SLOVENSKI STANDARD
oSIST prEN ISO/IEC 29151:2025

01-marec-2025

Informacijska varnost, kibernetska varnost in varstvo zasebnosti - Kontrole in smernice obnašanja pri varovanju osebnih podatkov

Information security, cybersecurity and privacy protection - Controls and guidance for personally identifiable information protection (ISO/IEC DIS 29151:2024)

Informationstechnik - Sicherheitsverfahren - Leitfaden für den Schutz personenbezogener Daten (ISO/IEC DIS 29151:2024)

Sécurité de l'information, cybersécurité et protection de la vie privée - Mesures de sécurité et recommandations pour la protection des données à caractère personnel (ISO/IEC DIS 29151:2024)

iTeh Standards
(https://standards.iteh.ai)
Document Preview
oSIST prEN ISO/IEC 29151:2025
https://standards.iteh.ai/catalog/standards/sist/d26f0a53-c8c3-460f-91c6-fde836e01168/osist-pren-iso-iec-29151-2025

Ta slovenski standard je istoveten z: prEN ISO/IEC 29151

ICS:

35.030	Informacijska varnost	IT Security

oSIST prEN ISO/IEC 29151:2025 en,fr,de

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

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

oSIST prEN ISO/IEC 29151:2025
https://standards.iteh.ai/catalog/standards/sist/d26f0a53-c8c3-460f-91c6-fde836e01168/osist-pren-iso-iec-29151-2025

DRAFT
International
Standard

ISO/IEC DIS 29151

Information security, cybersecurity and privacy protection – Controls and guidance for personally identifiable information protection

ICS: 35.030

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

Secretariat: **DIN**

Voting begins on:
2024-12-17

Voting terminates on:
2025-03-11

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

oSIST prEN ISO/IEC 29151:2025
https://standards.iteh.ai/catalog/standards/sist/d26f0a53-c8c3-460f-91c6-fde836e01168/osist-pren-iso-iec-29151-2025

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

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.

Reference number
ISO/IEC DIS 29151:2024(en)

© ISO/IEC 2024

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

oSIST prEN ISO/IEC 29151:2025
https://standards.iteh.ai/catalog/standards/sist/d26f0a53-c8c3-460f-91c6-fde836e01168/osist-pren-iso-iec-29151-2025

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

Contents

Page

iTeh Standards
(https://standards.iteh.ai)
Document Preview
oSIST prEN ISO/IEC 29151:2025
https://standards.iteh.ai/catalog/standards/sist/d26f0a53-e8c3-460f-91e6-fde836e01168/osist-pren-iso-iec-29151-2025

© ISO/IEC 2024 – All rights reserved

iTeh Standards
(https://standards.iteh.ai)
Document Preview
oSIST prEN ISO/IEC 29151:2025
https://standards.iteh.ai/catalog/standards/sist/d26f0a53-e8c3-460f-91e6-fde836e01168/osist-pren-iso-iec-29151-2025

© ISO/IEC 2024 – All rights reserved

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

oSIST prEN ISO/IEC 29151:2025
https://standards.iteh.ai/catalog/standards/sist/d26f0a53-c8c3-460f-91c6-fde836e01168/osist-pren-iso-iec-29151-2025

© ISO/IEC 2024 – All rights reserved

Introduction

The number of organizations processing personally identifiable information (PII) is increasing, as is the amount of PII that these organizations deal with. At the same time, societal expectations for the protection of PII and the security of data relating to individuals are also increasing. A number of countries are augmenting their laws to address the increased number of high profile data breaches.

As the number of PII breaches increases, organizations collecting or processing PII will increasingly need guidance on how they should protect PII in order to reduce the risk of privacy breaches occurring, and to reduce the impact of breaches on the organization and on the individuals concerned. This document provides such guidance.

This document offers guidance for PII controllers on a broad range of information security and PII protection controls that are commonly applied in many different organizations that deal with protection of PII. Other ISO/IEC standards that provide guidance or requirements on other aspects of the overall process of protecting PII are as follows:

- ISO/IEC 27001 specifies an information security management system, which is a suitable foundation for protecting any information, including PII.
- ISO/IEC 27002 provides guidelines for organizational, people-related, physical and technological information security controls that can be used for the protection of all kinds of information, including PII.
- ISO/IEC 27005 provides guidance to assist organizations to address information security risks and perform information security risk management activities, specifically information security risk assessment and treatment.
- ISO/IEC 27018 offers guidance to organizations acting as PII processors when offering processing capabilities as cloud services.
- ISO/IEC 27701 specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS).
- ISO/IEC 29100 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.
- ISO/IEC 29134 provides guidelines for assessing the potential impacts on privacy of a process, information system, programme, software module, device or other initiative which processes personally identifiable information (PII), while ISO/IEC 27001 together with ISO/IEC 27005 provides guidance to perform information security risk management activities.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
oSIST prEN ISO/IEC 29151:2025
https://standards.iteh.ai/catalog/standards/sist/d2610a33-c8c3-4601-91c6-1ac836c01168/osist-pren-iso-iec-29151-2025

Controls are chosen based on the risks identified as a result of a risk analysis to develop a comprehensive, consistent system of controls. Controls are adapted to the context of the particular processing of PII.

This document contains two parts: 1) the main body consisting of clauses 1 to 8, and 2) a normative annex A (Extended control set for PII protection) and informative Annex B (Correspondence of ISO/IEC 29151:202X (this document) with ISO/IEC 29151:2017). This structure reflects normal practice for the development of PII-specific extensions to ISO/IEC 27002 for the main body.

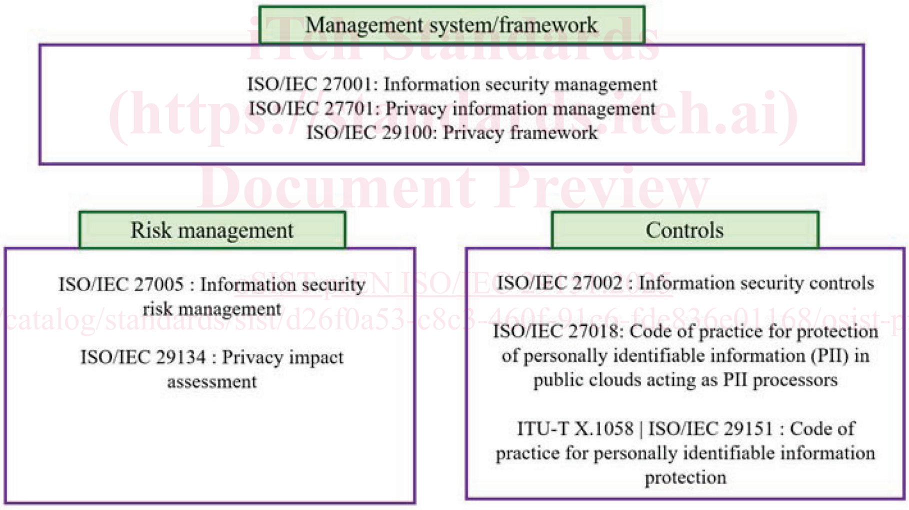
The structure of the main body of this document, including the clause titles, reflects the main body of ISO/IEC 27002:2022. The introduction and clauses 1 to 4 provide background on the use of this document. Headings for subclauses in clauses 5 to 8 mirror those of ISO/IEC 27002:2022, reflecting the fact that this document builds on the guidance in ISO/IEC 27002:2022, adding new controls specific to the protection of PII. Many of the controls in ISO/IEC 27002:2022 need no amplification in the context of PII controllers. However, in some cases, additional implementation guidance is needed, and this is given under the appropriate heading (and clause number) from ISO/IEC 27002:2022.

© ISO/IEC 2024 – All rights reserved

The normative annex contains an extended set of PII protection-specific controls. These new PII protection controls, with their associated guidance, are divided into twelve categories, corresponding to the privacy policy and the eleven privacy principles of ISO/IEC 29100:

- consent and choice;
- purpose, legitimacy and specification;
- collection limitation;
- data minimization;
- use, retention and disclosure limitation;
- accuracy and quality;
- openness, transparency and notice;
- individual participation and access;
- accountability;
- information security; and
- privacy compliance.

Figure 1 describes the relationship between this document and other ISO/IEC standards.


Management system/framework
ISO/IEC 27001: Information security management
ISO/IEC 27701: Privacy information management
ISO/IEC 29100: Privacy framework
Risk management
ISO/IEC 27005 : Information security risk management
ISO/IEC 29134 : Privacy impact assessment
Controls
ISO/IEC 27002 : Information security controls
ISO/IEC 27018: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ITU-T X.1058 | ISO/IEC 29151 : Code of practice for personally identifiable information protection

iTeh Standards (https://standards.iteh.ai) Document Preview
oSIST prEN ISO/IEC 29151:2025
https://standards.iteh.ai/catalog/standards/sist/d26f0a53-c8c3-460f-91e6-fde836e01168/osist-pren-iso-iec-29151-2025

Figure 1 — The relationship of this document and other ISO/IEC standards

This document includes guidelines based on ISO/IEC 27002, and adapts these as necessary to address the privacy needs that arise from the processing of PII:

a) In different processing domains such as:

  - public cloud services,
  - social networking applications,
  - internet-connected devices in the home,
  - search, analysis,
  - targeting of PII for advertising and similar purposes,

- big data analytics programmes,
- employment processing,
- business management in sales and service (enterprise resource planning, customer relationship management);

b) In different locations such as:

- on a personal processing platform provided to an individual (e.g., smart cards, smart phones and their apps, smart meters, wearable devices),
- within data transportation and collection networks (e.g., where mobile phone location data is created operationally by network processing, which may be considered PII in some jurisdictions),
- within an organization's own processing infrastructure,
- on a third party's processing platform;

c) For the collection characteristic such as:

- one-time data collection (e.g., on registering for a service),
- ongoing data collection (e.g., frequent health parameter monitoring by sensors on or in an individual's body, multiple data collections using contactless payment cards for payment, smart meter data collection systems, and so on).

  NOTE Ongoing data collection can contain or yield behavioural, locational and other types of PII. In such cases, the use of PII protection controls that allow access and collection to be managed based on consent and that allow the PII principal to exercise appropriate control over such access and collection, need to be considered.

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

oSIST prEN ISO/IEC 29151:2025
https://standards.iteh.ai/catalog/standards/sist/d26f0a53-c8c3-460f-91c6-fde836e01168/osist-pren-iso-iec-29151-2025

© ISO/IEC 2024 – All rights reserved

Information security, cybersecurity and privacy protection – Controls and guidance for personally identifiable information protection

1 Scope

This Recommendation | International Standard establishes controls, purpose, and guidance for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of personally identifiable information (PII).

In particular, this Recommendation | International Standard specifies guidance based on ISO/IEC 27002, taking into consideration the controls for processing PII that may be applicable within the context of an organization's privacy risk environment(s).

This Recommendation | International Standard is applicable to all types and sizes of organizations acting as PII controllers (as defined in ISO/IEC 29100), including public and private companies, government entities and not-for-profit organizations that process PII, in particular, organizations that do not establish or operate a privacy information management system.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
oSIST prEN ISO/IEC 29151:2025
https://standards.iteh.ai/catalog/standards/sist/d26f0a55-c8c5-4661-91e0-fde856e01f68/osist-pren-iso-iec-29151-2025

ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

ISO/IEC 29100:2024, *Information technology — Security techniques — Privacy framework*

3 Terms and Definitions and abbreviated terms

3.1 Definitions

For the purposes of this Recommendation | International Standard, the terms and definitions that are given in ISO/IEC 27000:2018, ISO/IEC 27002:2022, ISO/IEC 29100 and the following apply.

The ISO *Online browsing platform*, IEC *Electropedia* and ITU *Terms and definitions* are terminological databases for use in standardization.

3.1.1
chief privacy officer (CPO):
Senior management individual who is accountable for the protection of personally identifiable information (PII) in an organization.

© ISO/IEC 2024 – All rights reserved

3.1.2
de-identification process:
Process of removing the association between a set of identifying data and the data principal, using de-identification techniques.

3.1.3
organization:
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.

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.

3.1.4
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* (3.1.3). 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.

[SOURCE: ISO/IEC 29100:2024, 3.7]

3.1.5
PII controller:
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information (PII)* (3.1.4) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others [e.g. *PII processors* (3.1.7)] to process PII on its behalf while the responsibility for the processing remains with the PII controller.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
oSIST prEN ISO/IEC 29151:2025
https://standards.iteh.ai/catalog/standards/sist/d26f0a53-c8c3-460f-91c6-fde836e01168/osist-pren-iso-iec-29151-2025

[SOURCE: ISO/IEC 29100:2024, 3.8]

3.1.6
PII principal, data subject:
natural person to whom the *personally identifiable information (PII)* (3.1.4) relates

[SOURCE: ISO/IEC 29100:2024, 3.9]

3.1.7
PII processor:
privacy stakeholder that processes *personally identifiable information (PII)* (3.1.4) on behalf of and in accordance with the instructions of a *PII controller* (3.1.5)

[SOURCE: ISO/IEC 29100:2024, 3.10]

3.2 Abbreviated terms

For the purposes of this document, the following abbreviations apply.

CPO	Chief Privacy Officer
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information

4 Overview

4.1 Objective for the protection of PII

This document provides a set of controls for PII protection. The objective of the protection of PII is to enable organizations to put in place a set of controls as part of their overall PII protection programme. They can be used in a framework for demonstrating compliance with privacy-related laws and regulations, managing privacy risks and meeting the expectations of PII principals, regulators or clients, in accordance with the privacy principles described in ISO/IEC 29100.

4.2 Requirement for the protection of PII

An organization should identify its PII protection requirements. The privacy principles in ISO/IEC 29100 apply to the identification of requirements. There are three main sources of PII protection requirements:

- legal, statutory, regulatory and contractual requirements related to protection of PII including, for example, PII requirements that an organization, its trading partners, contractors and service providers have to comply with;
- assessment of risks (i.e., security risks and privacy risks) to the organization and the PII principal, taking into account the organization's overall business strategy and objectives, through a risk assessment;
- corporate policies: an organization may also choose voluntarily to go beyond the criteria that are derived from previous requirements.

Organizations should also adhere to the principles (i.e., privacy principles defined in ISO/IEC 29100), objectives and business requirements for processing PII that have been developed to support their operations.

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

PII protection controls (including security controls) should be selected on the basis of a risk assessment. The results of a privacy impact assessment (PIA), e.g., as specified in ISO/IEC 29134, will help to guide and determine the appropriate treatment action and priorities for managing risks to the protection of PII and for implementing controls selected to protect against these risks.

A PIA document such as that in ISO/IEC 29134 may provide PIA guidance, including advice on risk assessment, risk treatment plan, risk acceptance and risk review.

oSIST prEN ISO/IEC 29151:2025
https://standards.iteh.ai/catalog/standards/sist/e5010a55-e0e3-466f-97e6-fde836e01168/osist-pren-iso-iec-29151-2025

4.3 Controls

A privacy risk assessment can assist organizations in identifying the specific risks of privacy breaches resulting from unlawful processing or of infringements of the rights and freedom of the PII principal involved in an envisaged PII processing or from inadequate or not effective information security or privacy controls. Organizations should identify and implement controls to treat the risks identified by the risk impact process. The controls and treatments should then be documented, ideally in a separate risk register. Certain types of PII processing can warrant specific controls for which the need only becomes apparent once an envisaged operation has been carefully analysed.

4.4 Selecting controls

Controls can be selected from this document (which includes by reference the controls from ISO/IEC 27002, creating a combined reference control set). If required, controls can also be selected from other control sets or new controls can be designed to meet specific needs, as appropriate.

The selection of controls is dependent upon organizational decisions based on the criteria for risk treatment options and the general risk management approach, applied to the organization and, through contractual agreements, to its customers and suppliers, and should also be subject to all applicable national and international legislation and regulations.

The selection and implementation of controls is also dependent upon the organization's role in the provision of infrastructure or services. Many different organizations may be involved in providing infrastructure or services. In some circumstances, selected controls may be unique to a particular organization. In other instances, there may be shared roles in implementing controls. Contractual agreements should clearly specify the PII protection responsibilities of all organizations involved in providing or using the services.

The controls in this document can be used as reference for organizations that process PII, and are intended to be applicable for all organizations acting as PII controllers. Organizations acting as PII processors should do so, in accordance with the instructions of the PII controller. PII controllers should ensure that their PII processors are able to implement all the necessary controls included in their PII processing agreement, in accordance with the purpose of PII processing. PII controllers using cloud services as PII processors may review ISO/IEC 27018 to identify relevant controls to implement.

The controls in this document are explained in more detail in clauses 5 to 8, along with implementation guidance. Implementation may be made simpler if requirements for the protection of PII have been considered in the design of the organization's information systems, services and operations. Such consideration is an element of the concept that is often called privacy by design (PBD). More information about selecting controls and other risk treatment options can be found in ISO/IEC 29134. Other relevant references are listed in the bibliography.

4.5 Developing organization specific guidelines

This document can be regarded as a starting point for developing organization specific guidelines. Not all of the controls and guidance in this document are applicable to all organizations.

Furthermore, additional controls and guidelines not included in this document may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this document, where applicable, to facilitate compliance checking by auditors and business partners.

4.6 Life cycle considerations

PII has a natural life cycle, from creation or origination, collection, through storage, use and transfer to its eventual disposal (e.g., secure destruction). The value of, and risks to, PII may vary during its life cycle, but protection of PII remains important at all stages and in all contexts of its life cycle.

Information systems also have life cycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained, and eventually retired from service and disposed of. PII protection should also be taken into account at each of these stages. New system developments and changes to existing systems present opportunities for organizations to update and improve security controls as well as controls for the protection of PII, taking actual incidents, and current and projected information security and privacy risks into account.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
oSIST prEN ISO/IEC 29151:2025

4.7 Structure of this document

Control descriptions in ISO/IEC 27002:2022 are structured as follows. Each control has the following elements:

a) Control title: Short name of the control;

b) Attribute table: A table shows the value(s) of each attribute for the given control;

c) Control: What the control is;

d) Purpose: Why the control should be implemented;

e) Guidance: How the control should be implemented;

f) Other information: Explanatory text or references to other related documents.

Subheadings are used in the guidance text for some controls to aid readability where guidance is lengthy and addresses multiple topics. Such headings are not necessarily used in all guidance text. Subheadings are underlined.

© ISO/IEC 2024 – All rights reserved