SLOVENSKI STANDARD
oSIST prEN 17926:2023

01-januar-2023

Sistem upravljanja informacij o varstvu podatkov po ISO/IEC 27701 - Izboljšave v evropskem kontekstu

Privacy Information Management System per ISO/IEC 27701 - Refinements in European context

Datenschutz-Informationsmanagementsystem per ISO/IEC 27701 - Verfeinerungen im europäischen Kontext

Ta slovenski standard je istoveten z: **prEN 17926**

ICS:

35.030 Informacijska varnost IT Security

oSIST prEN 17926:2023 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 17926

November 2022

ICS

English version

Privacy Information Management System per ISO/IEC 27701 - Refinements in European context

Datenschutz-Informationsmanagementsystem per ISO/IEC 27701 - Verfeinerungen im europäischen Kontext

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/CLC/JTC 13.

If this draft becomes a European Standard, CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CEN and CENELEC in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

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.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.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

Contents

Page

European foreword 2
Introduction 3
1 Scope 4
2 Normative references 4
3 Terms and definitions 4
4 Structure of this document 4
5 Privacy information management system for PII processing operations 5
6 Requirement for PII processing operations 5
Annex A (normative) Information security *and privacy* controls 6
Annex B (normative) PIMS-specific reference control objectives and controls (PII Controllers) 18
Annex C (normative) PIMS-specific reference control objectives and controls (PII Processors) 25
Annex D (informative) Model for combination of management system certification governed by certification requirements in ISO/IEC 17021 with a non-tangible product-based certification governed by certification requirements in ISO/IEC 17065 28
Annex E (informative) Relationship between this European Standard and the General Data Protection Regulation 30
Bibliography 35

European foreword

This document (prEN 17926:2022) has been prepared by Technical Committee CEN/CLC/JTC 13, “Cybersecurity and Data Protection”, the secretariat of which is held by DIN.

This document is currently submitted to the CEN enquiry.

Introduction

EN ISO/IEC 27701 specifies requirements and provides guidance for estClishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS) which can be implemented in any jurisdiction. As a management system designed for international use, its requirements are generic, and the guidance can be adapted by the organizations according to their context and applicCle obligations.

Although EN ISO/IEC 27701 was written with the intention to be applicCle under any jurisdiction, including under the EU General Data Protection Regulation (GDPR) (ISO/IEC 27701 Annex D contains a mapping between clauses of the standard and GDPR), it is the responsibility of the organization to determine how to implement requirements and controls of EN ISO/IEC 27701 in the context of the GDPR.

This document provides refinements to EN ISO/IEC 27701 in the application of controls and guidance in EN ISO/IEC 27701 specific to GDPR where necessary. This document is applicCle to the same entities as is ISO/IEC 27701: all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS (information security management system). This is intended to be used by organizations in the GDPR context for the purpose of demonstrating compliance with their obligations. EN ISO/IEC 27701 combined with the refinements of this document constitutes a set of requirements which is more specifically designed and fit for the context of GDPR than the generic ones from EN ISO/IEC 27701 alone.

Thus EN ISO/IEC 27701 can be considered as an international framework, which can be refined for a particular regional context (in the case of this document, the GDPR), and even to add requirements fit for a given jurisdiction/country or sector (out of scope of this document).

The refinements to EN ISO/IEC 27701, for processing operations as part of products, processes, and services specified in this document can be used for conformity assessment which can be conducted, either by first, second, or third parties. In particular, certification bodies can use these requirements and refinements to assess the conformity of both a privacy information management system per ISO/IEC 17021 and the processing operations of a product, process or service per ISO/IEC 17065. Certification schemes for products involving PII processing can reference this document, as described in ISO/IEC 17067 for “type 6” schemes.

NOTE “product” can be read as “process” or “service” (ISO/IEC 17065, Clause 1 and Annex B).

The requirements in this document can be part of scheme governed under both ISO/IEC 17065 for the requirements on products involving PII processing activities (“products requirements” as per ISO/IEC 17065 Clause 3.8) and ISO/IEC 17021 for the management system requirements (ISO/IEC 17067 type 6 scheme).

GDPR Article 42 encourages the estClishment of data protection certification mechanisms. Provisions of this document can be used by competent bodies to specify data protection certification mechanisms as per GDPR article 42 in order to assess the conformity of processing operations in the PIMS as per ISO/IEC 17065 including assessment of privacy information management system systematic elements as allowed by Clause 6 of ISO/IEC 17067.

1 Scope

This document specifies refinements for an application of EN ISO/IEC 27701 in a European context.

This document is applicable to the same entities as is ISO/IEC 27701: all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS (information security management system).

An organization can use this document for the implementation of the generic requirements and controls of EN ISO/IEC 27701 according to its context and its applicable obligations.

Certification criteria based on these refinements can provide a certification model under ISO/IEC 17065 for processing operations performed within the scope of a privacy information management system according to EN ISO/IEC 27701, which can be combined with certification requirements for EN ISO/IEC 27701 under ISO/IEC 17021.

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.

EN ISO/IEC 27701:2021, *Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines*

EN ISO/IEC 27001:2017, *Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)*

3 Terms and definitions

No terms and definitions are listed in this document.

ISO and IEC maintain terminological datCases for use in standardization at the following addresses:

— IEC Electropedia: availCle at https://www.electropedia.org/

— ISO Online browsing platform: availCle at https://www.iso.org/obp

4 Structure of this document

Clause 5 refers to the privacy information management system as defined in EN ISO/IEC 27701, and specifies additional requirements and refinements of requirements.

Clause 6 specifies the requirements for PII processing operations as part of products, processes, or services; these are requirements for the organization to implement specific controls from Annexes A, B, C and related guidance.

Annex A refers to the ISO/IEC 27001 Annex A controls.

Annex B refers to the EN ISO/IEC 27701 Annex A controls for PII controllers.

Annex C refers to the EN ISO/IEC 27701 Annex B controls for PII processors.

The informative Annex D provides a model for combining certifications governed by ISO/IEC 17021 and ISO/IEC 17065. Finally, Annex E presents the relationship between this document and EU 2016/679 GDPR.

5 Privacy information management system for PII processing operations

The organization shall establish, implement, maintain, and continually improve a PIMS as defined in EN ISO/IEC 27701.

The organization shall determine the PII processing operations within the scope of the management system (EN ISO/IEC 27701, 5.2.3).

EN ISO/IEC 27701:2021, 5.2.3 is refined as follows:

When determining this scope, the organization shall consider interfaces and dependencies between PII processing activities internal and external to the organization.

EN ISO/IEC 27001:2013, 6.1.3 c) is refined as follows:

The controls determined in ISO/IEC 27001:2013 6.1.3 b) shall be compared with the controls in Annex A, Annex B and/or Annex C to verify that no necessary controls have been omitted.

When assessing the applicability of control objectives and controls from Annex A for the treatment of risks, the control objectives and controls shall be considered in the context of both risks to information security as well as risks related to the processing of PII, including risks to PII principals.

EN ISO/IEC 27001:2013, 6.1.3 d) is refined as follows:

Produce a Statement of Applicability that contains:

— the necessary controls [see ISO/IEC 27001:2013, 6.1.3 b) and c) as refined Cove];

— justification for their inclusion;

— whether the necessary controls are implemented or not; and

— the justification for excluding any of the controls in Annex A, and in Annex B and/or Annex C according to the organization's determination of its role (see EN ISO/IEC 27701, 5.2.1).

Annexes A, B, C specify which controls that the organization shall implement, depending on the role of the organization. Therefore, these controls cannot be excluded.

6 Requirement for PII processing operations

For all PII processing operations as determined in Clause 5, the organization shall implement the controls required per Annexes A, B, C depending on the role of the organization (see ISO/IEC 27701, 5.2.1).

Annex A
(normative)

Information security *and privacy* controls

This annex is for use by all organizations, whatever their role is (acting as PII controller, PII processor, or both). This annex lists all the controls from ISO/IEC 27001:2013 Annex A and states where extensions to those controls are included in ISO/IEC 27701 and where refinements in a European context are applicable.

In Table A.1, references to ISO/IEC 27001:2013 controls are of two types:

— references to ISO/IEC 27001:2013 controls in the form "The control ISO/IEC 27001:2013 [control number A.x.y.z] applies." mean that the organization shall consider the applicability of the control according to its risk assessment (EN ISO/IEC 27701, 5.4.1.2) and risk treatment (EN ISO/IEC 27701, 5.4.1.3);

— requirements in the form "The organization shall implement control ISO/IEC 27001:2013 [control number A.x.y.z], following the additional guidance in ..."; mean that the organization shall implement all these controls following the related guidance to fulfil the general requirements in Clause 6 (in all cases, whatever the risk assessment and the risk treatment in the management system). Some controls of this type include additional refinements to the guidance of EN ISO/IEC 27701 in line with the scope of this document.

NOTE Clause numbers in this annex relate to the subclause numbers in ISO/IEC 27001:2013 Annex A.

Table A.1 — Control objectives and controls

A.5 Information security policies		
A.5.1 Management direction for information security		
Objective: To provide management direction and support for information security and privacy in accordance with business requirements and relevant laws and regulations.		
A.5.1.1	Policies for information security	The organization shall implement control ISO/IEC 27001 A.5.1.1, following the additional guidance in EN ISO/IEC 27701, 6.2.1.1.
A.5.1.2	Review of the policies for information security	The control ISO/IEC 27001 A.5.1.2 applies.

A.6 Organization of information security		
A.6.1 Internal organization		
Objective: To establish a management framework to initiate and control the implementation and operation of information security and privacy within the organization.		
A.6.1.1	Information security roles and responsibilities	The organization shall implement control ISO/IEC 27001 A.6.1.1, following the additional guidance in EN ISO/IEC 27701, 6.3.1.1, and these additional refinements: — The organization shall appoint a data protection officer (DPO), if the nature, scope and purposes of the processing requires it as per the applicable obligations, as the responsible person per EN ISO/IEC 27701:2021, 6.3.1.1. — The organization shall ensure that the DPO has sufficient resources to undertake his/her tasks, reports to the highest management level, is involved in all issues related to the protection of PII, and that contact details of the DPO are published and communicated to the supervisory authority and the PII principals. — The organization shall ensure that the DPO does not receive any instructions regarding the exercise of those tasks.
A.6.1.2	Segregation of duties	The organization shall implement control ISO/IEC 27001 A.6.1.2.
A.6.1.3	Contact with authorities	The control ISO/IEC 27001 A.6.1.3 applies.
A.6.1.4	Contact with special interest groups	The control ISO/IEC 27001 A.6.1.4 applies.
A.6.1.5	Information security in project management	The control ISO/IEC 27001 A.6.1.5 applies.
A.6.2 Mobile devices and teleworking		
Objective: To ensure the security and privacy of teleworking and use of mobile devices		
A.6.2.1	Mobile device policy	The organization shall implement control ISO/IEC 27001 A.6.2.1, following the additional guidance in EN ISO/IEC 27701, 6.3.2.1.
A.6.2.2	Teleworking	The control ISO/IEC 27001 A.6.2.2 applies.
A.7 Human resource security		
A.7.1 Prior to employment		
Objective: To ensure that employees and contractors understand their responsibilities and are suitCle for the roles for which they are considered.		
A.7.1.1	Screening	The control ISO/IEC 27001 A.7.1.1 applies.

A.7.1.2	Terms and conditions of employment	The control ISO/IEC 27001 A.7.1.2 applies.
A.7.2 During employment		
Objective: To ensure that employees and contractors are aware of and fulfil their information security and privacy responsibilities.		
A.7.2.1	Management responsibilities	The control ISO/IEC 27001 A.7.2.1 applies.
A.7.2.2	Information security awareness, education and training	The organization shall implement control ISO/IEC 27001 A.7.2.2, following the additional guidance in EN ISO/IEC 27701, 6.4.2.2.
A.7.2.3	Disciplinary process	The control ISO/IEC 27001 A.7.2.3 applies.
A.7.3 Termination and change of employment		
Objective: To protect the organization's interests as part of the process of changing or terminating employment.		
A.7.3.1	Termination or change of employment responsibilities	The control ISO/IEC 27001 A.7.3.1 applies.
A.8 Asset management		
A.8.1 Responsibility for assets		
Objective: To identify organizational assets and define appropriate protection responsibilities.		
A.8.1.1	Inventory of assets	The control ISO/IEC 27001 A.8.1.1 applies.
A.8.1.2	Ownership of assets	The control ISO/IEC 27001 A.8.1.2 applies.
A.8.1.3	Acceptable use of assets	The control ISO/IEC 27001 A.8.1.3 applies.
A.8.1.4	Return of assets	The control ISO/IEC 27001 A.8.1.4 applies.
A.8.2 Information classification		
Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.		
A.8.2.1	Classification of information	The organization shall implement control ISO/IEC 27001 A.8.2.1, following the additional guidance in EN ISO/IEC 27701, 6.5.2.1.
A.8.2.2	Labelling of information	The organization shall implement control ISO/IEC 27001 A.8.2.2, following the additional guidance in EN ISO/IEC 27701, 6.5.2.2.
A.8.2.3	Handling of assets	The control ISO/IEC 27001 A.8.2.3 applies.