



SLOVENSKI STANDARD
oSIST prEN ISO/IEC 27701:2024
01-september-2024

Informacijska varnost, kibernetika varnost in varovanje zasebnosti - Sistem upravljanje informacij o zasebnosti - Zahteve in smernice (ISO/IEC DIS 27701:2024)

Information security, cybersecurity and privacy protection - Privacy information management systems - Requirements and guidance (ISO/IEC DIS 27701:2024)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Datenschutz-Informationenmanagementsysteme - Anforderungen und Leitlinien (ISO/IEC DIS 27701:2024)

Titre manque

Ta slovenski standard je istoveten z: prEN ISO/IEC 27701

[oSIST prEN ISO/IEC 27701:2024](https://standards.iteh.ai/catalog/standards/sist/6b52a4f6-e355-4b5e-a262-da82d8bbdeda/osist-pr-en-iso-iec-27701-2024)

<https://standards.iteh.ai/catalog/standards/sist/6b52a4f6-e355-4b5e-a262-da82d8bbdeda/osist-pr-en-iso-iec-27701-2024>

ICS:

35.030 Informacijska varnost IT Security

oSIST prEN ISO/IEC 27701:2024 **en,fr,de**



DRAFT International Standard

ISO/IEC DIS 27701.2

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

ICS: 35.030

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2024-07-02

Voting terminates on:
2024-08-27

Open Standards
(<https://standards.iteh.ai>)
Document Preview

[oSIST prEN ISO/IEC 27701:2024](https://standards.iteh.ai/catalog/standards/sist/6b52a4f6-e355-4b5e-a262-2-da82d8bbdeda/osist-pren-iso-iec-27701-2024)

<https://standards.iteh.ai/catalog/standards/sist/6b52a4f6-e355-4b5e-a262-2-da82d8bbdeda/osist-pren-iso-iec-27701-2024>

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

IMPORTANT — Please use this updated version dated 2024-06-19, and discard any previous version of this DIS as VA relation has been added.

Reference number
ISO/IEC DIS 27701.2:2024(en)

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

© ISO/IEC 2024

ISO/IEC DIS 27701.2:2024(en)

iTeh Standards (<https://standards.iteh.ai>) Document Preview

[oSIST prEN ISO/IEC 27701:2024](https://standards.iteh.ai/catalog/standards/sist/6b52a4f6-e355-4b5e-a262-da82d8bbdeda/osist-pren-iso-iec-27701-2024)

<https://standards.iteh.ai/catalog/standards/sist/6b52a4f6-e355-4b5e-a262-da82d8bbdeda/osist-pren-iso-iec-27701-2024>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

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

ISO/IEC DIS 27701.2:2024(en)

Contents

Page

Foreword.....	viii
Introduction.....	ix
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviations.....	1
4 Context of the organization.....	5
4.1 Understanding the organization and its context.....	5
4.2 Understanding the needs and expectations of interested parties.....	5
4.3 Determining the scope of the privacy information management system.....	6
4.4 Privacy information management system.....	6
5 Leadership.....	7
5.1 Leadership and commitment	7
5.2 Privacy Policy.....	7
5.3 Roles, responsibilities and authorities.....	7
6 Planning	8
6.1 Actions to address risks and opportunities.....	8
6.1.1 General	8
6.1.2 Privacy risk assessment.....	8
6.1.3 Privacy risk treatment.....	9
6.2 Privacy objectives and planning to achieve them.....	10
6.3 Planning of changes.....	10
7 Support.....	10
7.1 Resources	10
7.2 Competence	10
7.3 Awareness	11
7.4 Communication	11
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	12
8 Operation.....	12
8.1 Operational planning and control	12
8.2 Privacy risk assessment.....	12
8.3 Privacy risk treatment.....	13
9 Performance evaluation.....	13
9.1 Monitoring, measurement, analysis and evaluation	13
9.2 Internal audit	13
9.2.1 General	13
9.2.2 Internal audit programme	13
9.3 Management review	14
9.3.1 General	14
9.3.2 Management review inputs.....	14

ISO/IEC DIS 27701.2:2024(en)

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	15
Annex A	(normative) PIMS reference control objectives and controls for PII Controllers and PII Processors	16
Annex B	(normative) Implementation guidance for PII Controllers and PII processors	23
B.1	Implementation guidance for PII controllers	23
B.1.1	General	23
B.1.2	Conditions for collection and processing	23
B.1.2.1	Objective	23
B.1.2.2	Identify and document purpose	23
B.1.2.3	Identify lawful basis	23
B.1.2.4	Determine when and how consent is to be obtained	24
B.1.2.5	Obtain and record consent	24
B.1.2.6	Privacy impact assessment	25
B.1.2.7	Contracts with PII processors	25
B.1.2.8	Joint PII controller	26
B.1.2.9	Records related to processing PII	26
B.1.3	Obligations to PII principals	27
B.1.3.1	Objective	27
B.1.3.2	Determining and fulfilling obligations to PII principals	27
B.1.3.3	Determining information for PII principals	27
B.1.3.4	Providing information to PII principals	28
B.1.3.5	Providing mechanism to modify or withdraw consent	28
B.1.3.6	Providing mechanism to object to PII processing	29
B.1.3.7	Access, correction or erasure	29
B.1.3.8	PII controllers' obligations to inform third parties	30
B.1.3.9	Providing copy of PII processed	30
B.1.3.10	Handling requests	30
B.1.3.11	Automated decision making	31
B.1.4	Privacy by design and privacy by default	31
B.1.4.1	Objective	31
B.1.4.2	Limit collection	31
B.1.4.3	Limit processing	31
B.1.4.4	Accuracy and quality	32

ISO/IEC DIS 27701.2:2024(en)

B.1.4.5 PII minimization objectives	32
B.1.4.6 PII de-identification and deletion at the end of processing	33
B.1.4.7 Temporary files	33
B.1.4.8 Retention	33
B.1.4.9 Disposal	34
B.1.4.10 PII transmission controls.....	34
B.1.5 PII sharing, transfer and disclosure.....	34
B.1.5.1 Objective	34
B.1.5.2 Identify basis for PII transfer between jurisdictions.....	34
B.1.5.3 Countries and international organizations to which PII can be transferred	35
B.1.5.4 Records of transfer of PII	35
B.1.5.5 Records of PII disclosure to third parties	35
B.2 Implementation guidance for PII processors	35
B.2.1 General	35
B.2.2 Conditions for collection and processing.....	36
B.2.2.1 Objective	36
B.2.2.2 Customer agreement	36
B.2.2.3 Organization's purposes	36
B.2.2.4 Marketing and advertising use	37
B.2.2.5 Infringing instruction.....	37
B.2.2.6 Customer obligations	37
B.2.2.7 Records related to processing PII.....	37
B.2.3 Obligations to PII principals	37
B.2.3.1 Objective	38
B.2.3.2 Comply with obligations to PII principals	38
B.2.4 Privacy by design and privacy by default	38
B.2.4.1 Objective	38
B.2.4.2 Temporary files.....	38
B.2.4.3 Return, transfer or disposal of PII	38
B.2.4.4 PII transmission controls.....	39
B.2.5 PII sharing, transfer and disclosure.....	39
B.2.5.1 Objective	39
B.2.5.2 Basis for PII transfer between jurisdictions	39
B.2.5.3 Countries and international organizations to which PII can be transferred	40
B.2.5.4 Records of PII disclosures to third parties	40
B.2.5.5 Notification of PII disclosure requests.....	40

ISO/IEC DIS 27701.2:2024(en)

B.2.5.6 Legally binding PII disclosures	41
B.2.5.7 Disclosure of subcontractors used to process PII	41
B.2.5.8 Engagement of a subcontractor to process PII.....	41
B.2.5.9 Change of subcontractor to process PII.....	42
B.3 Implementation guidance for PII controllers and PII processors.....	42
B.3.1 Objective.....	42
B.3.2 General.....	42
B.3.3 Policies for information security.....	42
B.3.4 Information security roles and responsibilities.....	42
B.3.5 Classification of information.....	43
B.3.6 Labelling of information.....	43
B.3.7 Information transfer.....	43
B.3.8 Identity management	44
B.3.9 Access rights.....	44
B.3.10 Addressing information security within supplier agreements.....	44
B.3.11 Information security incident management planning and preparation.....	45
B.3.12 Response to information security incidents	45
B.3.13 Legal, statutory, regulatory and contractual requirements.....	47
B.3.14 Protection of records	47
B.3.15 Independent review of information security.....	47
B.3.16 Compliance with policies, rules and standards for information security	48
B.3.17 Information security awareness, education and training.....	48
B.3.18 Confidentiality or non-disclosure agreements.....	48
B.3.19 Clear desk and clear screen.....	49
B.3.20 Storage media.....	49
B.3.21 Secure disposal or re-use of equipment	49
B.3.22 User endpoint devices	50
B.3.23 Secure authentication.....	50
B.3.24 Information backup	50
B.3.25 Logging.....	51
B.3.26 Use of cryptography	51
B.3.27 Secure development life cycle	52
B.3.28 Application security requirements.....	52
B.3.29 Secure system architecture and engineering principles	52
B.3.30 Outsourced development.....	53
B.3.31 Test information.....	53

ISO/IEC DIS 27701.2:2024(en)

Annex C (informative) Mapping to ISO/IEC 29100	54
Annex D (informative) Mapping to the General Data Protection Regulation	57
Annex E (informative) Mapping to ISO/IEC 27018 and ISO/IEC 29151	61
Annex F (informative) Correspondence with ISO/IEC 27701:2019	64
Bibliography	72

iTeh Standards (<https://standards.iteh.ai>) Document Preview

[oSIST prEN ISO/IEC 27701:2024](https://standards.iteh.ai/catalog/standards/sist/6b52a4f6-e355-4b5e-a262-da82d8bbdeda/osist-pren-iso-iec-27701-2024)

<https://standards.iteh.ai/catalog/standards/sist/6b52a4f6-e355-4b5e-a262-da82d8bbdeda/osist-pren-iso-iec-27701-2024>

ISO/IEC DIS 27701.2:2024(en)

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 27701:2019), which has been redrafted as a stand-alone management system.

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 DIS 27701.2:2024(en)

Introduction

0.1 General

Almost every organization processes personally identifiable information (PII). Further, the quantity and types of PII processed is increasing, as is 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 legislation or regulation all over the world.

This document includes mapping to:

- the privacy framework and principles defined in ISO/IEC 29100;
- ISO/IEC 27018;
- ISO/IEC 29151; and
- the EU General Data Protection Regulation.

NOTE These can be interpreted to take into account local legislation or regulation.

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.

This document was initially developed as ISO/IEC 27552.01:2024

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 PIMS with the requirements of other management system standards, and in particular with the information security management system specified in ISO/IEC 27001.

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 provided to assist in the implementation of the requirements in this document.

This document is intended for 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 terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://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 information *management system* (3.4).

3.2

interested party (preferred term)

stakeholder (admitted term)

ISO/IEC DIS 27701.2:2024(en)

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

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 information 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* (3.22), privacy information objectives are set by the *organization* (3.1), consistent with the privacy information *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 (as defined in ISO Guide 73) and consequences (as defined in ISO Guide 73), or a combination of these.