designed to manage *risks* (3.7) to an *organization's* (3.1) assets, to ensure confidentiality, integrity and availability of information

Note 1 to entry: An information security programme can be, for example, an information security management system such as one based on ISO/IEC 27001.

3.25
statement of applicability
documentation of all necessary controls and justification for the inclusion or exclusion of such controls

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended result(s) of its privacy information management system.

The organization shall determine whether climate change is a relevant issue.

The organization shall determine if it is acting as a PII controller (including as a joint PII controller) or as a PII processor.

The organization shall determine external and internal issues that are relevant to its context and that affect its ability to achieve the intended outcome(s) of its PIMS.

NOTE 1 External and internal issues can include but are not limited to:

© ISO/IEC 2025 – All rights reserved