BS EN ISO/IEC 27701:2021

BSI Standards Publication

Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27701:2021

National foreword

This British Standard is the UK implementation of EN ISO/IEC 27701:2021. It is identical to ISO/IEC 27701:2019. It supersedes BS ISO/IEC 27701:2019, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/5, Identity Management and Privacy Technologies.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2021
Published by BSI Standards Limited 2021

ISBN 978 0 539 15799 4

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2019.

Amendments/corrigenda issued since publication

Date	Text affected
31 May 2021	This corrigendum renumbers BS ISO/IEC 27701:2019 as BS EN ISO/IEC 27701:2021

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27701:2021

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 27701

April 2021

ICS 35.030

English version

Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines (ISO/IEC 27701:2019)

Techniques de sécurité - Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée - Exigences et lignes directrices (ISO/IEC 27701:2019)

Sicherheitstechniken - Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz - Anforderungen und Richtlinien (ISO/IEC 27701:2019)

This European Standard was approved by CEN on 12 April 2021.

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, Turkey and United Kingdom.

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

© 2021 CEN/CENELEC All rights of exploitation in any form and by any means reserved worldwide for CEN national Members and for CENELEC Members.

Ref. No. EN ISO/IEC 27701:2021 E

AVA Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27701:2021

European foreword

The text of ISO/IEC 27701:2019 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 27701:2021 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 October 2021, and conflicting national standards shall be withdrawn at the latest by October 2021.

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.

According to the CEN-CENELEC Internal Regulations, the national standards organizations 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, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27701:2019 has been approved by CEN as EN ISO/IEC 27701:2021 without any modification.

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27701:2021

Contents

Page

Foreword ... **vi**
Introduction ... **vii**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms, definitions and abbreviations ... **1**
4 General ... **2**
4.1 Structure of this document ... 2
4.2 Application of ISO/IEC 27001:2013 requirements ... 2
4.3 Application of ISO/IEC 27002:2013 guidelines ... 3
4.4 Customer ... 4
5 PIMS-specific requirements related to ISO/IEC 27001 ... **4**
5.1 General ... 4
5.2 Context of the organization ... 4
5.2.1 Understanding the organization and its context ... 4
5.2.2 Understanding the needs and expectations of interested parties ... 5
5.2.3 Determining the scope of the information security management system ... 5
5.2.4 Information security management system ... 5
5.3 Leadership ... 5
5.3.1 Leadership and commitment ... 5
5.3.2 Policy ... 5
5.3.3 Organizational roles, responsibilities and authorities ... 5
5.4 Planning ... 6
5.4.1 Actions to address risks and opportunities ... 6
5.4.2 Information security objectives and planning to achieve them ... 7
5.5 Support ... 7
5.5.1 Resources ... 7
5.5.2 Competence ... 7
5.5.3 Awareness ... 7
5.5.4 Communication ... 7
5.5.5 Documented information ... 7
5.6 Operation ... 7
5.6.1 Operational planning and control ... 7
5.6.2 Information security risk assessment ... 7
5.6.3 Information security risk treatment ... 7
5.7 Performance evaluation ... 8
5.7.1 Monitoring, measurement, analysis and evaluation ... 8
5.7.2 Internal audit ... 8
5.7.3 Management review ... 8
5.8 Improvement ... 8
5.8.1 Nonconformity and corrective action ... 8
5.8.2 Continual improvement ... 8
6 PIMS-specific guidance related to ISO/IEC 27002 ... **8**
6.1 General ... 8
6.2 Information security policies ... 8
6.2.1 Management direction for information security ... 8
6.3 Organization of information security ... 9
6.3.1 Internal organization ... 9
6.3.2 Mobile devices and teleworking ... 10
6.4 Human resource security ... 10
6.4.1 Prior to employment ... 10
6.4.2 During employment ... 10
6.4.3 Termination and change of employment ... 11

© ISO/IEC 2019 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021

6.5 Asset management ... 11
6.5.1 Responsibility for assets ... 11
6.5.2 Information classification ... 11
6.5.3 Media handling ... 12
6.6 Access control ... 13
6.6.1 Business requirements of access control ... 13
6.6.2 User access management ... 13
6.6.3 User responsibilities ... 14
6.6.4 System and application access control ... 14
6.7 Cryptography ... 15
6.7.1 Cryptographic controls ... 15
6.8 Physical and environmental security ... 15
6.8.1 Secure areas ... 15
6.8.2 Equipment ... 16
6.9 Operations security ... 17
6.9.1 Operational procedures and responsibilities ... 17
6.9.2 Protection from malware ... 18
6.9.3 Backup ... 18
6.9.4 Logging and monitoring ... 18
6.9.5 Control of operational software ... 19
6.9.6 Technical vulnerability management ... 20
6.9.7 Information systems audit considerations ... 20
6.10 Communications security ... 20
6.10.1 Network security management ... 20
6.10.2 Information transfer ... 20
6.11 Systems acquisition, development and maintenance ... 21
6.11.1 Security requirements of information systems ... 21
6.11.2 Security in development and support processes ... 21
6.11.3 Test data ... 23
6.12 Supplier relationships ... 23
6.12.1 Information security in supplier relationships ... 23
6.12.2 Supplier service delivery management ... 24
6.13 Information security incident management ... 24
6.13.1 Management of information security incidents and improvements ... 24
6.14 Information security aspects of business continuity management ... 27
6.14.1 Information security continuity ... 27
6.14.2 Redundancies ... 27
6.15 Compliance ... 27
6.15.1 Compliance with legal and contractual requirements ... 27
6.15.2 Information security reviews ... 28

7 Additional ISO/IEC 27002 guidance for PII controllers ... 29
7.1 General ... 29
7.2 Conditions for collection and processing ... 29
7.2.1 Identify and document purpose ... 29
7.2.2 Identify lawful basis ... 29
7.2.3 Determine when and how consent is to be obtained ... 30
7.2.4 Obtain and record consent ... 30
7.2.5 Privacy impact assessment ... 31
7.2.6 Contracts with PII processors ... 31
7.2.7 Joint PII controller ... 32
7.2.8 Records related to processing PII ... 32
7.3 Obligations to PII principals ... 33
7.3.1 Determining and fulfilling obligations to PII principals ... 33
7.3.2 Determining information for PII principals ... 33
7.3.3 Providing information to PII principals ... 34
7.3.4 Providing mechanism to modify or withdraw consent ... 34
7.3.5 Providing mechanism to object to PII processing ... 35
7.3.6 Access, correction and/or erasure ... 35

AVA Documents
Document Sharing Hub

© ISO/IEC 2019 – All rights reserved

Full document details: BS EN ISO/IEC 27701:2021

7.3.7 PII controllers' obligations to inform third parties 36
7.3.8 Providing copy of PII processed 36
7.3.9 Handling requests 37
7.3.10 Automated decision making 37
7.4 Privacy by design and privacy by default 38
7.4.1 Limit collection 38
7.4.2 Limit processing 38
7.4.3 Accuracy and quality 38
7.4.4 PII minimization objectives 39
7.4.5 PII de-identification and deletion at the end of processing 39
7.4.6 Temporary files 39
7.4.7 Retention 40
7.4.8 Disposal 40
7.4.9 PII transmission controls 40
7.5 PII sharing, transfer, and disclosure 41
7.5.1 Identify basis for PII transfer between jurisdictions 41
7.5.2 Countries and international organizations to which PII can be transferred 41
7.5.3 Records of transfer of PII 41
7.5.4 Records of PII disclosure to third parties 42

8 Additional ISO/IEC 27002 guidance for PII processors 42
8.1 General 42
8.2 Conditions for collection and processing 42
8.2.1 Customer agreement 42
8.2.2 Organization's purposes 43
8.2.3 Marketing and advertising use 43
8.2.4 Infringing instruction 43
8.2.5 Customer obligations 43
8.2.6 Records related to processing PII 44
8.3 Obligations to PII principals 44
8.3.1 Obligations to PII principals 44
8.4 Privacy by design and privacy by default 44
8.4.1 Temporary files 44
8.4.2 Return, transfer or disposal of PII 45
8.4.3 PII transmission controls 45
8.5 PII sharing, transfer, and disclosure 46
8.5.1 Basis for PII transfer between jurisdictions 46
8.5.2 Countries and international organizations to which PII can be transferred 46
8.5.3 Records of PII disclosure to third parties 47
8.5.4 Notification of PII disclosure requests 47
8.5.5 Legally binding PII disclosures 47
8.5.6 Disclosure of subcontractors used to process PII 47
8.5.7 Engagement of a subcontractor to process PII 48
8.5.8 Change of subcontractor to process PII 48

Annex A (normative) **PIMS-specific reference control objectives and controls (PII Controllers) 49**

Annex B (normative) **PIMS-specific reference control objectives and controls (PII Processors) 53**

Annex C (informative) **Mapping to ISO/IEC 29100 56**

Annex D (informative) **Mapping to the General Data Protection Regulation 58**

Annex E (informative) **Mapping to ISO/IEC 27018 and ISO/IEC 29151 61**

Annex F (informative) **How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002 64**

Bibliography 66

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021

Introduction

0.1 General

Almost every organization processes Personally Identifiable Information (PII). Further, the quantity and types of PII processed is increasing, as is the number of situations where an organization needs to cooperate with other organizations regarding the processing of PII. Protection of privacy in the context of the processing of PII is a societal need, as well as the topic of dedicated legislation and/or regulation all over the world.

The Information Security Management System (ISMS) defined in ISO/IEC 27001 is designed to permit the addition of sector specific requirements, without the need to develop a new Management System. ISO Management System standards, including the sector specific ones, are designed to be able to be implemented either separately or as a combined Management System.

Requirements and guidance for PII protection vary depending on the context of the organization, in particular where national legislation and/or regulation exist. ISO/IEC 27001 requires that this context be understood and taken into account. This document includes mapping to:

— the privacy framework and principles defined in ISO/IEC 29100;

— ISO/IEC 27018;

— ISO/IEC 29151; and

— the EU General Data Protection Regulation.

However, these can need to be interpreted to take into account local legislation and/or regulation.

This document can be used by PII controllers (including those that are joint PII controllers) and PII processors (including those using subcontracted PII processors and those processing PII as subcontractors to PII processors).

An organization complying with the requirements in this document will generate documentary evidence of how it handles the processing of PII. Such evidence can be used to facilitate agreements with business partners where the processing of PII is mutually relevant. This can also assist in relationships with other stakeholders. The use of this document in conjunction with ISO/IEC 27001 can, if desired, provide independent verification of this evidence.

This document was initially developed as ISO/IEC 27552.

0.2 Compatibility with other management system standards

This document applies the framework developed by ISO to improve alignment among its Management System Standards.

This document enables an organization to align or integrate its PIMS with the requirements of other Management System standards.

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021

Documents
Document Sharing Hub

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

1 Scope

This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.

This document specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.

This document is applicable to 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.

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 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

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

3 Terms, definitions and abbreviations

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and ISO/IEC 29100 and the following apply.

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

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

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

3.1
joint PII controller
PII controller that determine the purposes and means of the processing of PII jointly with one or more other PII controllers

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021

3.2
privacy information management system
PIMS
information security management system which addresses the protection of privacy as potentially affected by the processing of PII

4 General

4.1 Structure of this document

This is a sector-specific document related to ISO/IEC 27001:2013 and to ISO/IEC 27002:2013.

This document focuses on PIMS-specific requirements. Compliance with this document is based on adherence to these requirements and with the requirements in ISO/IEC 27001:2013. This document extends the requirements of ISO/IEC 27001:2013 to take into account the protection of privacy of PII principals as potentially affected by the processing of PII, in addition to information security. For a better understanding, implementation guidance and other information regarding the requirements is included.

Clause 5 gives PIMS-specific requirements and other information regarding the information security requirements in ISO/IEC 27001 appropriate to an organization acting as either a PII controller or a PII processor.

NOTE 1 For completeness, Clause 5 contains a subclause for each of the clauses containing requirements in ISO/IEC 27001:2013, even in cases where there are no PIMS-specific requirements or other information.

Clause 6 gives PIMS-specific guidance and other information regarding the information security controls in ISO/IEC 27002 and PIMS-specific guidance for an organization acting as either a PII controller or a PII processor.

NOTE 2 For completeness, Clause 6 contains a subclause for each of the clauses containing objectives or controls in ISO/IEC 27002:2013, even in cases where there is no PIMS-specific guidance or other information.

Clause 7 gives additional ISO/IEC 27002 guidance for PII controllers, and Clause 8 gives additional ISO/IEC 27002 guidance for PII processors.

Annex A lists the PIMS-specific control objectives and controls for an organization acting as a PII controller, (whether it employs a PII processor or not, and whether acting jointly with another PII controller or not).

Annex B lists the PIMS-specific control objectives and controls for an organization acting as a PII processor (whether it subcontracts the processing of PII to a separate PII processor or not, and including those processing PII as subcontractors to PII processors).

Annex C contains a mapping to ISO/IEC 29100.

Annex D contains a mapping of the controls in this document to the European Union General Data Protection Regulation.

Annex E contains a mapping to ISO/IEC 27018 and ISO/IEC 29151.

Annex F explains how ISO IEC 27001 and ISO/IEC 27002 are extended to the protection of privacy when processing PII.

4.2 Application of ISO/IEC 27001:2013 requirements

Table 1 gives the location of PIMS-specific requirements in this document in relation to ISO/IEC 27001.

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021

Table 1 — Location of PIMS-specific requirements and other information for implementing controls in ISO/IEC 27001:2013

Clause in ISO/IEC 27001:2013	Title	Subclause in this document	Remarks
4	Context of the organization	5.2	Additional requirements
5	Leadership	5.3	No PIMS-specific requirements
6	Planning	5.4	Additional requirements
7	Support	5.5	No PIMS-specific requirements
8	Operation	5.6	No PIMS-specific requirements
9	Performance evaluation	5.7	No PIMS-specific requirements
10	Improvement	5.8	No PIMS-specific requirements

NOTE The extended interpretation of "information security" according to 5.1 always applies even when there are no PIMS-specific requirements.

4.3 Application of ISO/IEC 27002:2013 guidelines

Table 2 gives the location of PIMS-specific guidance in this document in relation to ISO/IEC 27002.

Table 2 — Location of PIMS-specific guidance and other information for implementing controls in ISO/IEC 27002:2013

Clause in ISO/IEC 27002:2013	Title	Subclause in this document	Remarks
5	Information security policies	6.2	Additional guidance
6	Organization of information security	6.3	Additional guidance
7	Human resource security	6.4	Additional guidance
8	Asset management	6.5	Additional guidance
9	Access control	6.6	Additional guidance
10	Cryptography	6.7	Additional guidance
11	Physical and environmental security	6.8	Additional guidance
12	Operations security	6.9	Additional guidance
13	Communications security	6.10	Additional guidance
14	System acquisition, development and maintenance	6.11	Additional guidance
15	Supplier relationships	6.12	Additional guidance
16	Information security incident management	6.13	Additional guidance
17	Information security aspects of business continuity management.	6.14	No PIMS-specific guidance
18	Compliance	6.15	Additional guidance

NOTE The extended interpretation of "information security" according to 6.1 always applies even when there is no PIMS-specific guidance.

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021

4.4 Customer

Depending on the role of the organization (see 5.2.1), "customer" can be understood as either:

a) an organization who has a contract with a PII controller (e.g. the customer of the PII controller);

NOTE 1 This can be the case of an organization which is a joint controller.

NOTE 2 An individual person in a business to consumer relationship with an organization is referred to as a "PII principal" in this document.

b) a PII controller who has a contract with a PII processor (e.g. the customer of the PII processor); or

c) a PII processor who has a contract with a subcontractor for PII processing (e.g. the customer of the subcontracted PII sub-processor).

NOTE 3 Where “customer” is referred to in Clause 6, the related provisions can be applicable in contexts a), b), or c).

NOTE 4 Where “customer” is referred to in Clause 7 and Annex A, the relation provisions are applicable in context a).

NOTE 5 Where “customer” is referred to in Clause 8 and Annex B, the relation provisions can be applicable in contexts b) and/or c).

5 PIMS-specific requirements related to ISO/IEC 27001

5.1 General

The requirements of ISO/IEC 27001:2013 mentioning "information security" shall be extended to the protection of privacy as potentially affected by the processing of PII.

NOTE In practice, where "information security" is used in ISO/IEC 27001:2013, "information security and privacy” applies instead (see Annex F).

5.2 Context of the organization

5.2.1 Understanding the organization and its context

A requirement additional to ISO/IEC 27001:2013, 4.1 is:

The organization shall determine its role as a PII controller (including as a joint PII controller) and/or a PII processor.

The organization shall determine external and internal factors that are relevant to its context and that affect its ability to achieve the intended outcome(s) of its PIMS. For example, these can include:

— applicable privacy legislation;

— applicable regulations;

— applicable judicial decisions;

— applicable organizational context, governance, policies and procedures;

— applicable administrative decisions;

— applicable contractual requirements.

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021

Where the organization acts in both roles (e.g. a PII controller and a PII processor), separate roles shall be determined, each of which is the subject of a separate set of controls.

NOTE The role of the organization can be different for each instance of the processing of PII, since it depends on who determines the purposes and means of the processing.

5.2.2 Understanding the needs and expectations of interested parties

A requirement additional to ISO/IEC 27001:2013, 4.2 is:

The organization shall include among its interested parties (see ISO/IEC 27001:2013, 4.2), those parties having interests or responsibilities associated with the processing of PII, including the PII principals.

NOTE 1 Other interested parties can include customers (see 4.4), supervisory authorities, other PII controllers, PII processors and their subcontractors.

NOTE 2 Requirements relevant to the processing of PII can be determined by legal and regulatory requirements, by contractual obligations and by self-imposed organizational objectives. The privacy principles set out in ISO/IEC 29100 provide guidance concerning the processing of PII.

NOTE 3 As an element to demonstrate compliance to the organization's obligations, some interested parties can expect that the organization be in conformity with specific standards, such as the Management System specified in this document, and/or any relevant set of specifications. These parties can call for independently audited compliance to these standards.

5.2.3 Determining the scope of the information security management system

A requirement additional to ISO/IEC 27001:2013, 4.3 is:

When determining the scope of the PIMS, the organization shall include the processing of PII.

NOTE The determination of the scope of the PIMS can require revising the scope of the information security management system, because of the extended interpretation of "information security" according to 5.1.

5.2.4 Information security management system

A requirement additional to ISO/IEC 27001:2013, 4.4 is:

The organization shall establish, implement, maintain and continually improve a PIMS in accordance with the requirements of ISO/IEC 27001:2013 Clauses 4 to 10, extended by the requirements in Clause 5.

5.3 Leadership

5.3.1 Leadership and commitment

The requirements stated in ISO/IEC 27001:2013, 5.1 along with the interpretation specified in 5.1, apply.

5.3.2 Policy

The requirements stated in ISO/IEC 27001:2013, 5.2 along with the interpretation specified in 5.1, apply.

5.3.3 Organizational roles, responsibilities and authorities

The requirements stated in ISO/IEC 27001:2013, 5.3 along with the interpretation specified in 5.1, apply.

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021

5.4 Planning

5.4.1 Actions to address risks and opportunities

5.4.1.1 General

The requirements stated in ISO/IEC 27001:2013, 6.1.1 along with the interpretation specified in 5.1, apply.

5.4.1.2 Information security risk assessment

The requirements stated in ISO/IEC 27001:2013, 6.1.2 apply with the following refinements:

ISO/IEC 27001:2013, 6.1.2 c) 1) is refined as follows:

The organization shall apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability, within the scope of the PIMS.

The organization shall apply privacy risk assessment process to identify risks related to the processing of PII, within the scope of the PIMS.

The organization shall ensure throughout the risk assessment processes that the relationship between information security and PII protection is appropriately managed.

NOTE The organization can either apply an integrated information security and privacy risk assessment process or two separate ones for information security and the risks related to the processing of PII.

ISO/IEC 27001:2013, 6.1.2 d) 1) is refined as follows:

The organization shall assess the potential consequences for both the organization and PII principals that would result if the risks identified in ISO/IEC 27001:2013, 6.1.2 c) as refined above, were to materialize.

5.4.1.3 Information security risk treatment

The requirements stated in ISO/IEC 27001:2013, 6.1.3 apply with the following additions:

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 and/or Annex B and ISO/IEC 27001:2013, Annex A to verify that no necessary controls have been omitted.

When assessing the applicability of control objectives and controls from ISO/IEC 27001:2013 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.

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)];

— 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/or Annex B and ISO/IEC 27001:2013, Annex A according to the organization's determination of its role (see 5.2.1).

Not all the control objectives and controls listed in the annexes need to be included in a PIMS implementation. Justification for exclusion can include where the controls are not deemed necessary

© ISO/IEC 2019 – All rights reserved
AVA Documents Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021

by the risk assessment, and where they are not required by (or are subject to exceptions under) the legislation and/or regulation including those applicable to the PII principal.

5.4.2 Information security objectives and planning to achieve them

The requirements stated in ISO/IEC 27001:2013, 6.2 along with the interpretation specified in 5.1, apply.

5.5 Support

5.5.1 Resources

The requirements stated in ISO/IEC 27001:2013, 7.1 along with the interpretation specified in 5.1, apply.

5.5.2 Competence

The requirements stated in ISO/IEC 27001:2013, 7.2 along with the interpretation specified in 5.1, apply.

5.5.3 Awareness

The requirements stated in ISO/IEC 27001:2013, 7.3 along with the interpretation specified in 5.1, apply.

5.5.4 Communication

The requirements stated in ISO/IEC 27001:2013, 7.4 along with the interpretation specified in 5.1, apply.

5.5.5 Documented information

5.5.5.1 General

The requirements stated in ISO/IEC 27001:2013, 7.5.1 along with the interpretation specified in 5.1, apply.

5.5.5.2 Creating and updating

The requirements stated in ISO/IEC 27001:2013, 7.5.2 along with the interpretation specified in 5.1, apply.

5.5.5.3 Control of documented information

The requirements stated in ISO/IEC 27001:2013, 7.5.3 along with the interpretation specified in 5.1, apply.

5.6 Operation

5.6.1 Operational planning and control

The requirements stated in ISO/IEC 27001:2013, 8.1 along with the interpretation specified in 5.1, apply.

5.6.2 Information security risk assessment

The requirements stated in ISO/IEC 27001:2013, 8.2 along with the interpretation specified in 5.1, apply.

5.6.3 Information security risk treatment

The requirements stated in ISO/IEC 27001:2013, 8.3 along with the interpretation specified in 5.1, apply.

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021

5.7 Performance evaluation

5.7.1 Monitoring, measurement, analysis and evaluation

The requirements stated in ISO/IEC 27001:2013, 9.1 along with the interpretation specified in 5.1, apply.

5.7.2 Internal audit

The requirements stated in ISO/IEC 27001:2013, 9.2 along with the interpretation specified in 5.1, apply.

5.7.3 Management review

The requirements stated in ISO/IEC 27001:2013, 9.3 along with the interpretation specified in 5.1, apply.

5.8 Improvement

5.8.1 Nonconformity and corrective action

The requirements stated in ISO/IEC 27001:2013, 10.1 along with the interpretation specified in 5.1, apply.

5.8.2 Continual improvement

The requirements stated in ISO/IEC 27001:2013, 10.2 along with the interpretation specified in 5.1, apply.

6 PIMS-specific guidance related to ISO/IEC 27002

6.1 General

The guidelines in ISO/IEC 27002:2013 mentioning "information security" should be extended to the protection of privacy as potentially affected by the processing of PII.

NOTE 1 In practice, where "information security" is used in ISO/IEC 27002:2013, "information security and privacy" applies instead (see Annex F).

All control objectives and controls should be considered in the context of both risks to information security as well as risks to privacy related to the processing of PII.

NOTE 2 Unless otherwise stated by specific provisions in Clause 6, or determined by the organization according to applicable jurisdictions, the same guidance applies for PII controllers and PII processors.

6.2 Information security policies

6.2.1 Management direction for information security

6.2.1.1 Policies for information security

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 5.1.1 and the following additional guidance applies:

Additional implementation guidance for 5.1.1, Policies for information security, of ISO/IEC 27002:2013 is:

Either by the development of separate privacy policies, or by the augmentation of information security policies, the organization should produce a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and/or regulation and with the contractual terms agreed between the organization and its partners, its subcontractors and its

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021

applicable third parties (customers, suppliers etc.), which should clearly allocate responsibilities between them.

Additional other information for 5.1.1, Policies for information security, of ISO/IEC 27002:2013 is:

Any organization that processes PII, whether a PII controller or a PII processor, should consider applicable PII protection legislation and/or regulation during the development and maintenance of information security policies.

6.2.1.2 Review of the policies for information security

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 5.1.2 applies:

6.3 Organization of information security

6.3.1 Internal organization

6.3.1.1 Information security roles and responsibilities

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 6.1.1 and the following additional guidance applies:

Additional implementation guidance for 6.1.1, Information security roles and responsibilities, of ISO/IEC 27002:2013 is:

The organization should designate a point of contact for use by the customer regarding the processing of PII. When the organization is a PII controller, designate a point of contact for PII principals regarding the processing of their PII (see 7.3.2).

The organization should appoint one or more persons responsible for developing, implementing, maintaining and monitoring an organization-wide governance and privacy program, to ensure compliance with all applicable laws and regulations regarding the processing of PII.

The responsible person should, where appropriate:

— be independent and report directly to the appropriate management level of the organization in order to ensure effective management of privacy risks;

— be involved in the management of all issues which relate to the processing of PII;

— be expert in data protection legislation, regulation and practice;

— act as a contact point for supervisory authorities;

— inform top-level management and employees of the organization of their obligations with respect to the processing of PII;

— provide advice in respect of privacy impact assessments conducted by the organization.

NOTE Such a person is called a data protection officer in some jurisdictions, which define when such a position is required, along with their position and role. This position can be fulfilled by a staff member or outsourced.

6.3.1.2 Segregation of duties

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 6.1.2 applies.

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021

6.3.1.3 Contact with authorities

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 6.1.3 applies.

6.3.1.4 Contact with special interest groups

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 6.1.4 applies.

6.3.1.5 Information security in project management

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 6.1.5 applies.

6.3.2 Mobile devices and teleworking

6.3.2.1 Mobile device policy

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 6.2.1 and the following additional guidance applies.

Additional implementation guidance for 6.2.1, Mobile device policy, of ISO/IEC 27002:2013 is:

The organization should ensure that the use of mobile devices does not lead to a compromise of PII.

6.3.2.2 Teleworking

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 6.2.2 applies.

6.4 Human resource security

6.4.1 Prior to employment

6.4.1.1 Screening

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 7.1.1 applies.

6.4.1.2 Terms and conditions of employment

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 7.1.2 applies.

6.4.2 During employment

6.4.2.1 Management responsibilities

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 7.2.1 applies.

6.4.2.2 Information security awareness, education and training

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 7.2.2 and the following additional guidance applies:

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021

Additional implementation guidance for 7.2.2, Information security awareness, education and training, of ISO/IEC 27002:2013 is:

Measures should be put in place, including awareness of incident reporting, to ensure that relevant staff are aware of the possible consequences to the organization (e.g. legal consequences, loss of business and brand or reputational damage), to the staff member (e.g. disciplinary consequences) and to the PII principal (e.g. physical, material and emotional consequences) of breaching privacy or security rules and procedures, especially those addressing the handling of PII.

NOTE Such measures can include the use of appropriate periodic training for personnel having access to PII.

6.4.2.3 Disciplinary procedures

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 7.2.3 applies.

6.4.3 Termination and change of employment

6.4.3.1 Termination or change of employment responsibilities

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 7.3.1 applies.

6.5 Asset management

6.5.1 Responsibility for assets

6.5.1.1 Inventory of assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.1.1 applies.

6.5.1.2 Ownership of assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.1.2 applies.

6.5.1.3 Acceptable use of assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.1.3 applies.

6.5.1.4 Return of assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.1.4 applies.

6.5.2 Information classification

6.5.2.1 Classification of information

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.2.1 and the following additional guidance applies:

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021

Additional implementation guidance for 8.2.1, Classification of Information, of ISO/IEC 27002:2013 is:

The organization's information classification system should explicitly consider PII as part of the scheme it implements. Considering PII within the overall classification system is integral to understanding what PII the organization processes (e.g. type, special categories), where such PII is stored and the systems through which it can flow.

6.5.2.2 Labelling of information

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.2.2 and the following additional guidance applies.

Additional implementation guidance for 8.2.2, labelling of information, of ISO/IEC 27002:2013 is:

The organization should ensure that people under its control are made aware of the definition of PII and how to recognize information that is PII.

6.5.2.3 Handling of assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.2.3 applies.

6.5.3 Media handling

6.5.3.1 Management of removable media

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.3.1 and the following additional guidance applies:

Additional implementation guidance for 8.3.1, Management of removable media, of ISO/IEC 27002:2013 is:

The organization should document any use of removable media and/or devices for the storage of PII. Wherever feasible, the organization should use removable physical media and/or devices that permit encryption when storing PII. Unencrypted media should only be used where unavoidable, and in instances where unencrypted media and/or devices are used, the organization should implement procedures and compensating controls (e.g. tamper-evident packaging) to mitigate risks to the PII.

Additional other information for 8.3.1, Management of removable media, of ISO/IEC 27002:2013 is:

Removable media which is taken outside the physical confines of the organization is prone to loss, damage and inappropriate access. Encrypting removable media adds a level of protection for PII which reduces security and privacy risks should the removable media be compromised.

6.5.3.2 Disposal of media

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.3.2 and the following additional guidance applies.

Additional implementation guidance for 8.3.2, Disposal of media, of ISO/IEC 27002:2013 is:

Where removable media on which PII is stored is disposed of, secure disposal procedures should be included in the documented information and implemented to ensure that previously stored PII will not be accessible.

6.5.3.3 Physical media transfer

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.3.3 and the following additional guidance applies:

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021

Additional implementation guidance for 8.3.3, Physical media transfer, of ISO/IEC 27002:2013 is:

If physical media is used for information transfer, a system should be put in place to record incoming and outgoing physical media containing PII, including the type of physical media, the authorized sender/recipients, the date and time, and the number of physical media. Where possible, additional measures such as encryption should be implemented to ensure that the data can only be accessed at the point of destination and not in transit.

The organization should subject physical media containing PII before leaving its premises to an authorization procedure and ensure the PII is not accessible to anyone other than authorized personnel.

NOTE One possible measure to ensure PII on physical media leaving the organization's premises is not generally accessible is to encrypt the PII concerned and restrict decryption capabilities to authorized personnel.

6.6 Access control

6.6.1 Business requirements of access control

6.6.1.1 Access control policy

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.1.1 applies.

6.6.1.2 Access to networks and network services

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.1.2 applies.

6.6.2 User access management

6.6.2.1 User registration and de-registration

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.2.1 and the following additional guidance applies:

Additional implementation guidance for 9.2.1, User registration and de-registration, of ISO/IEC 27002:2013 is:

Procedures for registration and de-registration of users who administer or operate systems and services that process PII should address the situation where user access control for those users is compromised, such as the corruption or compromise of passwords or other user registration data (e.g. as a result of inadvertent disclosure).

The organization should not reissue to users any de-activated or expired user IDs for systems and services that process PII.

In the case where the organization is providing PII processing as a service, the customer can be responsible for some or all aspects of user ID management. Such cases should be included in the documented information.

Some jurisdictions impose specific requirements regarding the frequency of checks for unused authentication credentials related to systems that process PII. Organizations operating in these jurisdictions should take compliance with these requirements into account.

6.6.2.2 User access provisioning

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.2.2 and the following additional guidance applies:

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021

Additional implementation guidance for 9.2.2, User access provisioning, of ISO/IEC 27002:2013 is:

The organization should maintain an accurate, up-to-date record of the user profiles created for users who have been authorized access to the information system and the PII contained therein. This profile comprises the set of data about that user, including user ID, necessary to implement the identified technical controls providing authorized access.

Implementing individual user access IDs enables appropriately configured systems to identify who accessed PII and what additions, deletions or changes they made. As well as protecting the organization, users are also protected as they can identify what they have processed and what they have not processed.

In the case where the organization is providing PII processing as a service, the customer can be responsible for some or all aspects of access management. Where appropriate, the organization should provide the customer the means to perform access management, such as by providing administrative rights to manage or terminate access. Such cases should be included in the documented information.

6.6.2.3 Management of privileged access rights

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.2.3 applies:

6.6.2.4 Management of secret authentication information of users

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.2.4 applies.

6.6.2.5 Review of user access rights

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.2.5 applies.

6.6.2.6 Removal or adjustment of access rights

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.2.6 applies.

6.6.3 User responsibilities

6.6.3.1 Use of secret authentication information

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.3.1 applies.

6.6.4 System and application access control

6.6.4.1 Information access restriction

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.4.1 applies.

6.6.4.2 Secure log-on procedures

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.4.2 and the following additional guidance applies:

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27701:2021