SLOVENSKI STANDARD
oSIST prEN 17926:2026

01-junij-2026

Sistem vodenja informacij o zasebnosti po EN ISO/IEC 27701 - Izboljšave v evropskem kontekstu

Privacy information management system per EN ISO/IEC 27701 – Refinements in European context

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

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

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

ICS:

35.030	Informacijska varnost	IT Security

oSIST prEN 17926:2026 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 17926

May 2026

ICS

English version

Privacy information management system per EN 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 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

This document (prEN 17926:2026) 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 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 EN 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 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 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. 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 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 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.

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 27701:2025, *Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance*

3 Terms and definitions

No terms and definitions are listed in this document.

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

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

— ISO Online browsing platform: available 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 27701:2025 Annex A controls.

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 27701:2025, 4.3).

EN ISO/IEC 27701:2025, 4.3 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 27701:2025 6.1.3 c) is refined as follows.

The information security programme at a minimum should address the following:

— information security risk management;

— policies for information security;

— organization of information security;

  — including segregation of duties

— human resources security;

— asset management;

— access control;

  — Access control policy, including :

  — Management of privileged access rights

    — Management of secret authentication information of users

    — Information access restriction

  — operations security;

    — including Separation of development, testing and operational environments

  — network security management;

  — development security;

  — supplier management;

    — including

      — Information and communication technology supply chain

      — Monitoring and review of supplier services

      — Managing changes to supplier services

    — incident management;

    — information security continuity;

    — information security reviews;

    — cryptography; and