DRAFT

ÖVE/ÖNORM EN 17926

Edition: 2022-12-15

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

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

Note:
Because of possible comments, the final version of this ÖVE/ÖNORM can differ from the present Draft Standard.
Please send your comments (in writing) by **2023-01-31** to Austrian Standards International.

Publisher and printing
OVE Austrian Electrotechnical Association
Austrian Standards International

Sale and distribution:
Austrian Standards International
Heinestraße 38, 1020 Vienna
E-Mail: service@austrian-standards.at
Internet: www.austrian-standards.at
Webshop: www.austrian-standards.at/webshop
Tel.: +43 1 213 00-300
Fax: +43 1 213 00-355

All electrotechnical standards are also available at:
OVE Austrian Electrotechnical Association
Eschenbachgasse 9, 1010 Vienna
E-Mail: verkauf@ove.at
Internet: www.ove.at
Webshop: www.ove.at/shop
Tel.: +43 1 587 63 73

ICS 35.030

Identical (IDT) with prEN 17926:2022-11

responsible Committee 001
Information technology

Explanations concerning this Draft Standard

The present Draft European Standard **EN 17926** has been submitted to CEN/CENELEC members for voting. In case of a positive result of the voting as required by CEN/CENELEC regulations, this Draft Standard will be published as EN.

Like all member organizations of CEN/CENELEC, Austrian Standards International is obliged to implement European Standards at national level and to withdraw conflicting standards.

Austrian Standards International herewith submits this Draft of a European Standard as Draft ÖNORM to public enquiry and information.

Since a German translation is not yet available, the English version of prEN 17926 is submitted to public enquiry and information, in order to observe the deadline fixed by CEN.

Comments on this Draft

Please find below some practical instructions intended to offer you and the responsible committee assistance for the processing of comments and proposals for modification:

Form	For your comments/proposals for change, please use the relevant form available from Internet. Download under http://www.austrian-standards.at/comments/ or use the Draft Standard Portal http://www.austrian-standards.at/standards-draft-portal/
Structure	Please use a new line for each comment. This facilitates the attribution of the comments received to the different clauses and chapters of the re-spective Draft.
Language	Please formulate technical comments on European Standards if possible **in English**, since English is the common working language of the most European standardizing bodies. **Editorial and/or linguistic** proposals for change/improvement of **German versions** of European Standards shall (certainly) be submitted in German.
Script/Format	Please use the script „**Arial**“ with **9 pt** font size. Please do not change the formats.
Dispatch	Comments can be submitted to the Draft Standards Portal (http://www.austrian-standards.at/standards-draft-portal/).
Aspects concerning patent law	The recipients of this Draft ÖVE/ÖNORM are requested to add information on any patent rights known to their comments and to provide supporting documentation, if available.

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

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.

A.8.3 Media handling		
Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.		
A.8.3.1	Management of removable media	The organization shall implement control ISO/IEC 27001 A.8.3.1, following the additional guidance in EN ISO/IEC 27701, 6.5.3.1.
A.8.3.2	Disposal of media	The organization shall implement control ISO/IEC 27001 A.8.3.2, following the additional guidance in EN ISO/IEC 27701, 6.5.3.2.
A.8.3.3	Physical media transfer	The organization shall implement control ISO/IEC 27001 A.8.3.3, following the additional guidance in EN ISO/IEC 27701, 6.5.3.3.
A.9 Access control		
A.9.1 Business requirements of access control		
Objective: To limit access to information and information processing facilities.		
A.9.1.1	Access control policy	The organization shall implement control ISO/IEC 27001 A.9.1.1.
A.9.1.2	Access to networks and network services	The control ISO/IEC 27001 A.9.1.2 applies.
A.9.2 User access management		
Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.		
A.9.2.1	User registration and de-registration	The organization shall implement control ISO/IEC 27001 A.9.2.1, following the additional guidance in EN ISO/IEC 27701, 6.6.2.1.
A.9.2.2	User access provisioning	The organization shall implement control ISO/IEC 27001 A.9.2.2, following the additional guidance in EN ISO/IEC 27701, 6.6.2.2.
A.9.2.3	Management of privileged access rights	The organization shall implement control ISO/IEC 27001 A.9.2.3.
A.9.2.4	Management of secret authentication information of users	The control ISO/IEC 27001 A.9.2.4 applies.
A.9.2.5	Review of user access rights	The organization shall implement control ISO/IEC 27001 A.9.2.5.
A.9.2.6	Removal or adjustment of access rights	The organization shall implement control ISO/IEC 27001 A.9.2.6.
A.9.3 User responsibilities		
Objective: To make users accountable for safeguarding their authentication information.		
A.9.3.1	Use of secret authentication information	The control ISO/IEC 27001 A.9.3.1 applies.

A.9.4 System and application control		
Objective: To prevent unauthorized access to systems and applications.		
A.9.4.1	Information access restriction	The organization shall implement control ISO/IEC 27001 A.9.4.1.
A.9.4.2	Secure log-on procedures	The organization shall implement control ISO/IEC 27001 A.9.4.2, following the additional guidance in EN ISO/IEC 27701, 6.6.2.2.
A.9.4.3	Password management system	The control ISO/IEC 27001 A.9.4.3 applies.
A.9.4.4	Use of privileged utility programs	The control ISO/IEC 27001 A.9.4.4 applies
A.9.4.5	Access control to program source code	The control ISO/IEC 27001 A.9.4.5 applies
A.10 Cryptography		
A.10.1 Cryptographic controls		
Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information		
A.10.1.1	Policy on the use of cryptographic controls	The organization shall implement control ISO/IEC 27001 A.10.1.1, following the additional guidance in EN ISO/IEC 27701, 6.7.1.1
A.10.1.2	Key management	The control ISO/IEC 27001 A.10.1.2 applies.
A.11 Physical and environmental security		
A.11.1 Secure areas		
Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.		
A.11.1.1	Physical security perimeter	The control ISO/IEC 27001 A.11.1.1 applies.
A.11.1.2	Physical entry controls	The control ISO/IEC 27001 A.11.1.2 applies.
A.11.1.3	Securing offices, rooms and facilities	The control ISO/IEC 27001 A.11.1.3 applies.
A.11.1.4	Protecting against external and environmental threats	The control ISO/IEC 27001 A.11.1.4 applies.
A.11.1.5	Working in secure areas	The control ISO/IEC 27001 A.11.1.5 applies.
A.11.1.6	Delivery and loading areas	The control ISO/IEC 27001 A.11.1.6 applies.

A.11.2 Equipment		
Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.		
A.11.2.1	Equipment siting and protection	The control ISO/IEC 27001 A.11.2.1 applies.
A.11.2.2	Supporting utilities	The control ISO/IEC 27001 A.11.2.2 applies.
A.11.2.3	Cabling security	The control ISO/IEC 27001 A.11.2.3 applies.
A.11.2.4	Equipment maintenance	The control ISO/IEC 27001 A.11.2.4 applies.
A.11.2.5	Removal of assets	The control ISO/IEC 27001 A.11.2.5 applies.
A.11.2.6	Security of equipment and assets off-premises	The control ISO/IEC 27001 A.11.2.6 applies.
A.11.2.7	Secure disposal or reuse of equipment	The organization shall implement control ISO/IEC 27001 A.11.2.7, following the additional guidance in EN ISO/IEC 27701, 6.8.2.7.
A.11.2.8	Unattended user equipment	The control ISO/IEC 27001 A.11.2.8 applies.
A.11.2.9	Clear desk and clear screen policy	The organization shall implement control ISO/IEC 27001 A.11.2.9, following the additional guidance in EN ISO/IEC 27701, 6.8.2.9.
A.12 Operations security		
A.12.1 Operational procedures and responsibilities		
Objective: To ensure correct and secure operations of information processing facilities.		
A.12.1.1	Documented operating procedures	The control ISO/IEC 27001 A.12.1.1 applies.
A.12.1.2	Change management	The control ISO/IEC 27001 A.12.1.2 applies.
A.12.1.3	Capacity management	The control ISO/IEC 27001 A.12.1.3 applies.
A.12.1.4	Separation of development, testing and operational environments	The organization shall implement control ISO/IEC 27001 A.12.1.4.
A.12.2 Protection from malware		
Objective: To ensure that information and information processing facilities are protected against malware.		
A.12.2.1	Controls against malware	The control ISO/IEC 27001 A.12.2.1 applies.
A.12.3 Backup		
Objective: To protect against loss of data.		
A.12.3.1	Information backup	The organization shall implement control ISO/IEC 27001 A.12.3.1, following the additional guidance in EN ISO/IEC 27701, 6.7.1.1.

A.12.4 Logging and monitoring		
Objective: To record events and generate evidence.		
A.12.4.1	Event logging	The organization shall implement control ISO/IEC 27001 A.12.4.1, following the additional guidance in EN ISO/IEC 27701, 6.9.4.1.
A.12.4.2	Protection of log information	The organization shall implement control ISO/IEC 27001 A.12.4.2, following the additional guidance in EN ISO/IEC 27701, 6.9.4.2.
A.12.4.3	Administrator and operator logs	The control ISO/IEC 27001 A.12.4.3 applies.
A.12.4.4	Clock synchronisation	The control ISO/IEC 27001 A.12.4.4 applies.
A.12.5 Control of operational software		
Objective: To ensure the integrity of operational systems.		
A.12.5.1	Installation of software on operational systems	The control ISO/IEC 27001 A.12.5.1 applies.
A.12.6 Technical vulnerability management		
Objective: To prevent exploitation of technical vulnerabilities.		
A.12.6.1	Management of technical vulnerabilities	The control ISO/IEC 27001 A.12.6.1 applies.
A.12.6.2	Restrictions on software installation	The control ISO/IEC 27001 A.12.6.2 applies.
A.12.7 Information systems audit considerations		
Objective: To minimize the impact of audit activities on operational systems.		
A.12.7.1	Information systems audit control	The control ISO/IEC 27001 A.12.7.1 applies.
A.13 Communications security		
A.13.1 Network security management		
Objective: To ensure the protection of information in networks and its supporting information processing facilities.		
A.13.1.1	Network controls	The control ISO/IEC 27001 A.13.1.1 applies.
A.13.1.2	Security of network services	The control ISO/IEC 27001 A.13.1.2 applies.
A.13.1.3	Segregation in networks	The control ISO/IEC 27001 A.13.1.3 applies.

A.13.2 Information transfer		
Objective: To maintain the security of information transferred within an organization and with any external entity.		
A.13.2.1	Information transfer policies and procedures	The organization shall implement control ISO/IEC 27001 A.13.2.1, following the additional guidance in EN ISO/IEC 27701, 6.10.2.1.
A.13.2.2	Agreements on information transfer	The control ISO/IEC 27001 A.13.2.2 applies.
A.13.2.3	Electronic messaging	The control ISO/IEC 27001 A.13.2.3 applies.
A.13.2.4	Confidentiality or nondisclosure agreements	The organization shall implement control ISO/IEC 27001 A.13.2.4, following the additional guidance in EN ISO/IEC 27701, 6.10.2.4.
A.14 System acquisition, development and maintenance		
A.14.1 Security requirements of information systems		
Objective: To ensure that information security and privacy is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.		
A.14.1.1	Information security requirements analysis and specification	The control ISO/IEC 27001 A.14.1.1 applies.
A.14.1.2	Securing application services on public networks	The organization shall implement control ISO/IEC 27001 A.14.1.2, following the additional guidance in EN ISO/IEC 27701, 6.11.1.2.
A.14.1.3	Protecting application services transactions	The control ISO/IEC 27001 A.14.1.3 applies.
A.14.2 Security in development and support processes		
Objective: To ensure that information security and privacy is designed and implemented within the development lifecycle of information systems.		
A.14.2.1	Secure development policy	The organization shall implement control ISO/IEC 27001 A.14.2.1, following the additional guidance in EN ISO/IEC 27701, 6.11.2.1.
A.14.2.2	System change control procedures	The control ISO/IEC 27001 A.14.2.2 applies.
A.14.2.3	Technical review of applications after operating platform changes	The control ISO/IEC 27001 A.14.2.3 applies.
A.14.2.4	Restrictions on changes to software packages	The control ISO/IEC 27001 A.14.2.4 applies.
A.14.2.5	Secure system engineering principle	The organization shall implement control ISO/IEC 27001 A.14.2.5, following the additional guidance in EN ISO/IEC 27701, 6.11.2.5.

A.14.2.6	Secure development environment	The control ISO/IEC 27001 A.14.2.6 applies.
A.14.2.7	Outsourced development	The organization shall implement control ISO/IEC 27001 A.14.2.7, following the additional guidance in EN ISO/IEC 27701, 6.11.2.7.
A.14.2.8	System security testing	The control ISO/IEC 27001 A.14.2.8 applies.
A.14.2.9	System acceptance testing	The control ISO/IEC 27001 A.14.2.9 applies.
A.14.3 Test data		
Objective: To ensure the protection of data used for testing.		
A.14.3.1	Protection of test data	The organization shall implement control ISO/IEC 27001 A.14.3.1, following the additional guidance in EN ISO/IEC 27701, 6.11.3.1.
A.15 Supplier relationships		
A.15.1 Information security in supplier relationships		
Objective: To ensure protection of the organization's assets that is accessible by suppliers.		
A.15.1.1	Information security policy for supplier relationships	The organization shall implement control ISO/IEC 27001 A.15.1.1.
A.15.1.2	Addressing security within supplier agreement	The organization shall implement control ISO/IEC 27001 A.15.1.2, following the additional guidance in EN ISO/IEC 27701, 6.12.1.2.
A.15.1.3	Information and communication technology supply chain	The organization shall implement control ISO/IEC 27001 A.15.1.3.
A.15.2 Supplier service delivery management		
Objective: To maintain an agreed level of information security and privacy, and service delivery in line with supplier agreements.		
A.15.2.1	Monitoring and review of supplier services	The organization shall implement control ISO/IEC 27001 A.15.2.1.
A.15.2.2	Managing changes to supplier services	The organization shall implement control ISO/IEC 27001 A.15.2.2.

A.16 Information security incident management		
A.16.1 Management of information security incidents and improvements		
Objective: To ensure a consistent and effective approach to the management of information security and privacy incidents, including communication on security and privacy events and weaknesses.		
A.16.1.1	Responsibilities and procedures	The organization shall implement control ISO/IEC 27001 A.16.1.1, following the additional guidance in EN ISO/IEC 27701, 6.13.1.1 and these additional refinements: — The organization shall establish responsibilities and procedures for information security and privacy incident management which includes: o criteria for notifications to required parties (supervisory authority, customer, (joint) controller, PII principals); o timing of notifications; and o content of notifications. — The organization shall identify applicable obligations related to notifications and document alignment with those obligations (e.g. notification to a competent supervisory authority without undue delay, where feasible within 72 h after having become aware of it).
A.16.1.2	Reporting information security events	The control ISO/IEC 27001 A.16.1.2. applies.
A.16.1.3	Reporting information security weaknesses	The control ISO/IEC 27001 A.16.1.3. applies.
A.16.1.4	Assessment of and decision on information security events	The control ISO/IEC 27001 A.16.1.4 applies.

A.16.1.5	Response to information security incidents	The organization shall implement control ISO/IEC 27001 A.16.1.5, following the additional guidance in EN ISO/IEC 27701, 6.13.1.5 and these additional refinements: **Refinements for PII controllers:** The organization shall identify applicable obligations related to criteria for notifications to the supervisory authority, and/or to the PII principals, and document alignment with those obligations (for example criteria related to risks for the PII principals). Notifications shall contain as a minimum the following: — a contact point where more information can be obtained; — a description of and the likely consequences of the breach; — the number of individuals concerned as well as the number of records concerned; — measures taken or planned to be taken. **Refinements of PII processors:** In case of breach of PII, the PII processor shall notify the PII controller of the existence of the breach without undue delay after becoming aware of the breach so that the PII controller can take the appropriate actions.
A.16.1.6	Learning from information security incidents	The control ISO/IEC 27001 A.16.1.6. applies.
A.16.1.7	Collection of evidence	The control ISO/IEC 27001 A.16.1.7 applies.
A.17 Information security aspects of business continuity management		
A.17.1 Information security continuity		
Objective: Information security and privacy continuity shall be embedded in the organization's business continuity management systems.		
A.17.1.1	Planning information security continuity	The control ISO/IEC 27001 A.17.1.1 applies.
A.17.1.2	Implementing information security continuity	The control ISO/IEC 27001 A.17.1.2 applies.
A.17.1.3	Verify, review and evaluate information security continuity	The control ISO/IEC 27001 A.17.1.3 applies.

A.17.2 Redundancies		
Objective: To ensure availability of information processing facilities.		
A.17.2.1	Availability of information processing facilities	The control ISO/IEC 27001 A.17.2.1 applies.
A.18 Compliance		
A.18.1 Compliance with legal and contractual requirements		
Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and privacy and of any security and privacy requirements.		
A.18.1.1	Identification of applicable legislation and contractual requirements	The organization shall implement control ISO/IEC 27001 A.18.1.1, following the additional guidance in EN ISO/IEC 27701, 6.15.1.1.
A.18.1.2	Intellectual property rights	The control ISO/IEC 27001 A.18.1.2 applies.
A.18.1.3	Protection of records	The organization shall implement control ISO/IEC 27001 A.18.1.3, following the additional guidance in EN ISO/IEC 27701, 6.15.1.3.
A.18.1.4	Privacy and protection of personally identifiable information	The organization shall implement control ISO/IEC 27001 A.18.1.4.
A.18.1.5	Regulation of cryptographic control	The control ISO/IEC 27001 A.18.1.5 applies.
A.18.2 Information security reviews		
Objective: To ensure that information security and privacy is implemented and operated in accordance with the organizational policies and procedures.		
A.18.2.1	Independent review of information security	The organization shall implement control ISO/IEC 27001 A.18.2.1, following the additional guidance in EN ISO/IEC 27701, 6.15.2.1.
A.18.2.2	Compliance with security policies and standards	The control ISO/IEC 27001 A.18.2.2 applies.
A.18.2.3	Technical compliance review	The organization shall implement control ISO/IEC 27001 A.18.2.3, following the additional guidance in EN ISO/IEC 27701, 6.15.2.3.

Annex B
(normative)

PIMS-specific reference control objectives and controls (PII Controllers)

This annex is for use by organizations acting as PII controllers, with or without the use of PII processors. It refines EN ISO/IEC 27701:2021, Annex A.

In Table B.1, references to EN ISO/IEC 27701:2021 controls are in the form "The organization shall implement control EN ISO/IEC 27701 [control number A.x.y.z.] following the additional guidance in …"; it means that the organization shall implement all these controls following the related guidance to fulfil the general requirement in Clause 6 (in all cases, whatever the risk assessment and risk treatment).

NOTE Clause numbers in this annex relate to the subclause numbers in EN ISO/IEC 27701:2021, Annex A.

Table B.1 — Control objectives and controls

B.7.2 Conditions for collection and processing Objective: To determine and document that processing is lawful, with legal basis as per applicCle jurisdictions, and with clearly defined and legitimate purposes		
B.7.2.1	Identify and document purpose	The organization shall implement control EN ISO/IEC 27701 A.7.2.1, following the guidance in EN ISO/IEC 27701, 7.2.1.
B.7.2.2	Identify lawful basis	The organization shall implement control EN ISO/IEC 27701 A.7.2.2, following the guidance in EN ISO/IEC 27701, 7.2.2.
B.7.2.3	Determine when and how consent is to be obtained	The organization shall implement control EN ISO/IEC 27701 A.7.2.3, following the guidance in EN ISO/IEC 27701, 7.2.3.
B.7.2.4	Obtain and record consent	The organization shall implement control EN ISO/IEC 27701 A.7.2.4, following the guidance in EN ISO/IEC 27701, 7.2.4.

B.7.2.5	Privacy impact assessment	The organization shall implement control EN ISO/IEC 27701 A.7.2.5, following the guidance in EN ISO/IEC 27701, 7.2.5 and these additional refinements: — The organization shall identify processing operations which may result in high risks to the rights and freedoms of PII principals. — The organization shall undertake and document privacy impact assessments for high risk processing operations. — The organization shall involve the DPO or the persons in charge of privacy matters (where a DPO is not designated) in the review of high risk processing and in the carrying on the PIA. — The organization, where appropriate, shall seek the views of the PII principals or their representative, without prejudice to the protection of commercial or public interests or the security of processing operations. — When a PIA identifies processing that may result in high risks to PII principals, in the Csence of measures taken by the controller to mitigate residual risk, the organization shall consult the supervisory authorities prior to processing, and supply them with the details required. The PIA shall at the minimum: — describe systematically the envisaged processing operations and their purposes; — describe the legal basis of the processing activity; — assess the necessity and proportionality of the processing operations in relation to the purposes; — identify and assess risks to PII principals; — identify the measures that will address the risks to PII principals.
B.7.2.6	Contracts with PII processors	The organization shall implement control EN ISO/IEC 27701 A.7.2.6, following the guidance in EN ISO/IEC 27701, 7.2.6.

B.7.2.7	Joint PII controller	The organization shall implement control EN ISO/IEC 27701 A.7.2.7, following the guidance in EN ISO/IEC 27701, 7.2.7.
B.7.2.8	Records related to processing PII	The organization shall implement control EN ISO/IEC 27701 A.7.2.8, following the guidance in EN ISO/IEC 27701, 7.2.8.
B.7.3 Obligations to PII principals Objective: To ensure that PII principals are provided with appropriate information about the processing of their PII and to meet any other applicable obligations to PII principals related to the processing of their PII.		
B.7.3.1	Determining and fulfilling obligations to PII principals	The organization shall implement control EN ISO/IEC 27701 A.7.3.1, following the guidance in EN ISO/IEC 27701, 7.3.1.
B.7.3.2	Determining information for PII principals	The organization shall implement control EN ISO/IEC 27701 A.7.3.2, following the guidance in EN ISO/IEC 27701, 7.3.2.
B.7.3.3	Providing information to PII principals	The organization shall implement control EN ISO/IEC 27701 A.7.3.3, following the guidance in EN ISO/IEC 27701, 7.3.3.

B.7.3.4	Providing mechanism to modify or withdraw consent	The organization shall implement control EN ISO/IEC 27701 A.7.3.4, following the guidance in EN ISO/IEC 27701, 7.3.4, and these additional refinements: — The organization shall provide a mechanism for PII principals to be Cle to place restrictions on the processing of their PII: o during verification by the organization of the accuracy of the PII processed, if accuracy is contested by PII principal; o if the PII principal opposes the erasure of data collected under unlawful processing; o if the PII principal, in order to support a legal claim, requests the organization to keep PII that is no longer necessary for the processing; o during verification of the legitimate grounds of the organization for PII processing, if the PII principal objects to the processing. — Restricted PII shall be stored and used only under consent of PII principal or in specific lawful contexts (legal claims, protection of rights of a person, important public interest). — PII principal shall be informed by the organization before the restriction is lifted. — Restriction of processing shall in principle be ensured by technical measures, such as clear labelling of restricted PII.
B.7.3.5	Providing mechanism to object to PII processing	The organization shall implement control EN ISO/IEC 27701 A.7.3.5, following the guidance in EN ISO/IEC 27701, 7.3.5.
B.7.3.6	Access, correction and/or erasure	The organization shall implement control EN ISO/IEC 27701 A.7.3.6, following the guidance in EN ISO/IEC 27701, 7.3.6.
B.7.3.7	PII controllers' obligations to inform third parties	The organization shall implement control EN ISO/IEC 27701 A.7.3.7, following the guidance in EN ISO/IEC 27701, 7.3.7.
B.7.3.8	Providing copy of PII processed	The organization shall implement control EN ISO/IEC 27701 A.7.3.8, following the guidance in EN ISO/IEC 27701, 7.3.8.

B.7.3.9	Handling requests	The organization shall implement control EN ISO/IEC 27701 A.7.3.9, following the guidance in EN ISO/IEC 27701, 7.3.9.
B.7.3.10	Automated decision making	The organization shall implement control EN ISO/IEC 27701 A.7.3.10, following the guidance in EN ISO/IEC 27701, 7.3.10.
B.7.4 Privacy by design and by privacy default Objective: To ensure that processes and systems are designed such that the collection and processing (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.		
B.7.4.1	Limit collection	The organization shall implement control EN ISO/IEC 27701 A.7.4.1, following the guidance in EN ISO/IEC 27701, 7.4.1.
B.7.4.2	Limit processing	The organization shall implement control EN ISO/IEC 27701 A.7.4.2, following the guidance in EN ISO/IEC 27701, 7.4.2.
B.7.4.3	Accuracy and quality	The organization shall implement control EN ISO/IEC 27701 A.7.4.3, following the guidance in EN ISO/IEC 27701, 7.4.3.
B.7.4.4	PII minimization objectives	The organization shall implement control EN ISO/IEC 27701 A.7.4.4, following the guidance in EN ISO/IEC 27701, 7.4.4.
B.7.4.5	PII de-identification and deletion at the end of processing	The organization shall implement control EN ISO/IEC 27701 A.7.4.5, following the guidance in EN ISO/IEC 27701, 7.4.5.
B.7.4.6	Temporary files	The organization shall implement control EN ISO/IEC 27701 A.7.4.6, following the guidance in EN ISO/IEC 27701, 7.4.6.
B.7.4.7	Retention	The organization shall implement control EN ISO/IEC 27701 A.7.4.7, following the guidance in EN ISO/IEC 27701, 7.4.7.
B.7.4.8	Disposal	The organization shall implement control EN ISO/IEC 27701 A.7.4.8, following the guidance in EN ISO/IEC 27701, 7.4.8.
B.7.4.9	PII transmission controls	The organization shall implement control EN ISO/IEC 27701 A.7.4.9, following the guidance in EN ISO/IEC 27701, 7.4.9.
B.7.5 PII sharing, transfer and disclosure Objective: To determine whether and document when PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.		

B.7.5.1	Identify basis for PII transfer between jurisdictions	The organization shall implement control EN ISO/IEC 27701 A.7.5.1, following the guidance in EN ISO/IEC 27701, 7.5.1 and these additional refinements: — The organization shall identify and document the relevant basis for transfers of PII between jurisdictions, which can be permission from regulatory authorities to transfer PII to jurisdictions providing an adequate level of protection, or, in its absence, transfer tools containing "appropriate safeguards" to ensure that, overall, the PII transferred will benefit from a level of protection at least equivalent to the originating jurisdiction. o Transfer tools include standard data protection clauses, binding corporate rules, and codes of conduct or certification mechanisms recognized as transfer tools under the applicable legislation (e.g. in the European context the GDPR), and ad hoc contractual clauses. o If the legislation and practice of the third country to which PII is to be transferred does not offer to the PII transferred protection essentially equivalent to that provided in the jurisdiction from where it originates, the organization shall supplement the transfer tools and the safeguards they contain with "supplementary measures", i.e. contractual, technical and organizational measures to ensure the protection of PII being transferred, including security and confidentiality, equivalent to the level of protection provided in the jurisdiction from where it originates. The technical and organisational measures shall use techniques with due regard to the state of the art and in accordance with the risk involved, aiming at ensuring that the PII transferred are not accessible to the third country's public authorities. — If the organization receives notification (see C.8.5.1) or otherwise becomes aware that a subcontracted PII processor is no longer Cle to comply with the transfer tool it relies on, the organization shall identify appropriate measures to address the situation, if necessary,

		in consultation with the competent supervisory authority. o Such measures shall include "supplementary measures", i.e. contractual, technical and organizational measures adopted by the organization and/or the processor to ensure the protection of PII being transferred, including security and confidentiality, equivalent to the level of protection provided in the jurisdiction from where it originates. The technical and organisational measures shall use techniques, with due regard to the state of the art and in accordance with the risk involved, aiming at ensuring that the PII transferred are not accessible to the third country's public authorities. — The organization shall suspend the transfer if it considers that no appropriate safeguards can be ensured, or if so, instructed by the competent supervisory authority.
B.7.5.2	Countries and international organizations to which PII can be transferred	The organization shall implement control EN ISO/IEC 27701 A.7.5.2, following the guidance in EN ISO/IEC 27701, 7.5.2.
B.7.5.3	Records of transfer of PII	The organization shall implement control EN ISO/IEC 27701 A.7.5.3, following the guidance in EN ISO/IEC 27701, 7.5.3.
B.7.5.4	Records of PII disclosures to third parties	The organization shall implement control EN ISO/IEC 27701 A.7.5.4, following the guidance in EN ISO/IEC 27701, 7.5.4.

Annex C
(normative)

PIMS-specific reference control objectives and controls (PII Processors)

This annex is for use by organizations acting as PII processors, with or without the use of PII subcontractors. It refines EN ISO/IEC 27701:2021, Annex B.

In Table C.1, references to EN ISO/IEC 27701:2021 controls are in the form "The organization shall implement control EN ISO/IEC 27701 [control number A.x.y.z.] following the additional guidance in …"; it means that the organization shall implement all these controls following the related guidance to fulfil the general requirement in Clause 6, in all cases, regardless of the risk assessment and risk treatment.

NOTE Clause numbers in this annex relate to the subclause numbers in EN ISO/IEC 27701:2021, Annex B.

Table C.1 — Control objectives and controls

C.8.2 Conditions for collection and processing Objective: To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes		
C.8.2.1	Customer agreement	The organization shall implement control EN ISO/IEC 27701 B.8.2.1, following the guidance in EN ISO/IEC 27701, 8.2.1.
C.8.2.2	Organization's purposes	The organization shall implement control EN ISO/IEC 27701 B.8.2.2, following the guidance in EN ISO/IEC 27701, 8.2.2.
C.8.2.3	Marketing and advertising use	The organization shall implement control EN ISO/IEC 27701 B.8.2.3, following the guidance in EN ISO/IEC 27701, 8.2.3.
C.8.2.4	Infringing instruction	The organization shall implement control EN ISO/IEC 27701 B.8.2.4, following the guidance in EN ISO/IEC 27701, 8.2.4.
C.8.2.5	Customer obligations	The organization shall implement control EN ISO/IEC 27701 B.8.2.5, following the guidance in EN ISO/IEC 27701, 8.2.5.
C.8.2.6	Records related to processing PII	The organization shall implement control EN ISO/IEC 27701 B.8.2.6, following the guidance in EN ISO/IEC 27701, 8.2.6.
C.8.3 Obligations to PII principals Objective: To ensure that PII principals are provided with appropriate information about the processing of their PII and to meet any other applicable obligations to PII principals related to the processing of their PII.		
C.8.3.1	Obligations to PII principals	The organization shall implement control EN ISO/IEC 27701 B.8.3.1, following the guidance in EN ISO/IEC 27701, 8.3.1.

C.8.4 Privacy by design and by privacy default Objective: To ensure that processes and systems are designed such that the collection and processing (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.		
C.8.4.1	Temporary files	The organization shall implement control EN ISO/IEC 27701 B.8.4.1, following the guidance in EN ISO/IEC 27701, 8.4.1.
C.8.4.2	Return, transfer or disposal of PII	The organization shall implement control EN ISO/IEC 27701 B.8.4.2, following the guidance in EN ISO/IEC 27701, 8.4.2.
C.8.4.3	PII transmission controls	The organization shall implement control EN ISO/IEC 27701 B.8.4.3, following the guidance in EN ISO/IEC 27701, 8.4.3.
C.8.5 PII sharing, transfer and disclosure Objective: To determine whether and document when PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.		
C.8.5.1	Basis for PII transfer between jurisdictions	The organization shall implement control EN ISO/IEC 27701 B.8.5.1, following the guidance in EN ISO/IEC 27701, 8.5.1 and these additional refinements: — The organization shall inform the customer if, after agreeing to a transfer tool (see B.7.5.1), it has reason to believe that it is not Cle to comply with it due to legislation and practice of the jurisdictions involved. — Appropriate measures to address the situation shall include "supplementary measures" adopted by the customer and/or the organization, i.e. contractual, technical and organizational measures to ensure the protection of PII being transferred, including security and confidentiality, equivalent to the level of protection provided in the jurisdiction from where it originates. The technical and organisational measures shall use techniques, with due regard to the state of the art and in accordance with the risk involved, aiming at ensuring that the PII transferred are not accessible to the third country's public authorities in the countries involved.
C.8.5.2	Countries and international organizations to which PII can be transferred	The organization shall implement control EN ISO/IEC 27701 B.8.5.2, following the guidance in EN ISO/IEC 27701, 8.5.2.

C.8.5.3	Records of PII disclosures to third parties	The organization shall implement control EN ISO/IEC 27701 B.8.5.3, following the guidance in EN ISO/IEC 27701, 8.5.3.
C.8.5.4	Notification of PII disclosure requests	The organization shall implement control EN ISO/IEC 27701 B.8.5.4, following the guidance in EN ISO/IEC 27701, 8.5.4.
C.8.5.5	Legally binding PII disclosures	The organization shall implement control EN ISO/IEC 27701 B.8.5.5, following the guidance in EN ISO/IEC 27701, 8.5.5.
C.8.5.6	Disclosure of subcontractors used to process PII	The organization shall implement control EN ISO/IEC 27701 B.8.5.6, following the guidance in EN ISO/IEC 27701, 8.5.6.
C.8.5.7	Engagement of a subcontractor to process PII	The organization shall implement control EN ISO/IEC 27701 B.8.5.7, following the guidance in EN ISO/IEC 27701, 8.5.7.
C.8.5.8	Change of subcontractor to process PII	The organization shall implement control EN ISO/IEC 27701 B.8.5.8, following the guidance in EN ISO/IEC 27701, 8.5.8.

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

D.1 Introduction

ISO/IEC 17065 provides requirements for certification bodies certifying products, processes, and services.

Similarly, ISO/IEC 17021 provides requirements for certification bodies certifying management systems.

This annex discusses a potential model for bringing these two types of conformity assessment requirements together into a joint certification model based on EN ISO/IEC 27701 together with this document. The purpose of this annex is to outline the perspectives of this model, but a formalization of such a model is out of scope of this document.

D.2 Relationship between ISO/IEC 17021 and ISO/IEC 17065

ISO/IEC 17065 treats ISO/IEC 17021 as a normative reference and specifies that when the certification body operates a scheme for the assessment of a management system, in conjunction with the scheme for products, process and service certification, it shall meet the requirements of ISO/IEC 17021. (ISO/IEC 17065 Clause 6.2.1 and Clause 7.1.1).

D.3 Possibility of certification schemes per ISO/IEC 17067 for non-tangible products, processes, and services, requiring the operation of a management system

ISO/IEC 17067 describes the fundamentals of product certification and guidelines for product certification schemes. It specifies several types of certification schemes for products, some of which are purely focused on products themselves. However, types 5 and 6 specify a combination of management system auditing in conjunction with product (type 5) or service/process (type 6) requirements testing.

Therefore ISO/IEC 17067 type 5 or type 6 are the suitable scheme types to use, when the scheme requires the operation of a management system such as ISO/IEC 27701 for certification of products or services.

For non-tangible products and services, ISO/IEC 17067 type 6 is the suitable type and ISO/IEC 17028 give guidelines and examples of these schemes. Therefore, schemes for products and services which are about PII processing operations can be based on the guidelines from ISO/IEC 17028, and can include:

— the requirements against which the products and services are evaluated (ISO/IEC 17067:2013 6.5.1 b), ISO/IEC 17028 6.3 b));

— the requirements to operate a management system (ISO/IEC 17067:2013 6.5.1 d); ISO/IEC 17028 6.3 c));

— following this model, a scheme for certification against this document, for products and services which are about PII processing operations, will include:

  o the requirements against which PII processing operations are evaluated as stated in Clause 6 of this document;

  o the requirements to operate a management system as stated in Clause 5 of this document.

The following Figure B.1 illustrates a model for combination of management system certification governed by ISO/IEC 17021 with a non-tangible product-based certification governed by ISO/IEC 17065.

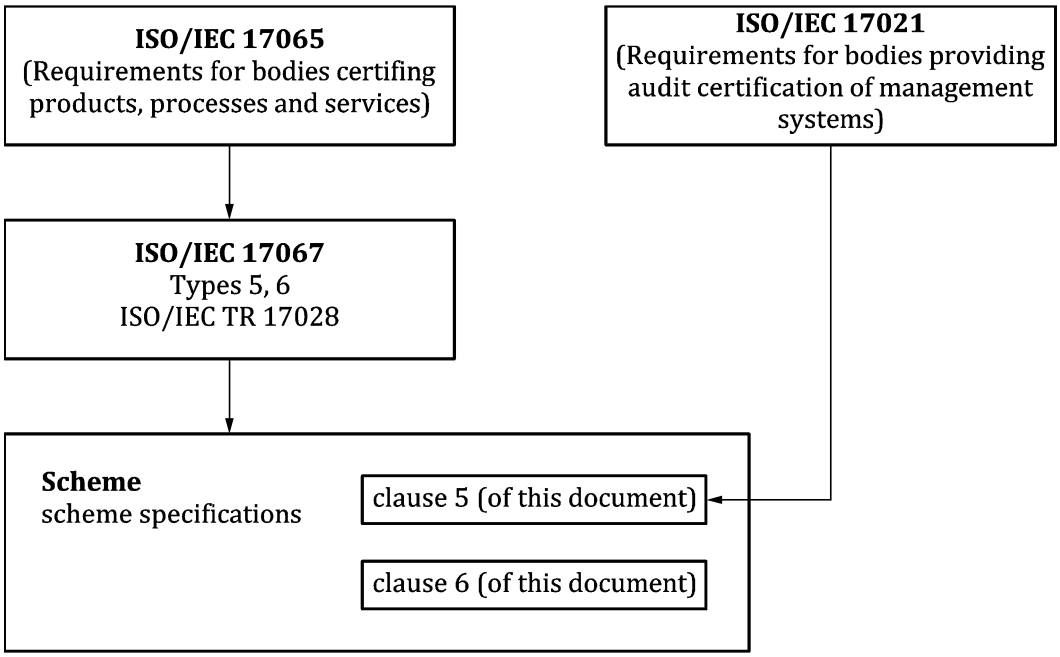

Figure D.1 — Joint certification model operated under ISO/IEC 17065 and ISO/IEC 17021-requirements

Annex E
(informative)

Relationship between this European Standard and the General Data Protection Regulation

This document has been prepared to support the application of EN ISO/IEC 27701 in the European context of the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC).

Annex D of EN ISO/IEC 27701 gives an indicative mapping between provisions of EN ISO/IEC 27701 and Articles of the General Data Protection Regulation, which these provisions are intended to support.

A given clause in this document which corresponds normatively to a clause in EN ISO/IEC 27701, can be mapped to the same GDPR article(s).

Table E.1 — Mapping of GDPR articles to this document

GDPR article	Subclause in this document
(1)-(4)	N/A
(5)(1)(a)	B.7.2.2, C.8.2.2
(5)(1)(b)	B.7.2.1, B.7.4.1, C.8.2.2
(5)(1)(c)	B.7.4.1, B.7.4.4, B.7.4.5, B.7.4.6, B.7.4.7, C.8.4.1
(5)(1)(d)	B.7.3.7, B.7.4.3
(5)(1)(e)	B.7.4.6
(5)(1)(f)	A.8.2.1, A.8.3.1, A.8.3.3, A.9.2.1, A.9.2.2, A.9.4.2, A.11.2.7, A.11.2.9, A.12.3.1, A.12.4.1, A.12.4.2, A.13.2.1, A.13.2.4, A.14.1.2, A.14.3.1, A.15.1.2, A.16.1.1, A.18.1.1, B.7.4.9, B.7.5.5, C.8.4.3
(5)(2)	A.18.1.3, B.7.2.6, B.7.2.8
(6)(1)(a)-(6)(1)(f), (6)(2), (6)(3), (6)(4)(a)-(6)(4)(d)	B.7.2.2
(6)(4)(e)	B.7.2.2, B.7.4.6
(7)(1), (7)(2)	B.7.2.4
(7)(3)	B.7.3.4
(7)(4)	C.*8.2.3*
(8)(1), (8)(2)	B.7.2.3
(8)(3)	B.7.2.2
(9)(1)	B.7.2.2
(9)(2)(a)	B.7.2.4

GDPR article	Subclause in this document
(9)(2)(b)-(9)(2)(j), (9)(3), (9)(4)	B.7.2.2
(10)	B.7.2.2
(11)(1)	B.7.4.6
(11)(2)	B.7.3.2, 7.3.3
(12)(1)	B.7.3.3
(12)(2)	B.7.3.1
(12)(3)-(12)(6)	B.7.3.9
(12)(7), (12)(8)	B.7.3.3
(13)(1)(a)	B.7.3.2
(13)(1)(b)-(13)(1)(f)	B.7.3.2
(13)(2)(a)	B.7.4.8
(13)(2)(b)	B.7.3.5, B.7.3.7, B.7.3.8
(13)(2)(c)	B.7.3.2, B.7.3.4
(13)(2)(d), (13)(2)(e)	B.7.3.2
(13)(2)(f)	B.7.3.10
(13)(3)	B.7.3.2, B.7.3.3
(13)(4)	B.7.3.2
(14)(1)(a)-(14)(1)(f)	B.7.3.2
(14)(2)(a)	B.7.4.8
(14)(2)(b)	B.7.3.2
(14)(2)(c)	B.7.3.5, B.7.3.7, B.7.3.8
(14)(2)(d)	B.7.3.4
(14)(2)(e), (14)(2)(f)	B.7.3.2
(14)(2)(g)	B.7.3.10
(14)(3)(a)-(14)(3)(c), (14)(4), (14)(5)(a)-(14)(5)(d)	B.7.3.2
(15)(1)(a)-(15)(1)(g)	B.7.3.2, B.7.3.3, B.7.3.9
(15)(1)(h)	B.7.3.2, B.7.3.3, B.7.3.9, B.7.3.10
(15)(2)	B.7.3.2, B.7.5.1, B.7.5.2
(15)(3)	B.7.3.8, C.8.3.1
(15)(4)	B.7.3.8
(16)	B.7.3.7
(17)(1)(a)-(17)(1)(f)	B.7.3.7
(17)(2)	B.7.3.7, C.8.3.1

GDPR article	Subclause in this document
(17)(3)(a)-(17)(3)(e)	B.7.2.2
(18)(1)(a)-(18)(1)(d)	B.7.3.4
(18)(2)	B.7.2.2
(18)(3)	B.7.3.2
(19)	B.7.3.6
(20)(1)–(20)(4)	B.7.3.8
(21)(1)–(21)(3)	B.7.3.5
(21)(4)	B.7.3.2, B.7.3.3
(21)(5), (21)(6)	B.7.3.5
(22)(1)	B.7.3.10
(22)(2)(a)-(22)(2)(c)	B.7.2.2
(22)(3)	B.7.3.10
(22)(4)	B.7.2.2
(23)(1)(a)-(23)(1)(j), (23)(2)(a)-(23)(2)(h)	5 (→ ISO/IEC 27001, 5.2.1)
(24)(1)	B.7.2.8
(24)(2)	A.5.1.1, A.18.1.3
(24)(3)	5 (→ ISO/IEC 27001, 5.2.1)
(25)(1)	A.14.2.5
(25)(2)	B.7.4.2
(25)(3)	5 (→ ISO/IEC 27001, 5.2.1)
(26)(1)–(26)(3)	B.7.2.7
(27)(1), (27)(2)(a)- (27)(2)(b), (27)(3)–(27)(5)	A.6.1.1
(28)(1)	A.15.1.2, A.18.1.1
(28)(2)	C.8.5.6, C.8.5.7, C.8.5.8
(28)(3)(a)	A.15.1.2, A.18.1.1, C.8.2.2, C.8.5.4
(28)(3)(b)	A.13.2.4, A.15.1.2, A.18.1.1
(28)(3)(c)	A.15.1.2, A.18.1.1
(28)(3)(d)	A.15.1.2, A.18.1.1, C.8.5.7
(28)(3)(e)	A.15.1.2, A.18.1.1, B.7.2.6, C.8.2.1, C.8.3.1
(28)(3)(f)	A.15.1.2, A.18.1.1, C.8.2.1
(28)(3)(g)	A.15.1.2, A.18.1.1, C.8.4.2
(28)(3)(h)	A.15.1.2, A.18.1.1, C.8.2.4, C.8.2.5

GDPR article	Subclause in this document
(28)(4)	C.8.5.6
(28)(5)–(28)(8)	5 (→ ISO/IEC 27001, 5.2.1)
(28)(9)	B.7.2.6, C.8.2.1
(28)(10)	5 (→ ISO/IEC 27001, 5.2.1)
(29)	C.8.2.2
(30)(1)(a)-(30)(1)(c)	B.7.2.8
(30)(1)(d)	B.7.2.8, B.7.5.4, C.8.5.3
(30)(1)(e)	B.7.5.1, B.7.5.2, B.7.5.3
(30)(1)(f)	B.7.2.8, C.8.4.2
(30)(1)(g)	B.7.2.8
(30)(2)(a), (30)(2)(b)	C.8.2.6
(30)(2)(c)	C.8.5.2
(30)(2)(d)	A.15.1.2, A.18.1.1
(30)(3)-(30)(5)	B.7.2.8, C.8.2.6
(31)	5 (→ ISO/IEC 27001, 5.2.2)
(32)(1)(a)	A.8.3.1, A.8.3.3, A.10.1.1, A.14.1.2, B.7.4.6
(32)(1)(b)	5 (→ ISO/IEC 27001, 5.4.1.2), 5 (→ ISO/IEC 27001, 5.4.1.3), A.15.1.2, A.18.1.1
(32)(1)(c)	A.12.3.1
(32)(1)(d)	A.18.2.1, A.18.2.3
(32)(2)	5 (→ ISO/IEC 27001, 5.2.4), 5 (→ ISO/IEC 27001, 5.4.1.2), 5 (→ ISO/IEC 27001, ~~5.4.1.3~~), A.8.2.1, A.18.2.1, A.18.2.3
(32)(3)	5 (→ ISO/IEC 27001, 5.2.1)
(32)(4)	B.7.2.1, C.8.2.2
(33)(1)	A.16.1.1, A.16.1.5
(33)(2)	A.16.1.5
(33)(3)(a)-(33)(3)(d), (33)(4), (33)(5)	A.16.1.1, A.16.1.5
(34)(1), (34)(2)	A.16.1.1, A.16.1.5
(34)(3)(a)-(34)(3)(c), (34)(4)	A.16.1.1
(35)(1)	B.7.2.5, C.8.2.1
(35)(2), (35)(3)(a)-(35)(3)(c), (35)(4)- (35)(6), (35)(7)(a)-(35)(7)(d), (35)(8)	B.7.2.5
(35)(9)	5 (→ ISO/IEC 27001, 5.2.2), B.7.2.5

GDPR article	Subclause in this document
(35)(10), (35)(11)	B.7.2.5
(36)(1), (36)(2), (36)(3)(a)-(36)(3)(f), (36)(4), (36)(5)	5 (→ ISO/IEC 27001, 5.2.2), B.7.2.5
(37)(1)(a)-(37)(1)(c), (37)(2)-(37)(7)	A.6.1.1
(38)(1)-(38)(4)	A.6.1.1
(38)(5)	A.6.1.1, A.13.2.4
(38)(6)	A.6.1.1
(39)(1)(a)	A.6.1.1
(39)(1)(b)	A.6.1.1, 6.4.2.2
(39)(1)(c)-(39)(1)(e), (39)(2)	A.6.1.1
(40)(1), (40)(2)(a)-(40)(2)(k), (40)(3)- (40)(11)	5 (→ ISO/IEC 27001, 5.2.1)
(41)(1), (41)(2)(a)-(41)(2)(d), (41)(3)-(41)(6)	5 (→ ISO/IEC 27001, 5.2.1)
(42)(1)–(42)(8)	5 (→ ISO/IEC 27001, 5.2.1)
(43)(1)(a)-(43)(1)(b), (43)(2)(a)-(43)(2)(e), (43)(3)-(43)(9)	N/A
(44)	B.7.5.1, C.8.5.1
(45)(1), (45)(2)(a)- (45)(2)(c), (45)(3)- (45)(9)	B.7.5.1
(46)(1), (46)(2)(a)- (46)(2)(f), (46)(3)(a)- (46)(3)(b)	B.7.5.1, C.8.5.1
(46)(4), (46)(5)	B.7.5.1
(47)(1)(a)- (47)(1)(c), (47)(2)(a)- (47)(2)(n)	B.7.5.1
(48)	B.7.5.1, C.8.5.1, C.8.5.5
(49)(1)(a)- (49)(1)(g), (49)(2)-(49)(6)	B.7.5.1, C.8.5.1
(50)–(99)	N/A

Requirements from this document are intended to be part of certification criteria as per GDPR article 42. Other criteria, such as criteria related to certification schemes, including requirements for accreditation of certifications bodies, are not covered in this document.

In addition to this document, a certification mechanism suitable for GDPR article 42 will also encompass requirements for a certification scheme.

If the accreditation mechanism is, as per GDPR article 43 (1) b, in accordance with ISO/IEC 17065, a scheme of the “type 5” or “type 6” as defined in ISO/IEC 17067 can be used (see Annex B for such certification model).

Bibliography

[1] EDPB Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679

[2] ISO/IEC 17065, *Conformity assessment — Requirements for bodies certifying products, processes and services*

[3] ISO/IEC 17021, *Conformity assessment — Requirements for bodies providing audit and certification of management systems*