ICS 35.020 SLOVENSKÁ TECHNICKÁ NORMA Apríl 2024

STN	**Systém riadenia bezpečnosti osobných údajov podľa ISO/IEC 27701 Spresnenia v európskom kontexte**	**STN EN 17926** 97 4177

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

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 03/24

Obsahuje: EN 17926:2023

138075

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 17926

November 2023

ICS 35.030

English version

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

Système de management de la protection de la vie privée conformément à l'EN ISO/IEC 27701 - Affinements relatifs au contexte européen

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

This European Standard was approved by CEN on 13 April 2023.

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. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists 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.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword 3

Introduction 4

1 Scope 5

2 Normative references 5

3 Terms and definitions 5

4 Structure of this document 5

5 Privacy information management system for PII processing operations 6

6 Requirement for PII processing operations 6

Annex A (normative) Information security and privacy controls 7

Annex B (normative) PIMS-specific reference control objectives and controls (PII Controllers) 19

Annex C (normative) PIMS-specific reference control objectives and controls (PII Processors) 26

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 29

Annex E (informative) Relationship between this European Standard and the General Data Protection Regulation 31

Bibliography 37

European foreword

This document (EN 17926:2023) has been prepared by Technical Committee CEN/CLC/JTC 13, “Cybersecurity and Data Protection”, the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by May 2024, and conflicting national standards shall be withdrawn at the latest by May 2024.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users’ national standards body. A complete listing of these bodies can be found on the CEN website.

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: 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 the United Kingdom.

Introduction

ISO/IEC 27701 specifies requirements and provides guidance for establishing, 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 applicable obligations.

Although ISO/IEC 27701 was written with the intention to be applicable 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 ISO/IEC 27701 in the context of the GDPR.

This document provides refinements to ISO/IEC 27701 in the application of controls and guidance in ISO/IEC 27701 specific to GDPR where necessary. 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). This is intended to be used by organizations in the GDPR context for the purpose of demonstrating compliance with their obligations. 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 ISO/IEC 27701 alone.

Thus 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 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 establishment 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 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 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 ISO/IEC 27701, which can be combined with certification requirements for 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.

ISO/IEC 27701:—,[1] *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)*

[1] Under preparation. Stage at time of publication: ISO/IEC DIS 27701:2023.