ISO/IEC JTC1/SC 27 N19115

Date: 2018-10-10

ISO/IEC DIS 27552

ISO/IEC TC JTC1/SC 27/WG 5

Secretariat: DIN

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

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

Document type: International Standard
Document subtype:
Document stage: (40) Enquiry
Document language: E

C:\altes-NB\Documents\Project_admin\27552_NP_Enhanc_27001_priv_mgmt\04_01_1st_DIS_27552_201812dd\N19xxx_Text_1st_DIS_27552_20181015\ISO-IEC_27552_(E) Revised text for DIS N1615 111018.doc STD Version 2.1c2

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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

ISO/IEC 27552 was prepared by Technical Committee ISO/TC JTC1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

0 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 laws and regulations all over the world.

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

This document defines additional requirements and provides guidance for the protection of privacy as potentially affected by the processing of PII, enabling the organizations' overall Management System to be extended to cover both the general requirements for information security (an Information Security Management System (ISMS)) and the more specific requirements for PII protection, both together constituting a Privacy Information Management System (PIMS). These additional requirements and guidance are written in such a way that they are practically usable for PII protection by organizations of all sizes and cultural environments.

Requirements and guidance for PII protection vary depending upon the context of the organization, in particular where national laws and regulations are applicable. 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; also to ISO/IEC 27018, ISO/IEC 29151 and the EU General Data Protection Regulation. However these might need to be interpreted to take into account local laws and regulations.

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 sub-contractors 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 might 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, although compliance with this document cannot be taken as compliance with laws and regulations.

0.2 Compatibility with other management system standards

This document applies the framework developed by ISO to improve alignment amongst its International Standards for Management Systems.

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

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.

In particular, 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.

Excluding any of the requirements specified in Clause 5 of this document is not acceptable when an organization claims conformity to this document.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000:2018, *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 29100:2011, *Information technology — Security techniques — Privacy framework*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

3.1.1
joint PII controller
two or more PII controllers that jointly determine the purposes and means of the processing of PII

3.1.2
privacy information management system
PIMS
information security management system which addresses the protection of privacy as potentially affected by the processing of PII

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply:

ISMS Information Security Management System

PII Personally Identifiable Information

PIMS Privacy Information Management System

3.3 Alternative terms

The protection of PII is subject to laws and regulations in many jurisdictions. In some cases, those laws and regulations use terminology which has both similarities and differences to the terminology used in this document.

The mapping between the terminology used in this document and that used in some laws and regulations is shown in Annex F.

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, in addition to information security, the protection of privacy of PII principals as potentially affected by the processing of PII. For a better understanding, implementation guidance and other information regarding the requirements is included.

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 are given in Clause 5.

NOTE 1 For completeness, clause 5 of this document contains a sub-clause 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.

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 are given in Clause 6.

NOTE 2 For completeness, clause 6 of this document contains a sub-clause 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.

Additional ISO/IEC 27002 guidance for PII controllers is given in Clause 7, and additional ISO/IEC 27002 guidance for PII processors is given in Clause 8.

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

The PIMS specific control objectives and controls for an organization acting as a PII processor are listed in Annex B (whether it subcontracts the processing of PII to a separate PII processor or not).

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

Annex D of this document contains a mapping to ISO/IEC 29100, and Annex E contains a mapping to ISO/IEC 27018 and ISO/IEC 29151.

Annex F contains a list of some of the terms used in this document and alternative terms used in specific jurisdictions.

Annex G contains explanatory text on 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.

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

Clause number in ISO/IEC 27001:2013	Title	Sub-clause number 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 No PIMS-specific requirements, but extended interpretation of "information security" according to 5.1.

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 number in ISO/IEC 27002:2013	Title	Clause number 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 No PIMS-specific guidance, but extended interpretation of “information security” according to 6.1.

4.4 Customer

Depending on the role of the organization (see 5.2.1 Understanding the organization and its context), "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 PII sub-processor (e.g., the customer of the 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 is 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 G).

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.

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 upon 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 amongst 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, supervisory authorities, other PII controllers, PII processors and their sub-contractors.

NOTE 2 Requirements relevant to the processing of PII could 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 Clauses 4 to 10, extended by the requirements in Clause 5 of this document.

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 of this document, apply.

5.3.2 Policy

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

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 of this document, 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(s) to identify risks associated with the loss of confidentiality, integrity and availability, within the scope of the PIMS.

The organization shall apply the privacy risk assessment process(s) 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) 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 6.1.2.c) of ISO/IEC 27001:2013, 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 6.1.3 b) of ISO/IEC 27001:2013 shall be compared with those in ISO/IEC 27001:2013, Annex A and/or Annex B of this document 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 ISO/IEC 27001:2013, Annex A and/or in B of this document 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 may include where the controls are not deemed necessary by the risk assessment, or where they are not required by (or are subject to exceptions under) the laws and/or regulations 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 of this document, 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 of this document, apply.

5.5.2 Competence

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

5.5.3 Awareness

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

5.5.4 Communication

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

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 of this document, apply.

5.7.2 Internal audit

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

5.7.3 Management review

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

5.8.2 Continual improvement

The requirements stated in ISO/IEC 27001:2013, 10.2 along with the interpretation specified in 5.1 of this document, 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 G).

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 the applicable jurisdiction or by specific provisions in Clause 6, 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 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 with the contractual terms agreed between the organization and its partners, its subcontractors and its applicable third parties (customers, suppliers etc.), which should clearly allocate responsibilities between them.

Additional other information for control 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 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);
- 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 law, regulation and practices;
- 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 defines 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:

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 compromise 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:

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 could 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 use 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:

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. Including PII as part of 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 the organizations control are made aware of the definition of PII and how to recognize whether information 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:

Wherever feasible, the organization should use removable physical media and/or devices that permit encryption for the storage of PII.

The organization should document any use of removable media and/or devices for the storage of PII. The organization should not use removable physical media and/or devices that do not permit encryption for the storage of PII, except where it is unavoidable. Instances where unencrypted physical media and/or devices is used, the organization should implement procedures and compensating controls (e.g., tamper-evident packaging) to mitigate risks to the PII.

Removable media which is taken outside the physical confines of the organization are 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 upon which PII is stored is disposed of, secure disposal procedures should be documented 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:

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 authorized 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 that the corruption or compromise of passwords or other user registration data (e.g., as a result of inadvertent disclosure).

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

In the context of distributed systems, the customer can be responsible for some or all aspects of user ID management. Such cases should be documented.

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 ensure that they comply with these requirements.

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:

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

In the context of the service providers, 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 documented.

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.

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:

Additional implementation guidance for 9.4.2, Secure log-on procedures, of ISO/IEC 27002:2013 is:

Where required by the customer, the organization should provide the capability for secure log-on procedures for any user accounts under the customer's control.

6.6.4.3 Password management system

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.4.3 applies.

6.6.4.4 Use of privileged utility programs

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.4.4 applies.

6.6.4.5 Access control to program source code

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 9.4.5 applies.

6.7 Cryptography

6.7.1 Cryptographic controls

6.7.1.1 Policy on the use of cryptographic controls

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 10.1.1 and the following additional guidance applies:

Additional implementation guidance for 10.1.1, Policy on the use of cryptographic controls, of ISO/IEC 27002:2013 is:

Some jurisdictions can require the use of cryptography to protect particular kinds of PII, such as health data, resident registration numbers, passport numbers and driver's licence numbers.

The organization should provide information to the customer regarding the circumstances in which it uses cryptography to protect the PII it processes. The organization should also provide information to the customer about any capabilities it provides that can assist the customer in applying their own cryptographic protection.

6.7.1.2 Key management

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 10.1.2 applies.

6.8 Physical and environmental security

6.8.1 Secure areas

6.8.1.1 Physical security perimeter

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.1.1 applies.

6.8.1.2 Physical entry controls

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.1.2 applies.

6.8.1.3 Securing offices, rooms and facilities

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.1.3 applies.

6.8.1.4 Protecting against external and environmental threats

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.1.4 applies.

6.8.1.5 Working in secure areas

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.1.5 applies.

6.8.1.6 Delivery and loading areas

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.1.6 applies.

6.8.2 Equipment

6.8.2.1 Equipment siting and protection

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.1 applies.

6.8.2.2 Supporting utilities

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.2 applies.

6.8.2.3 Cabling security

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.3 applies.

6.8.2.4 Equipment maintenance

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.4 applies.

6.8.2.5 Removal of assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.5 applies.

6.8.2.6 Security of equipment and assets off-premises

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.6 applies.

6.8.2.7 Secure disposal or re-use of equipment

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.7 and the following additional guidance applies:

Additional implementation guidance for 11.2.7, Secure disposal or re-use of equipment, of ISO/IEC 27002:2013 is:

The organization should ensure that, whenever PII storage space is re-assigned, any PII previously residing on that storage space is not visible.

Upon deletion of PII held in an information system, performance issues can mean that explicit erasure of that PII is impractical. This creates the risk that another user can be able to read the PII. Such risk should be avoided by specific technical measures.

For secure disposal or re-use, equipment containing storage media that could possibly contain PII should be treated as though it does contain PII.

6.8.2.8 Unattended user equipment

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.8 applies.

6.8.2.9 Clear desk and clear screen policy

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.9 and the following additional guidance applies:

Additional implementation guidance for 11.2.9, Clear desk and clear screen policy, of ISO/IEC 27002:2013 is:

The organization should restrict the creation of hardcopy material displaying PII to the minimum needed to fulfil the identified processing purpose.

6.9 Operations security

6.9.1 Operational procedures and responsibilities

6.9.1.1 Documenting operating procedures

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.1.1 applies.

6.9.1.2 Change management

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.1.2 applies.

6.9.1.3 Capacity management

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.1.3 applies.

6.9.1.4 Separation of development, testing and operational environments

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.1.4 applies.

6.9.2 Protection from malware

6.9.2.1 Controls against malware

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.2.1 applies.

6.9.3 Backup

6.9.3.1 Information backup

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.3.1 and the following additional guidance applies:

Additional implementation guidance for 12.3.1 Information backup, of ISO/IEC 27002:2013 is:

The organization should have a policy which addresses the requirements for backup, recovery and restoration of PII (which could be part of an overall information backup policy) and any further requirements (e.g., contractual and/or legal requirements) for the erasure of PII contained in information held for backup requirements.

PII-specific responsibilities in this respect can lie with the customer. In this case, the organization should ensure that the customer has been informed of the limits of the service regarding backup.

Where the organization explicitly provides backup and restore services to customers, the organization should provide them with clear information about their capabilities with respect to backup and restoration of PII.

Some jurisdictions impose specific requirements regarding the frequency of backups of PII, the frequency of reviews and tests of backup, or regarding the recovery procedures for PII. Organizations operating in these jurisdictions should ensure that they comply with these requirements.

There can be occasions where PII needs to be restored, perhaps due to a system malfunction, attack or disaster. When PII is restored (typically from backup media), processes need to be in place to ensure that the PII is restored into a state where PII accuracy can be assured, or where PII inaccuracies are identified and processes put in place to resolve these inaccuracies (which can involve the PII principal).

The organization should have a procedure for, and a log of, PII restoration efforts. At a minimum, the log of the PII restoration efforts should contain:

- the name of person responsible for the restoration;
- a description of the restored PII.

Some jurisdictions can prescribe the content of the logs of PII restoration efforts. Organizations should familiarize themselves with the applicable legislation and/or regulations.

The use of subcontractors to store replicated or backup copies of PII being processed is covered by the controls in this document applying to subcontracted PII processing (6.12.1.2). Where physical media transfers take place related to backups and restoration, this is also covered by controls in this document (6.10.2.1).

6.9.4 Logging and monitoring

6.9.4.1 Event logging

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.4.1 and the following additional guidance applies:

Additional implementation guidance for 12.4.1, Event logging, of ISO/IEC 27002:2013 is:

A process should be put in place to review event logs using continuous, automated monitoring and alerting processes, or else manually where such review should be performed with a specified, documented periodicity, to identify irregularities and propose remediation efforts.

Where possible, event logs should record access to PII, including by whom, when, which PII principal's PII was accessed, and what (if any) changes were made (additions, modifications or deletions) as a result of the event.

Where multiple service providers are involved in providing services, there can be varied or shared roles in implementing this guidance. These roles should be clearly defined and documented, and agreement on any log access between providers should be addressed.

Implementation guidance for PII processors:

The organization should define criteria regarding if, when and how log information can be made available to or usable by the customer. These criteria should be made available to the customer.

Where the organization permits its customers to access log records controlled by the organization, the organization should implement appropriate controls to ensure that the customer can only access records that relate to that customer’s activities, cannot access any log records which relate to the activities of other customers, and cannot amend the logs in any way.

6.9.4.2 Protection of log information

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.4.2 and the following additional guidance applies:

Additional implementation guidance for 12.4.2, Protection of log information, of ISO/IEC 27002:2013 is:

Log information recorded for, for example, security monitoring and operational diagnostics, could contain PII. Measures such as controlling access (see 9.2.3 of ISO/IEC 27002) should be put in place to ensure that logged information is only used as intended.

A procedure, preferably automatic, should be put in place to ensure that logged information is either deleted or de-identified within a specified and documented period.

6.9.4.3 Administrator and operator logs

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.4.3 applies.

6.9.4.4 Clock synchronization

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.4.4 applies.

868 **6.9.5 Control of operational software**

869 **6.9.5.1 Installation of software on operational systems**

870 The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.5.1 applies.

871 **6.9.6 Technical vulnerability management**

872 **6.9.6.1 Management of technical vulnerabilities**

873 The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.6.1 applies.

874 **6.9.6.2 Restriction on software installation**

875 The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.6.2 applies.

876 **6.9.7 Information systems audit considerations**

877 **6.9.7.1 Information systems audit controls**

878 The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 12.7.1 applies.

879 ## 6.10 Communications security

880 **6.10.1 Network security management**

881 **6.10.1.1 Network controls**

882 The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.1.1 applies.

883 **6.10.1.2 Security in network services**

884 The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.1.2 applies.

885 **6.10.1.3 Segregation in networks**

886 The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.1.3 applies.

887 **6.10.2 Information transfer**

888 **6.10.2.1 Information transfer policies and procedures**

889 The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.2.1 and the
890 following additional guidance applies:

891 **Additional implementation guidance for 13.2.1, Information transfer policies and procedures, of**
892 **ISO/IEC 27002:2013 is:**

893 The organization should consider procedures for ensuring that rules related to the processing of PII are
894 enforced throughout and outside of the system, where applicable (e.g., metadata tags).

895 **6.10.2.2 Agreements for information transfer**

896 The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.2.2 applies.

6.10.2.3 Electronic messaging

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.2.3 applies.

6.10.2.4 Confidentiality or non-disclosure agreements

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 13.2.4 and the following additional guidance applies:

Additional implementation guidance for 13.2.4, Confidentiality or non-disclosure agreements, of ISO/IEC 27002:2013 is:

The organization should ensure that individuals operating under its control with access to PII are subject to a confidentiality obligation. The confidentiality agreement, whether part of a contract or separate, should specify the length of time the obligations should be adhered to.

When the organization is a PII processor, a confidentiality agreement, in whatever form, between the organization, its employees and its agents should ensure that employees and agents comply with the policy and procedures concerning data handling and protection.

6.11 Systems acquisition, development and maintenance

6.11.1 Security requirements of information systems

6.11.1.1 Information security requirements analysis and specification

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.1.1 applies.

6.11.1.2 Securing application services on public networks

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.1.2 and the following additional guidance applies:

Additional implementation guidance for 14.1.2, Securing application services on public networks, of ISO/IEC 27002:2013 is:

The organization should ensure that PII that is transmitted over untrusted data transmission networks is encrypted for transmission.

Untrusted networks can include the public internet and other facilities outside of the operational control of the organization.

NOTE In some cases (e.g., the exchange of e-mail) the inherent characteristics of untrusted data transmission network systems might require that some header or traffic data be exposed for effective transmission.

6.11.1.3 Protecting application services transactions

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.1.3 applies.

6.11.2 Security in development and support processes

6.11.2.1 Secure development policy

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.1 and the following additional guidance applies.

Additional implementation guidance for 14.2.1, Secure development policy, of ISO/IEC 27002:2013 is:

Policies for system development and design should include guidance for the organization's processing of PII needs, based on obligations to PII principals and/or any applicable laws or regulations and the types of processing performed by the organization. Clauses 7 and 8 provide control considerations for processing of PII, which may be useful in developing policies for privacy in systems design.

Policies that contribute to privacy by design and privacy by default should consider the following aspects:

a) guidance on PII protection and the implementation of the privacy principles (see ISO/IEC 29100) in the software development lifecycle;
b) privacy and PII protection requirements in the design phase, which should be based on the output from a privacy impact assessment (see 7.2.5);
c) PII protection checkpoints within project milestones;
d) required privacy and PII protection knowledge;
e) by default minimise processing of PII.

6.11.2.2 System change control procedures

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.2 applies.

6.11.2.3 Technical review of applications after operating platform changes

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.3 applies.

6.11.2.4 Restrictions of changes to software packages

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.4 applies.

6.11.2.5 Secure systems engineering principles

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.5 and the following additional guidance applies:

Additional implementation guidance for 14.2.5, Secure systems engineering principles, of ISO/IEC 27002:2013 is:

Systems and/or components related to the processing of PII should be designed following the principles of privacy by design and privacy by default, and to anticipate and facilitate the implementation of relevant controls (as described in clauses 7 and 8, for PII controllers and PII processors, respectively), in particular such that the collection and processing of PII in those systems is limited to what is necessary for the identified purposes of the processing of PII (clause 7.2).

For example, an organization that processes PII can need to ensure that, based on the relevant jurisdiction, it disposes of PII after a specified period. The system that processes that PII should be designed in a way to facilitate this deletion requirement.

The same principles of privacy by design and privacy by default should be applied, if applicable, to outsourced information systems.

6.11.2.6 Secure development environment

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.6 applies.

6.11.2.7 Outsourced development

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.7 applies.

6.11.2.8 System security testing

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.8 applies.

6.11.2.9 System acceptance testing

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.2.9 applies.

6.11.3 Test data

6.11.3.1 Protection of test data

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 14.3.1 and the following additional guidance applies:

Additional implementation guidance for 14.3.1, Protection of test data, of ISO/IEC 27002:2013 is:

PII should not be used for testing purposes; false or synthetic PII should be used. Where the use of PII for testing purposes cannot be avoided, technical and organizational measures equivalent to those used in the production environment should be implemented to minimize the risks. Where such equivalent measures are not feasible, a risk-assessment should be undertaken and used to inform the selection of appropriate mitigating controls.

6.12 Supplier relationships

6.12.1 Information security in supplier relationships

6.12.1.1 Information security policy for supplier relationships

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 15.1.1 applies.

6.12.1.2 Addressing security within supplier agreements

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 15.1.2 and the following additional guidance applies:

Additional implementation guidance for 15.1.2, Addressing security within supplier agreements, of ISO/IEC 27002:2013 is:

The organization should specify in contracts between themselves and any suppliers whether PII is being processed and the minimum technical and organizational measures that the supplier needs to meet in order for the organization's to meet its information security and PII protection obligations.

Contractual agreements should clearly allocate responsibilities between the organization, its partners, its suppliers and its applicable third parties (customers, suppliers, etc.) taking into account the type of PII processed.

The contract between the organization and its customers should provide a mechanism for ensuring the organization supports and manages compliance with all applicable legislation and regulation. The contract should call for independently audited compliance, acceptable to the customer.

NOTE For such audit purposes, compliance with relevant and applicable security and privacy standards such as ISO/IEC 27001 or this document can be considered acceptable.

Implementation guidance for PII processors

The organization should specify in contracts with any suppliers that PII is only processed on its instructions.

6.12.1.3 Information and communication technology supply chain

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 15.1.3 applies.

6.12.2 Supplier service delivery management

6.12.2.1 Monitoring and review of supplier services

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 15.2.1 applies.

6.12.2.2 Managing changes to supplier services

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 15.2.2 applies.

6.13 Information security incident management

6.13.1 Management of information security incidents and improvements

6.13.1.1 Responsibilities and procedures

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.1 and the following additional guidance applies:

Additional implementation guidance for 16.1.1, Responsibilities and procedures, of ISO/IEC 27002:2013 is:

As part of the overall incident management process, the organization should establish responsibilities and procedures for the identification and recording of breaches of PII processing. Additionally, the organization should establish responsibilities and procedures related to notification to required parties of PII breaches (including the timing of such notifications) and the disclosure to authorities as required by applicable legislation and/or regulation.

Some jurisdictions impose specific regulations regarding breach responses, including notification. Organizations operating in these jurisdictions should ensure responsibilities to ensure that they comply with these requirements.

6.13.1.2 Reporting information security events

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.2 applies.

6.13.1.3 Reporting information security weaknesses

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.3 applies.

6.13.1.4 Assessment of and decisions on information security events

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.4 applies.

6.13.1.5 Response to information security incidents

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.5 and the following additional guidance applies:

Additional implementation guidance for 16.1.5, Response to information security incidents, of ISO/IEC 27002:2013 is:

Implementation guidance for PII controllers

An incident that involves PII should trigger a review by the organization, as part of its information security incident management process, to determine if a breach involving PII that requires a response has taken place.

An event does not necessarily trigger such a review.

NOTE 1 An event is one that does not result in actual, or the significant probability of, unauthorized access to PII or to any of the organization's equipment or facilities storing PII. These can include, but not limited to, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks and packet sniffing.

When a breach of PII has occurred, response procedures should include relevant notifications and records.

Some jurisdictions define cases when the breach should be notified to the supervisory authority, and when it should be notified to PII principals.

Notifications should be clear, and, depending on jurisdiction, could be required.

NOTE 2 Notification could contain details such as:

- a contact point where more information can be obtained;
- a description of and the likely consequences of the breach;
- a description of the breach including the number of individuals concerned as well as the number of records concerned;
- measures taken or planned to be taken.

NOTE 3 Information on the management of security incidents can be found in ISO/IEC 27035.

Where a breach involving PII has occurred, a record should be maintained with sufficient information to provide a report for regulatory and/or forensic purposes, such as:

— a description of the incident;
— the time period;
— the consequences of the incident;
— the name of the reporter;
— to whom the incident was reported;
— the steps taken to resolve the incident (including the person in charge and the data recovered);
— the fact that the incident resulted in unavailability, loss, disclosure or alteration of PII.

In the event that a breach involving PII has occurred, the record should also include a description of the PII compromised, if known; and if notifications were performed, the steps taken to notify PII individuals, regulatory agencies or customers.

Implementation guidance for PII processors

Provisions covering the notification of a breach involving PII should form part of the contract between the organization and the customer. The contract should specify how the organization will provide the information necessary for the customer to fulfil their obligation to notify relevant authorities. This notification obligation does not extend to a breach caused by the customer or PII principal or within system components for which they are responsible. The contract should also define the maximum delay in notification of a breach involving PII.

- where a breach involving PII has occurred, a record should be maintained with sufficient information to provide a report for regulatory and/or forensic purposes, such as:
- a description of the incident;
- the time period;
- the consequences of the incident;
- the name of the reporter;
- to whom the incident was reported;

- the steps taken to resolve the incident (including the person in charge and the data recovered);
- the fact that the incident resulted in unavailability, loss, disclosure or alteration of PII.

In the event that a breach involving PII has occurred, the record should also include a description of the PII compromised, if known; and if notifications were performed, the steps taken to notify the customer and/or the regulatory agencies.

In some jurisdictions, the PII processor should notify the PII controller of the existence of a breach without undue delay (i.e. as soon as possible), preferably, as soon as it is discovered so that the PII controller can take the appropriate actions.

In some jurisdictions, applicable legislation or regulations can require the organization to directly notify appropriate regulatory authorities (e.g., a PII protection authority) of a breach involving PII.

6.13.1.6 Learning from information security incidents

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.6 applies.

6.13.1.7 Collection of evidence

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.7 applies:

6.14 Information security aspects of business continuity management

6.14.1 Information security continuity

6.14.1.1 Planning information security continuity

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 17.1.1 applies.

6.14.1.2 Implementing information security continuity

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 17.1.2 applies.

6.14.1.3 Verify, renew and evaluate information security continuity

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 17.1.3 applies.

6.14.2 Redundancies

6.14.2.1 Availability of information processing facilities

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 17.2.1 applies.

6.15 Compliance

6.15.1 Compliance with legal and contractual requirements

6.15.1.1 Identification of applicable legislation and contractual requirements

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.1.1 and the following additional guidance applies:

Additional other information for 18.1.1, Identification of applicable legislation and contractual requirements, of ISO/IEC 27002:2013 is:

The organization should identify any potential legal sanctions (which could result from some obligations being missed) related to the processing of PII, including substantial fines directly from the local supervisory authority. In some jurisdictions, International Standards such as this document can be used to form the basis for a contract between the organization and the customer, outlining their respective security, privacy and PII protection responsibilities. The terms of the contract can provide a basis for contractual sanctions in the event of a breach of those responsibilities.

6.15.1.2 Intellectual property rights

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.1.2 applies.

6.15.1.3 Protection of records

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.1.3 and the following additional guidance applies:

Additional implementation guidance for 18.1.3, Protection of records, of ISO/IEC 27002:2013 is:

Review of current and historical policies and procedures can be required (e.g., in the cases of customer dispute resolution and investigation by a supervisory authority).

The organization should retain copies of its privacy policies and associated procedures for a specified, documented period of time (see 7.2.8). This includes retaining copies of previous versions of these documents when they are updated.

6.15.1.4 Privacy and protection of personally identifiable information

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.1.4 applies.

6.15.1.5 Regulation of cryptographic controls

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.1.5 applies.

6.15.2 Information security reviews

6.15.2.1 Independent review of information security

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.2.1 and the following additional guidance applies:

Additional implementation guidance for 18.2.1, Independent review of information security, of ISO/IEC 27002:2013 is:

Where an organization is acting as a PII processor, and where individual customer audits are impractical or could increase risks to security, the organization should make available to customers, prior to entering into, and for the duration of, a contract, independent evidence that information security is implemented and operated in accordance with the organization's policies and procedures. A relevant independent audit, as selected by the organization, should normally be an acceptable method for fulfilling the customer's interest in reviewing the organization's processing operations, if it covers the needs of anticipated users and if results are provided in a sufficient transparent manner.

6.15.2.2 Compliance with security policies and standards

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.2.2 applies.

6.15.2.3 Technical compliance review

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.2.3 and the following additional guidance applies:

Additional implementation guidance for 18.2.3, Technical compliance review, of ISO/IEC 27002:2013 is:

As part of technical reviews of compliance with security policies and standards, the organization should include methods of reviewing those tools and components related to processing PII. This can include:

- Ongoing monitoring to verify that only permitted processing is taking place; and/or
- Specific penetration or vulnerability tests (for example, de-identified datasets can be subject to a motivated intruder test to validate that de-identification methods are compliant with organizational requirements).

7 Additional ISO/IEC 27002 guidance for PII controllers

7.1 General

The guidance contained in Clause 6 plus the additions in the current clause create the PIMS-specific guidance for PII controllers. The implementation guidance documented in the current clause relate to the controls listed in Annex A.

7.2 Conditions for collection and processing

Objective: To ensure that processing is lawful, with legal basis as per applicable jurisdictions, with clearly defined and legitimate purposes.

7.2.1 Identify and document purpose

Control

The organization should identify and document the specific purposes for which the PII will be processed.

Implementation guidance

The organization should ensure that PII principals understand the purpose for which their PII is processed. It is the responsibility of the organization to clearly document and communicate this to PII principals. Without a clear statement of the purpose for processing, consent and choice cannot be adequately given.

Documentation of the purpose(s) for processing PII should be sufficiently clear and detailed to be usable in the required information to be provided to PII principals (see 7.3.2). This includes information necessary to obtain consent (see 7.2.3), as well as records of policies and procedures (see 7.2.8).

Other information

In the deployment of cloud computing services, the taxonomy and definitions in ISO/IEC 19944 can be helpful in providing terms for describing the purpose of the processing of PII.

7.2.2 Identify lawful basis

Control

The organization should determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes.

Implementation guidance

Some jurisdictions require the organization to be able to demonstrate that the lawfulness of processing was duly established before the processing.

The legal basis for the processing of PII could include:

- consent from PII principals;
- performance of a contract;
- compliance with a legal obligation;
- protect the vital interests of PII principals;
- performance of a task carried out in the public interests;
- legitimate interests of the PII controller.

The organization should document tis basis for each PII processing activity (see 7.2.8).

The legitimate interests of the organization could include, for instance, information security objectives, which should be balanced against the obligations to PII principals with regards to privacy protection.

Whenever special categories of PII are defined, either by the nature of the PII (e.g. health information) or by the PII principals concerned (e.g. PII relating to children), the organization should include those categories of PII in its classification schemes.

The classification of PII that falls into these categories can vary from one jurisdiction to another and can vary between different regulatory regimes that apply to different kinds of business, so the organization needs to be aware of the classification(s) that apply to the PII processing being performed.

The use of special categories of PII might also be subject to more stringent controls.

Changing or extending the purposes for the processing of PII might require updating and/or revision of the legal basis. It might also require additional consent to be obtained from the PII principal.

7.2.3 Determine when and how consent is to be obtained

Control

The organization should determine and document a process by which it can demonstrate if, when and how consent for the processing of PII was obtained from PII principals.

Implementation guidance

Consent is normally required for processing of PII unless other lawful grounds apply. The organization should clearly document when consent needs to be obtained and the requirements for obtaining consent. It can be useful to correlate the purpose(s) for processing with information about if and how consent is obtained.

Some jurisdictions have specific requirements for how consent is collected and recorded (e.g., not bundled with other agreements). Additionally, certain types of data collection (for scientific research for example) and certain types of PII principals, such as children, can be subject to additional requirements. The organization should take into account such requirements and document how mechanisms for consent meet those requirements.

7.2.4 Obtain and record consent

Control

The organization should obtain and record consent from PII principals according to the documented processes.

Implementation guidance

The organization should obtain and record consent from PII principals in such a way that it can provide on request details of the consent provided (for example the time that consent was provided, the identification of the PII principal, and the consent statement).

The information delivered to the PII principal before the consent process should follow the guidance in 7.3.3

The consent should fulfil the following conditions:

— be freely given;
— be specific regarding the purpose for processing;
— be unambiguous and explicit.

7.2.5 Privacy impact assessment

Control

The organization should assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of PII or changes to existing processing of PII is planned.

Implementation guidance

PII processing generates risks for PII principals. These risks should be assessed through a privacy impact assessment. Some jurisdictions define cases for which a privacy impact assessment should be performed. Criteria could include automated decision making which produces legal effects on PII principals, large scale processing of special categories of PII (e.g., health related information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data or biometric data), or systematic monitoring of a publicly accessible area on a large scale.

The organization should determine the elements that are necessary for the completion of a privacy impact assessment. These could include a list of the types of PII being processed, where the PII is stored and where it can be transferred. Data flow diagrams and data maps could also be helpful in this context. See 7.2.8 for details of records of the processing of PII that might inform a privacy impact or other risk assessment.

Other information

Guidance on the assessment of privacy impacts related to the processing of PII can be found in ISO/IEC 29134

7.2.6 Contracts with PII processors

Control

The organization should have a written contract with any PII processor that it uses, and should ensure that their contracts with PII processors address the implementation of the appropriate controls in Annex B.

Implementation guidance

The contract between the organization and any PII processor processing PII on its behalf should require the PII processor to implement the appropriate controls specified in Annex B, taking account of the information security risk assessment process (see 5.4.1.2) and the scope of the processing of PII performed by the PII processor (see 6.12). By default, all controls specified in Annex B should be assumed as relevant. If the organization decides to not require the PII processor to implement a control from Annex B, it should justify its exclusion.

A contract can define the responsibilities of each party differently but, to be consistent with this document, all controls should be considered and documented.

7.2.7 Joint PII controller

Control

The organization should determine respective roles and responsibilities for the processing of PII (including PII protection and security requirements) with any joint PII controller.

Implementation guidance

Roles and responsibilities for the processing of PII should be determined in a transparent manner. They should at least address the requirements of applicable legislation(s) and/or regulation(s).

These roles and responsibilities should be documented in a contract or any similar binding document that contains the terms and conditions for the joint processing of PII. In some jurisdictions, such an agreement is termed a data sharing agreement.

A joint PII controller agreement can include (this list is neither definitive nor exhaustive):

- purpose of PII sharing / joint PII controller relationship;
- identity of the organizations (PII controllers) that are part of the joint PII controller relationship;
- categories of PII to be shared and/or transferred and processed under the agreement;
- overview of the processing operations (e.g., transfer, use);
- description of the respective roles and responsibilities;
- responsibility for implementing technical and organizational security measures for PII protection;
- definition of responsibility in case of a PII breach (e.g. who will notify, when, mutual information);
- terms of retention and/or disposal of PII;
- liabilities for failure to comply with the agreement;
- how obligations to PII principals are met;
- how to provide PII principals with information covering the essence of the arrangement between the joint PII controllers;
- how PII principals can obtain other information they are entitled to receive; and
- a contact point for PII principals.

7.2.8 Records related to processing PII

Control

The organization should determine and securely maintain the necessary records in support of its obligations for the processing of PII.

Implementation guidance

A step in maintaining records of the processing of PII is to have an inventory or list of the PII processing activities that the organization performs. Such an inventory could include:

- the type of processing;
- the purposes for the processing;
- a description of the categories of PII and PII principals (e.g., children);
- the categories of recipients to whom PII has been or will be disclosed, including recipients in third countries or international organizations;
- a general description of the technical and organizational security measures; and
- a Privacy Impact Assessment report.

Such an inventory should have an owner who is responsible for its accuracy and completeness.

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.

7.3.1 Determining and fulfilling obligations to PII principals

Control

The organization should determine, document and comply with their legal, regulatory and business obligations to PII principals, related to the processing of their PII and provide the means to meet these obligations.

Implementation guidance

Obligations to PII principals and the means to support them vary from one jurisdiction to another.

The organization should ensure that they provide the appropriate means to meet the obligations to PII principals in an accessible and timely manner. Clear documentation should be provided to the PII principal describing the extent and manner in which the obligations to them are fulfilled, along with an up-to-date contact point where they can address their requests.

The contact point should be provided in a manner similar to the one used to collect PII and consent (e.g. if PII are collected by email or a website, the contact point should be by email or the website, not an alternative such as phone or fax).

7.3.2 Determining information for PII principals

Control

The organization should determine and document the information which is to be provided to PII principals regarding the processing of their PII and the timing of such a provision.

Implementation guidance

The organization should determine the legal, regulatory and/or business requirements for when information is to be provided to the PII principal (e.g., prior to processing, within a certain time from when it is requested, etc.) and for the type of information to be provided.

Depending on the requirements, the information can take the form of a notice. Examples of types of information that can be provided to PII principals are:

- information about the purpose of the processing;
- contact details for the PII controller or its representative;
- information about the basis for the processing;
- information on where the PII was obtained, if not obtained directly from the PII principal;
- information about whether the provision of PII is a statutory or contractual requirement, and where appropriate, the possible consequences of failure to provide PII;
- information on how the PII principal can trigger the obligations described in 7.3.1 especially regarding access, amend, correct, request erasure, receive a copy of their PII and object to the processing;
- information on how the PII principal can withdraw consent;
- information about transfers of PII;
- information about recipients or categories of recipients of PII;
- information about the period for which the PII will be retained;
- information about the use of automated decision making based on the automated processing of PII;
- information about the right to lodge a complaint and how to lodge such a complaint;
- information regarding the frequency with which information is provided (e.g. “just in time” notification, organization defined frequency, etc.).

The organization should provide updated information if the purposes for the processing of PII are changed or extended.

7.3.3 Providing information to PII principals

Control

The organization should provide PII principals with clear and easily accessible information related to the PII controller and the processing of their PII.

Implementation guidance

The organization should provide the information detailed in 7.3.2 to PII principals in a timely, concise, complete, transparent, intelligible and easily accessible form, using clear and plain language, as appropriate to the target audience.

Where appropriate, the information should be given at the time of PII collection. It should also be permanently accessible.

NOTE Icons and images can be helpful to the PII principal by giving a visual overview of the intended processing.

7.3.4 Provide mechanism to modify or withdraw consent

Control

The organization should provide a mechanism for PII principals to modify or withdraw their consent.

Implementation guidance

The organization should provide information to PII principals informing them of their right to withdraw consent at any time, and provide the mechanism by which to withdraw consent. The mechanism used for withdrawal will be dependent on the system; it should be consistent with the mechanisms used for obtaining consent when possible. For example, if the consent is collected by email or a website, the mechanism for withdrawing it should be the same, not an alternative solution such as phone or fax.

Modifying consent can include placing restrictions on the processing of PII, which can include restricting the PII controller from deleting the PII in some cases.

Some jurisdictions impose restrictions on the circumstances under which, and the extent to which, a PII principal can modify or withdraw their consent.

The organization should record any request to withdraw or change consent in a similar way to the recording of the consent itself.

Any change of consent should be disseminated, through appropriate systems, to authorized users and to relevant third parties.

The organization should define a response time and requests should be handled according to it.

Additional information

When consent for particular processing of PII is withdrawn, all the processing of PII performed before withdrawal should normally be considered as appropriate, but the results of such processing should not be used for new processing. For example, if a PII principal withdraws their consent for profiling, their profile should not be further used or consulted.

7.3.5 Provide mechanism to object to PII processing

Control

The organization should provide a mechanism for PII principals to object to the processing of their PII.

Implementation guidance

Some jurisdictions provide PII principals with a right to object to the processing of their PII. Organizations operating in these jurisdictions should ensure that they implement appropriate measures to enable PII principals to exercise this right.

The organization should document the legal and regulatory requirements related to objections by the PII principals to processing (e.g., objection relating to the processing of PII for direct marketing purposes). The organization should provide information to principals regarding the ability to object in these situations. Mechanisms to object can vary, but should be consistent with the type of service provided (e.g., online services should provide this capability online).

7.3.6 Access, correction and/or erasure

Control

The organization should implement policies, procedures and/or mechanisms to meet their obligations to PII principals to access, correct and/or erase their PII.

Implementation guidance

The organization should implement policies, procedures and/or mechanisms for enabling PII principals to obtain access to, correction and erasure of their PII, if requested and without undue delay, if not against applicable laws.

The organization should define a response time and requests should be handled according to it.

Any corrections or erasures should be disseminated through the system and/or to authorized users, and should be passed to third parties (see 7.3.7) to whom the PII has been transferred.

NOTE Records generated by the control specified in 7.5.3 could help in this regard.

The organization should implement policies, procedures and/or mechanisms for use when there could be a dispute about the accuracy or correction of the data by the PII principal. These policies, procedures and/or mechanisms should include informing the PII principal of what changes were made, and of reasons why corrections could not be made (where this is the case).

Some jurisdictions impose restrictions on the circumstances under which, and the extent to which, a PII principal can request correction or erasure of their PII. The organization should determine, keep up to date and abide by, any such restrictions that could be applicable.

7.3.7 PII controllers' obligations to inform third parties

Control

The organization should implement policies, procedures and/or mechanisms to inform third parties with whom the PII has been shared of any modification, withdrawal or objections pertaining to the shared PII.

Implementation guidance

Some jurisdictions impose a legal requirement to inform these third parties of these results.

The organization should take appropriate steps, bearing in mind the available technology, to inform third parties of any modification or withdrawal of consent, or objections pertaining to the shared PII.

The organization should determine and maintain active communication channels with third parties. Related responsibilities can be assigned to individuals in charge of their operations and maintenance. When informing third parties, the organization should monitor their acknowledgement of receipt of the information.

NOTE Changes resulting from the obligations to PII principals could include modification or withdrawal of consent, requests for correction, erasure, or restrictions on processing, or objections to the processing of PII as requested by the PII principal.

7.3.8 Providing copy of PII processed

Control

The organization should be able to provide a copy of the PII that is being processed when requested by the PII principal.

Implementation guidance

The organization should provide a copy of the PII that is being processed in a structured, commonly used, format accessible by the PII principal.

Some jurisdictions define cases where the organization should provide a copy of the PII being processed in a format allowing portability to the PII principals or to recipient PII controllers (typically structured, commonly used and machine readable).

The organization should ensure that any copies of PII provided to a PII principal relate specifically to that PII principal.

Where the requested PII has already been deleted subject to the retention and disposal policy (as described in 7.4.6), the PII controller should inform the PII principal that the requested PII has been deleted.

In cases where the organization is no longer able to identify the PII principal (e.g. as a result of a de-identification process), the organization should not seek to (re-)identify the PII principals for the sole reason of implementing this control. In this case, additional information should be requested from the PII principal to enable re-identification and subsequent disclosure.

Where technically feasible, it should be possible to transfer a copy of the PII from one organization directly to another organization, at the request of the PII principal.

7.3.9 Handling requests

Control

The organization should define and document policies and procedures for handling and responding to legitimate requests from PII principals.

Implementation guidance

Legitimate requests could include requests for a copy of PII being processed, or requests to lodge a complaint.

Some jurisdictions allow the organization to charge a fee in certain cases (e.g., excessive or repetitive requests).

Requests should be handled within the appropriate defined response times and in accordance with applicable legislation and/or regulation.

Some jurisdictions define response times, depending on the complexity and number of the requests, as well as requirements to inform PII principals of any delay. The appropriate response times should be defined in the privacy policy.

7.3.10 Automated decision making

Control

The organization should identify and address all obligations, including legal obligations, to the PII principals resulting from decisions made by the organization and related to the PII principal based solely on automated processing of PII.

Implementation guidance

Some jurisdictions define specific obligations to PII principals when a decision based solely on automated processing of PII significantly affects them, such as notifying the existence of automated decision making, allowing for the PII principals to object to such decision making, and/or obtaining human intervention.

NOTE In some jurisdictions, some processing of PII cannot be fully automated.

Organizations operating in these jurisdictions should ensure that they comply with these obligations.

7.4 Privacy by design and privacy by 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.

7.4.1 Limit collection

Control

The organization should limit the collection of PII to the minimum that is relevant, proportional and necessary for the identified purposes.

Implementation guidance

The organization should limit the collection of PII to what is adequate, relevant and necessary in relation to the identified purposes. This includes limiting the amount of PII that the organization collects indirectly (e.g., through web logs, system logs, etc.).

Privacy by default implies that, where any optionality in the collection and processing of PII exists, each option should be disabled by default and only enabled by explicit choice of the PII principal.

7.4.2 Limit processing

Control

The organization should limit the processing of PII to that which is adequate, relevant and necessary for the identified purposes.

Implementation guidance

Limiting the processing of PII needs to be managed through information security and privacy policies (see 6.2) along with documented procedures for their adoption and compliance.

Processing of PII, including the period of PII storage and who is able to access the PII, should be limited by default to the minimum necessary relative to the identified purposes.

7.4.3 Accuracy and quality

Control

The organization should ensure and document that PII is as accurate, complete and up-to-date as is necessary for the purposes for which it is to be processed, throughout the life-cycle of the PII.

Implementation guidance

The organization should implement policies, procedures and/or mechanisms to minimize inaccuracies in the PII it processes. There should also be policies, procedures and/or mechanisms to respond to instances of inaccurate PII. These policies, procedures and/or mechanisms should be well documented (e.g., through technical system configurations, etc.) and should apply throughout the PII lifecycle.

Additional information

For further information on the PII processing life-cycle, see ISO/IEC 29101:2013, 6.2.

7.4.4 PII minimization and de-identification objectives

Control

The organization should define and document data minimization objectives and how those objectives are met, including what mechanisms (such as de-identification) are used.

Implementation guidance

Organizations should identify how the specific PII and amount of PII collected and processed is limited relative to the identified purposes: this can include the use of de-identification or other data minimization techniques.

The identified purpose (see 7.2.1) can require the processing of PII that has not been de-identified, in which case the organization should be able to describe such processing.

In other cases, the identified purpose might not require the processing of the original PII, and the processing of PII which has been de-identified can suffice to achieve the identified purpose. In these cases, the organization should define and document the extent to which the PII needs to be associated with the PII principal, as well as the mechanisms and techniques designed to process PII, such that the de-identification and/or PII minimization objectives are achieved.

Mechanisms used to minimize PII will vary depending on the type of processing and the systems used for the processing. The organization should document any mechanisms (technical system configurations, etc.) used to implement data minimization.

In those cases where processing of de-identified data is sufficient for the purposes, the organization should document any mechanisms (technical system configurations, etc.) designed to implement de-identification objectives set by the organization in a timely manner. For instance, the removal of attributes associated with PII principals can be sufficient to allow the organization to achieve its identified purpose. In other cases, other de-identification techniques, such as generalization (e.g., rounding) or randomization techniques (e.g., noise addition) can be used to achieve an adequate level of de-identification.

NOTE 1 For further information on de-identification techniques, refer to ISO IEC 20889.

NOTE 2 For Cloud computing, ISO/IEC 19944 provides a definition of data identification qualifiers that can be used to classify the degree to which the data can identify a PII principal or associate a PII principal with a set of characteristics in the PII.

7.4.5 PII de-identification and deletion at the end of processing

Control

The organization should either delete PII or render it in a form which does not permit (re-)identification of PII principals, as soon as the original PII is no longer necessary for the identified purpose(s).

Implementation guidance

The organization should have mechanisms to erase the PII when no further processing is anticipated. Alternatively, some de-identification techniques can be used as long as the resulting de-identified data cannot reasonably permit re-identification of PII principals.

7.4.6 Temporary files

Control

The organization should ensure that temporary files created as a result of the processing of PII are disposed of (e.g., erased or destroyed) following documented procedures within a specified, documented period.

Implementation guidance

The organization should perform periodic checks that unused temporary files are deleted within the identified time period.

Other information

Information systems can create temporary files in the normal course of their operation. Such files are specific to the system or application, but can include file system roll-back journals and temporary files associated with the updating of databases and the operation of other application software. Temporary files are not needed after the related information processing task has completed but there are circumstances in which they cannot be deleted. The length of time for which these files remain in use is not always deterministic but a “garbage collection” procedure should identify the relevant files and determine how long it has been since they were last used.

7.4.7 Retention

Control

The organization should not retain PII for longer than is necessary for the purposes for which the PII is processed.

Implementation guidance

The organization should develop and maintain retention schedules for information it retains, taking into account the requirement to retain PII for no longer than is necessary. Such schedules should take into account legal, regulatory and business requirements. Where such requirements conflict, a business decision needs to be taken (based on a risk assessment) and documented in the appropriate schedule.

7.4.8 Disposal

Control

The organization should have documented policies, procedures and/or mechanisms for the disposal of PII.

Implementation guidance

The choice of PII disposal techniques will depend on a number of factors, as disposal techniques differ in their properties and outcomes (for example in the granularity of the resultant physical media, or the ability to recover deleted information on electronic media). Factors to consider when choosing an appropriate disposal technique include, but are not limited to, the nature and extent of the PII to be disposed of, whether or not there is metadata associated with the PII, and the physical characteristics of the media upon which the PII is stored.

7.4.9 PII transmission controls

Control

The organization should subject PII transmitted (e.g. sent to another organization) over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.

Implementation guidance

Transmission of PII needs to be controlled, typically by ensuring that only authorized individuals have access to transmission systems, and by following the appropriate processes (including the retention of audit logs) to ensure that PII is transmitted without compromise to the correct recipients.

7.5 PII sharing, transfer, and disclosure

Objective: To ensure that PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.

7.5.1 Identify basis for PII transfer between jurisdictions

Control

The organization should identify and document the relevant basis for transfers of PII between jurisdictions.

Implementation guidance

PII transfer can be subject to laws or regulations depending on the jurisdiction or international organization to which data is to be transferred (and from where it originates). The organization should document compliance to such requirements as the basis for transfer.

Some jurisdictions may require that information transfer agreements be reviewed by a designated supervisory authority. Organizations operating in such jurisdictions should ensure they are aware of any such requirements.

NOTE Where transfers take place within a specific jurisdiction, the applicable laws and regulations will be the same for the sender and recipient.

7.5.2 Countries and international organizations to which PII might be transferred

Control

The organization should specify and document the countries and international organizations to which PII might possibly be transferred.

Implementation guidance

The identities of the countries and international organizations to which PII might possibly be transferred in normal operations should be made available to customers. The identities of the countries arising from the use of subcontracted PII processing should be included. The countries included should be considered in relation to 7.5.1 and any applicable legal or regulatory requirements.

Out of normal operations, there can be cases of transfer made at the request of a law enforcement authority, for which the identity of the countries cannot be specified in advance, or is prohibited by applicable jurisdictions to preserve the confidentiality of a law enforcement investigation (see 7.5.1, 8.5.4 and 8.5.5).

7.5.3 Records of transfer of PII

Control

The organization should record transfers of PII to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the PII principals.

Implementation guidance

Recording can include transfers from third parties of PII which has been modified as a result of PII controllers' managing their obligations, or transfers to third parties to implement legitimate requests from PII principals, including requests to erase PII (e.g., after consent withdrawal).

The organization should have a policy defining the amount of time these records are maintained.

The organization should apply the minimization principle to the records of transfers by collecting only the strictly needed information.

7.5.4 Records of PII disclosure to third parties

Control

The organization should record disclosures of PII to third parties, including what PII has been disclosed, to whom and at what time.

Implementation guidance

PII can be disclosed during the course of normal operations. These disclosures should be recorded. Any additional disclosures to third parties, such as those arising from lawful investigations or external audits, should also be recorded. The records should include the source of the disclosure and the source of the authority to make the disclosure.

8 Additional ISO/IEC 27002 guidance for PII processors

8.1 General

The guidance contained in ISO/IEC 27002:2013 plus the additions of this clause create the PIMS-specific guidance for PII processors. The implementation guidance documented in clause 8 relate to the controls listed in Annex B.

8.2 Conditions for collection and processing

Objective: To ensure that processing is lawful, based on legitimate purposes or consent, and/or other bases as applicable by jurisdiction.

8.2.1 Cooperation agreement

Control

The organization should ensure that the contract to process PII addresses (wherever relevant and taking into account the nature of processing and the information available to the organization) the organization’s role in providing assistance with the customer’s obligations.

Implementation guidance

The contract between the organization and the customer should, wherever relevant, and depending upon the customer's role (PII controller or PII processor), include (this list is neither definitive nor exhaustive):

- Privacy by Design and Privacy by Default (see 7.4, 8.4);
- Achieving security of processing;
- Notification of personal data breaches to a supervisory authority;
- Notification of personal data breaches to customers and PII principals;
- Conducting Privacy Impact Assessments (PIA); and
- The assurance of assistance by the PII processor if prior consultations with relevant PII protection authorities are needed.

Some jurisdictions require that the contract include the subject matter and duration of the processing, the nature and purpose of the processing, the type of PII and categories of PII principals.

8.2.2 Organization's purposes

Control

The organization should ensure that PII processed on behalf of a customer is not processed for any purpose independent of the documented instructions of the customer.

Implementation guidance

The contract between the organization and the customer should include, but not be limited to, the objective and time frame to be achieved by the service.

In order to achieve the customer's purpose, there could be technical reasons why it is appropriate for the organization to determine the method for processing PII, consistent with the general instructions of the customer but without the customer's express instruction. For example, in order to efficiently utilize network or processing capacity it can be necessary to allocate specific processing resources depending on certain characteristics of the PII principal.

The organization should allow the customer to verify their compliance with the purpose specification and limitation principles. This will also ensure that no PII is processed by the organization or any of its subcontractors for further purposes independent of the instructions of the customer.

8.2.3 Marketing and advertising use

Control

The organization should not use PII processed under a contract for the purposes of marketing and advertising without prior consent from the appropriate PII principal. The organization should not make providing such consent a condition for receiving the service.

Implementation guidance

PII processors need to comply with the customer's contractual requirements, especially where marketing and/or advertising is planned.

Organizations should not insist on the inclusion of marketing and/or advertising uses where express consent has not been fairly obtained from PII principals.

NOTE This control is in addition to the more general control in 8.2.2 and does not replace or otherwise supersede it.

8.2.4 Infringing instruction

Control

The organization should inform the customer if, in its opinion, a processing instruction infringes applicable legislation or regulation.

Implementation guidance

The organization's ability to check if the instruction infringes legislation can depend on the technological context, on the instruction itself, and on the contract between the organization and the customer.

8.2.5 Customer obligations

Control

The organization should provide the customer with the appropriate information such that it can demonstrate compliance with its obligations.

Implementation guidance

The information needed by the customer might include whether the organization allows for and contributes to audits, including inspections, conducted by the customer or another auditor mandated or otherwise agreed by the customer.

8.2.6 Records related to processing PII

Control

The organization should determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable agreement) for the processing of PII carried out on behalf of a customer.

Implementation guidance

Some jurisdictions can require the organization to record information such as:

- categories of processing carried out on behalf of each customer;
- transfers to third countries or international organizations; and
- a general description of the technical and organizational security measures.

8.3 Obligations to PII principals

Objective: To ensure that PII principals are provided with the 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.

8.3.1 Obligations to PII principals

Control

The organization should provide the customer with the means to comply with its obligations related to PII principals.

Implementation guidance

A PII controller's obligations can be defined by law, by regulations or by contract. These obligations can include matters where the customer uses the services of the organization for implementation of these obligations. For example, this could include the correction or deletion of PII in a timely fashion.

Where a customer depends on the organization for information or technical measures to facilitate meeting the obligations to PII principals rights, the relevant information or technical measures should be specified in a contract.

8.4 Privacy by design and privacy by 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.

8.4.1 Temporary files

Control

The organization should ensure that temporary files created as a result of the processing of PII are disposed of (e.g., erased or destroyed) following documented procedures within a specified, documented period.

Implementation guidance

The organization should perform periodic checks that unused temporary files are deleted within the identified time period.

Other information

Information systems can create temporary files in the normal course of their operation. Such files are specific to the system or application, but can include file system roll-back journals and temporary files associated with the updating of databases and the operation of other application software. Temporary files are not needed after the related information processing task has completed but there are circumstances in which they cannot be deleted. The length of time for which these files remain in use is not always deterministic but a “garbage collection” procedure should identify the relevant files and determine how long it has been since they were last used.

8.4.2 Return, transfer or disposal of PII

Control

The organization should provide a capability for the return, transfer and/or disposal of PII in a secure manner and should make its policy for the exercise of this capability available to the customer.

Implementation guidance

At some point in time, PII might need to be disposed of in some manner. This can involve returning the PII to the customer, transferring it to another organization or to a PII controller (e.g., as a result of a merger), deleting or otherwise destroying it, de-identifying it or archiving it. Such capabilities should be managed in a secure manner.

The organization should provide the assurance necessary to allow the customer to ensure that PII processed under a contract is erased (by the organization and any of its subcontractors) from wherever they are stored, including for the purposes of backup and business continuity, as soon as they are no longer necessary for the identified purposes of the customer.

The organization should develop and implement a policy in respect of the disposition of PII and should make this policy available to customer when requested.

The policy should cover the retention period for PII before its disposal after termination of a contract, to protect the customer from losing PII through an accidental lapse of the contract.

NOTE This control and guidance is also relevant under the retention principle (see 7.4.8).

8.4.3 PII transmission controls

Control

The organization should subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.

Implementation guidance

Transmission of PII needs to be controlled, typically by ensuring that only authorized individuals have access to transmission systems, and by following the appropriate processes (including the retention of audit data) to ensure that PII is transmitted without compromise to the correct recipients. Requirements for transmission controls can be included in the PII processor – customer contract; if so these requirements should ensure that these requirements are met.

Where no contractual requirements related to transmission are in place, it can be appropriate to take advice from the customer prior to transmission.

8.5 PII sharing, transfer, and disclosure

Objective: To ensure that PII is shared, transferred to other jurisdictions or third parties, and/or disclosed in accordance with applicable obligations.

8.5.1 Basis for PII transfer between jurisdictions

Control

The organization should inform the customer in a timely manner of the basis for PII transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract.

Implementation guidance

PII transfer between jurisdictions can be subject to laws or regulations depending on the jurisdiction or organization to which PII is to be transferred (and from where it originates). The organization should document compliance with such requirements as the basis for transfer.

The organization should inform the customer of any transfer of PII, including transfers to:

- suppliers;
- other parties;
- other countries or international organizations.

In case of changes, the organization should inform the customer in advance, according to an agreed timeframe, so that the customer has the ability to object to such changes or to terminate the contract.

The agreement between the organization and the customer can have clauses where the organization can implement changes without informing the customer. In these cases, the limits of this allowance should be set (e.g. the organization can change suppliers without informing the customer, but cannot transfer PII to other countries).

In case of international transfer of PII, agreements such as Model Contract Clauses, Binding Corporate Rules or Cross Border Privacy Rules, the countries involved and the circumstances in which such agreements apply, should be identified.

8.5.2 Countries and international organizations to which PII might be transferred

Control

The organization should specify and document the countries and international organizations to which PII might possibly be transferred.

Implementation guidance

The identities of the countries and international organizations to which PII might possibly be transferred in normal operations should be made available to customers. The identities of the countries arising from the use of subcontracted PII processing should be included. The countries included should be considered in relation to 8.5.1 and any applicable legal or regulatory requirements.

Out of normal operations, there can be cases of transfer made at the request of a law enforcement authority, for which the identity of the countries cannot be specified in advance, or is prohibited by applicable jurisdictions to preserve the confidentiality of a law enforcement investigation (see 7.5.1, 8.5.4 and 8.5.5).

8.5.3 Records of PII disclosure to third parties

Control

The organization should record disclosures of PII to third parties, including what PII has been disclosed, to whom and when.

Implementation guidance

PII can be disclosed during the course of normal operations. These disclosures should be recorded. Any additional disclosures to third parties, such as those arising from lawful investigations or external audits, should also be recorded. The records should include the source of the disclosure and the source of the authority to make the disclosure.

8.5.4 Notification of PII disclosure requests

Control

The organization should notify the customer of any legally binding requests for disclosure of PII, unless otherwise prohibited by law.

Implementation guidance

The organization can receive legally binding requests for disclosure of PII (e.g. from law enforcement authorities). In these cases, and where permitted by law, the organization should notify the customer of any such request within agreed timeframes and according to an agreed procedure (which may be included in the data processing contract).

In some cases, the legally binding requests include the requirement for the organization not to notify anyone about the event (an example of a possible prohibition on disclosure would be a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

8.5.5 Legally binding PII disclosures

Control

The organization should reject any requests for PII disclosures that are not legally binding, consult the corresponding customer where legally permissible before making any PII disclosures and accepting any contractually agreed requests for PII disclosures that are authorized by the corresponding customer.

Implementation guidance

Details relevant to the implementation of the control can be included in the data processing contract.

Such requests might originate from several sources, including courts, tribunals and administrative authorities. They can arise from any jurisdiction.

8.5.6 Disclosure of subcontractors used to process PII

Control

The organization should disclose any use of subcontractors to process PII to the customer before use.

Implementation guidance

Provisions for the use of subcontractors to process PII should be included in the contract between the organization and the customer.

Information disclosed should cover the fact that subcontracting is used and the names of relevant subcontractors. The information disclosed should also include the countries and international organisations to which subcontractors can transfer data (see 8.5.2) and the means by which subcontractors are obliged to meet or exceed the obligations of the organization (see 8.5.7).

Where public disclosure of subcontractor information is assessed to increase security risk beyond acceptable limits, disclosure should be made under a non-disclosure agreement and/or on the request of the customer. The customer should be made aware that the information is available.

This does not concern the list of countries where the PII might be transferred. This list should be disclosed to the customer in all cases in a way that allow them to inform the appropriate PII principals.

8.5.7 Engagement of a subcontractor to process PII

Control

The organization should only engage a subcontractor to process PII according to the contract agreed with the customer.

Implementation guidance

Where the organization subcontracts some or all of the processing of that PII to another organization, then written authorization from the customer is required prior to the PII being processed by the subcontractor. This can be in the form of appropriate clauses in the PII processor – customer agreement, or can be a specific 'one-off' agreement.

The organization should have a written contract with any sub-contractors that it uses, and should ensure that their contracts with sub-contractors address the implementation of the appropriate controls in Annex B.

The contract between the organization and any sub-contractor processing PII on its behalf should require the sub-contractor to implement the appropriate controls specified in Annex B, taking account of the information security risk assessment process (see 5.4.1.2) and the scope of the processing of PII performed by the PII processor (see 6.12). By default, all controls specified in Annex B should be assumed as relevant. If the organization decides to not require the sub-contractor to implement a control from Annex B, it should justify its exclusion.

A contract can define the responsibilities of each party differently but, to be consistent with this document, all controls should be considered and documented.

8.5.8 Change of subcontractor to process PII

Control

The organization should, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to object to such changes.

Implementation guidance

Where the organization changes the organization with which it subcontracts some or all of the processing of that PII, then written authorization from the customer is required for the change, prior to the PII being processed by the new subcontractor. This can be in the form of appropriate clauses in the PII processor – customer agreement, or can be a specific 'one-off' agreement.

Annex A
(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 extends Annex A of ISO/IEC 27001:2013.

The additional or modified control objectives and controls listed in Table A.1 are directly derived from and aligned with those defined in this document and are to be used in context with ISO/IEC 27001:2013, 6.1.3 as refined by Clause 5.3 of this document.

Not all the control objectives and controls listed in this Annex need to be included in the PIMS implementation. A justification for excluding any control objectives shall be included in the Statement of Applicability (see 5.4.1.3). Justification for exclusion may include where the controls are not deemed necessary by the risk assessment, or where they are not required by (or are subject to exceptions under) the laws and/or regulations applicable to the PII principal.

NOTE Section numbers in this Annex relate to the paragraph numbers in section 7 of this document.

Table A.1 — Control objectives and controls

A.7.2 Conditions for collection and processing Objective: To ensure that processing is lawful, with legal basis as per applicable jurisdictions, with clearly defined and legitimate purposes.		
A.7.2.1	Identify and document purpose	*Control* The organization shall identify and document the specific purposes for which the PII will be processed.
A.7.2.2	Identify lawful basis	*Control* The organization shall determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes.
A.7.2.3	Determine when and how consent is to be obtained	*Control* The organization shall determine and document a process by which it can demonstrate if, when and how consent for the processing of PII was obtained from PII principals
A.7.2.4	Obtain and record consent	*Control* The organization shall obtain and record consent from PII principals according to the documented processes.

A.7.2.5	Privacy impact assessment	*Control* The organization shall assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of PII or changes to existing processing of PII is planned.
A.7.2.6	Contracts with PII processors	*Control* The organization shall have a written contract with any PII processor that it uses, and shall ensure that their contracts with PII processors address the implementation of the appropriate controls in Annex B.
A.7.2.7	Joint PII controller	*Control* The organization shall determine respective roles and responsibilities for the processing of PII (including PII protection and security requirements) with any joint PII controller.
A.7.2.8	Records related to processing PII	*Control* The organization shall determine and securely maintain the necessary records in support of its obligations for the processing of PII.
A.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.		
A.7.3.1	Determining and fulfilling obligations to PII principals	*Control* The organization shall determine, document and comply with their legal, regulatory and business obligations to PII principals, related to the processing of their PII and provide the means to meet these obligations.
A.7.3.2	Determining information for PII principals	*Control* The organization shall determine and document the information which is to be provided to PII principals regarding the processing of their PII and the timing of such a provision.
A.7.3.3	Providing information to PII principals	*Control* The organization shall provide PII principals with clear and easily accessible information related to the PII controller and the processing of their PII.
A.7.3.4	Provide mechanism to modify or withdraw consent	*Control* The organization shall provide a mechanism for PII principals to modify or withdraw their consent.

A.7.3.5	Provide mechanism to object to PII processing	*Control* The organization shall provide a mechanism for PII principals to object to the processing of their PII.
A.7.3.6	Access, correction and/or erasure	*Control* The organization shall implement policies, procedures and/or mechanisms to meet their obligations to PII principals to access, correct and/or erase their PII.
A.7.3.7	PII controllers' obligations to inform third parties	*Control* The organization shall implement policies, procedures and mechanisms to inform third parties with whom the PII has been shared of any modification, withdrawal or objections pertaining to the shared PII.
A.7.3.8	Providing copy of PII processed	*Control* The organization shall be able to provide a copy of the PII that is being processed when requested by the PII principal.
A.7.3.9	Handling requests	*Control* The organization shall define and document policies and procedures for handling and responding to legitimate requests from PII principals.
A.7.3.10	Automated decision making	*Control* The organization shall identify and address all obligations, including legal obligations, to the PII principals resulting from decisions made by the organization and related to the PII principal based solely on automated processing of PII.
A.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.		
A.7.4.1	Limit collection	*Control* The organization shall limit the collection of PII to the minimum that is relevant, proportional and necessary for the identified purposes.
A.7.4.2	Limit processing	*Control* The organization shall limit the processing of PII to that which is adequate, relevant and necessary for the identified purposes.

A.7.4.3	Accuracy and quality	*Control* The organization shall ensure and document that PII is as accurate, complete and up-to-date as is necessary for the purposes for which it is to be processed, throughout the life-cycle of the PII.
A.7.4.4	PII minimization and de-identification objectives	*Control* The organization should define and document data minimization objectives and how those objectives are met, including what mechanisms (such as de-identification) are used.
A.7.4.5	PII de-identification and deletion at the end of processing	*Control* The organization shall either delete PII or render it in a form which does not permit (re-)identification of PII principals, as soon as the original PII is no longer necessary for the identified purpose(s).
A.7.4.6	Temporary files	*Control* The organization shall ensure that temporary files created as a result of the processing of PII are disposed of (e.g., erased or destroyed) following documented procedures within a specified, documented period.
A.7.4.7	Retention	*Control* The organization shall not retain PII for longer than is necessary for the purposes for which the PII is processed.
A.7.4.8	Disposal	*Control* The organization shall have documented policies, procedures and/or mechanisms for the disposal of PII.
A.7.4.9	PII transmission controls	*Control* The organization shall subject PII transmitted (e.g. sent to another organization) over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.
A.7.5 PII sharing, transfer and disclosure Objective: To ensure that PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.		
A.7.5.1	Identify basis for PII transfer between jurisdictions	*Control* The organization shall identify and document the relevant basis for transfers of PII between jurisdictions.

A.7.5.2	Countries and international organizations to which PII might be transferred	*Control* The organization shall specify and document the countries and international organizations to which PII might possibly be transferred.
A.7.5.3	Records of transfer of PII	*Control* The organization shall record transfers of PII to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the PII principals.
A.7.5.4	Records of PII disclosures to third parties	*Control* The organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and at what time.

1898

1899

Annex B
(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 extends Annex A of ISO/IEC 27001:2013.

The additional or modified control objectives and controls listed in Table B.1 are directly derived from and aligned with those defined in this document and are to be used in context with ISO/IEC 27001:2013, 6.1.3 as refined by this document.

Not all the control objectives and controls listed in this Annex need to be included in the PIMS implementation. A justification for excluding any control objectives shall be included in the Statement of Applicability (see 5.4.1.3). Justification for exclusion may include where the controls are not deemed necessary by the risk assessment, or where they are not required by (or are subject to exceptions under) the laws and/or regulations applicable to the PII principal.

NOTE Section numbers in this Annex relate to the paragraph numbers in section 7 of this document.

Table B.1 — Control objectives and controls

B.8.2 Conditions for collection and processing Objective: To ensure that processing is lawful, based on legitimate purposes or consent, and/or other bases as applicable by jurisdiction.		
B.8.2.1	Cooperation agreement	*Control* The organization shall ensure that the contract to process PII addresses (wherever relevant and taking into account the nature of processing and the information available to the organization) the organization's role in providing assistance with the customer's obligations.
B.8.2.2	Organization's purposes	*Control* The organization shall ensure that PII processed on behalf of a customer is not processed for any purpose independent of the documented instructions of the customer.
B.8.2.3	Marketing and advertising use	*Control* The organization shall not use PII processed under a contract for the purposes of marketing and advertising without prior consent from the appropriate PII principal. The organization shall not make providing such consent a condition for receiving the service.
B.8.2.4	Infringing instruction	*Control* The organization shall inform the customer if, in its opinion, a processing instruction infringes applicable legislation or regulation.

B.8.2.5	Customer obligations	*Control* The organization shall provide the customer with the appropriate information such that it can demonstrate compliance with its obligations.
B.8.2.6	Records related to processing PII	*Control* The organization shall determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable agreement) for the processing of PII carried out on behalf of a customer.
B.8.3 Obligations to PII principals Objective: To ensure that PII principals are provided with the 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.8.3.1	Obligations to PII principals	*Control* The organization shall provide the customer with the means to comply with its obligations related to PII principals.
B.8.4 Privacy by design and privacy by 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.8.4.1	Temporary files	*Control* The organization shall ensure that temporary files created as a result of the processing of PII are disposed of (e.g., erased or destroyed) following documented procedures within a specified, documented period.
B.8.4.2	Return, transfer or disposal of PII	*Control* The organization shall provide a capability for the return, transfer and/or disposal of PII in a secure manner and shall make its policy for the exercise of this capability available to the customer.
B.8.4.3	PII transmission controls	*Control* The organization shall subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.
B.8.5 PII sharing, transfer and disclosure Objective: To ensure that PII is shared, transferred to other jurisdiction or third parties, and/or disclosed in accordance with applicable obligations.		

B.8.5.1	Basis for PII transfer between jurisdictions	*Control* The organization shall inform the customer in a timely manner of the basis for PII transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract.
B.8.5.2	Countries and international organizations to which PII might be transferred	*Control* The organization shall specify and document the countries and international organizations to which PII might possibly be transferred.
B.8.5.3	Records of PII disclosures to third parties	*Control* The organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and when.
B.8.5.4	Notification of PII disclosure requests	*Control* The organization shall notify the customer of any legally binding requests for disclosure of PII, unless otherwise prohibited by law.
B.8.5.5	Legally binding PII disclosures	*Control* The organization shall reject any requests for PII disclosures that are not legally binding, consult the corresponding customer where legally permissible before making any PII disclosures and accepting any contractually agreed requests for PII disclosures that are authorized by the corresponding customer.
B.8.5.6	Disclosures of subcontractors used to process PII	*Control* The organization shall disclose any use of subcontractors to process PII to the customer before use.
B.8.5.7	Engagement of a subcontractor to process PII	*Control* The organization shall only engage a subcontractor to process PII according to the contract agreed with the customer.
B.8.5.8	Change of subcontractor to process PII	*Control* The organization shall, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to object to such changes.

1916

1917

Annex C
(informative)

Mapping to the General Data Protection Regulation

This table gives an indicative mapping between provisions of this document and Articles 5 to 49 except 43 of the General Data Protection Regulation of the European Union. It shows how compliance to requirements and controls of this document can be relevant to fulfil obligations of GDPR.

However it is purely indicative and as per this document, it is the organizations responsibility to assess its legal obligations and decide how to comply with them.

C.1 Mapping ISO/IEC 27552 structure to GDPR articles

ISO/IEC 27552 sub-clause	GDPR article
5.2.1	(23)(1)(a), (23)(1)(b), (23)(1)(c), (23)(1)(d), (23)(1)(e), (23)(1)(f), (23)(1)(g), (23)(1)(h), (23)(1)(i), (23)(1)(j), (23)(2)(a), (23)(2)(b), (23)(2)(c), (23)(2)(d), (23)(2)(e), (23)(2)(f), (23)(2)(g), (23)(2)(h), (24)(3), (25)(3), (28)(5), (28)(6), (28)(7), (28)(8), (28)(10), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)
5.2.2	(31), (35)(9), (36)(1), (36)(2), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(4), (36)(5)
5.2.3	(32)(2)
5.2.4	(32)(2)
5.4.1.2	(32)(1)(b), (32)(2)
5.4.1.3	(32)(1)(b), (32)(2)
6.2.1.1	(24)(2)
6.3.1.1	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)
6.4.2.2	(39)(1)(b)
6.5.2.1	(5)(1)(f), (32)(2)
6.5.3.1	(5)(1)(f), (32)(1)(a)
6.5.3.3	(5)(1)(f), (32)(1)(a)
6.6.2.1	(5)(1)(f)
6.6.2.2	(5)(1)(f)
6.6.4.2	(5)(1)(f)
6.7.1.1	(32)(1)(a)
6.8.2.7	(5)(1)(f)
6.8.2.9	(5)(1)(f)

6.9.3.1	(5)(1)(f), (32)(1)(c)
6.9.4.1	(5)(1)(f)
6.9.4.2	(5)(1)(f)
6.10.2.1	(5)(1)(f)
6.10.2.4	(5)(1)(f), (28)(3)(b), (38)(5)
6.11.1.2	(5)(1)(f), (32)(1)(a)
6.11.2.5	(25)(1)
6.11.3.1	(5)(1)(f)
6.12.1.2	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
6.13.1.1	(5)(1)(f), (33)(1), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2), (34)(3)(a), (34)(3)(b), (34)(3)(c), (34)(4)
6.13.1.5	(33)(1), (33)(2), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2)
6.15.1.1	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
6.15.1.3	(5)(2), (24)(2)
6.15.2.1	(32)(1)(d), (32)(2)
6.15.2.3	(32)(1)(d), (32)(2)
7.2.1	(5)(1)(b), (32)(4)
7.2.2	(10), (5)(1)(a), (6)(1)(a), (6)(1)(b), (6)(1)(c), (6)(1)(d), (6)(1)(e), (6)(1)(f), (6)(2), (6)(3), (6)(4)(a), (6)(4)(b), (6)(4)(c), (6)(4)(d), (6)(4)(e), (8)(3), (9)(1), (9)(2)(b), (9)(2)(c), (9)(2)(d), (9)(2)(e), (9)(2)(f), (9)(2)(g), (9)(2)(h), (9)(2)(i), (9)(2)(j), (9)(3), (9)(4), (17)(3)(a), (17)(3)(b), (17)(3)(c), (17)(3)(d), (17)(3)(e), (18)(2), (22)(2)(a), (22)(2)(b), (22)(2)(c), (22)(4)
7.2.3	(8)(1), (8)(2)
7.2.4	(7)(1), (7)(2), (9)(2)(a)
7.2.5	(35)(1), (35)(2), (35)(3)(a), (35)(3)(b), (35)(3)(c), (35)(4), (35)(5), (35)(7)(a), (35)(7)(b), (35)(7)(c), (35)(7)(d), (35)(8), (35)(9), (35)(10), (35)(11), (36)(1), (36)(2), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(4), (36)(5)
7.2.6	(5)(2), (28)(3)(e), (28)(9)
7.2.7	(26)(1), (26)(2), (26)(3)
7.2.8	(5)(2), (24)(1), (30)(1)(a), (30)(1)(b), (30)(1)(c), (30)(1)(d), (30)(1)(f), (30)(1)(g), (30)(3), (30)(4), (30)(5)
7.3.1	(12)(2)
7.3.2	(11)(2), (13)(3), (13)(1)(a), (13)(1)(b), (13)(1)(c), (13)(1)(d), (13)(1)(e), (13)(1)(f), (13)(2)(c), (13)(2)(d), (13)(2)(e), (13)(4), (14)(1)(a), (14)(1)(b), (14)(1)(c), (14)(1)(d), (14)(1)(e), (14)(1)(f), (14)(2)(b), (14)(2)(e), (14)(2)(f), (14)(3)(a), (14)(3)(b), (14)(3)(c), (14)(4), (14)(5)(a), (14)(5)(b), (14)(5)(c), (14)(5)(d), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (15)(2), (18)(3), (21)(4)
7.3.3	(11)(2), (12)(1), (12)(7), (12)(8), (13)(3), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (21)(4)
7.3.4	(7)(3), (13)(2)(c), (14)(2)(d), (18)(1)(a), (18)(1)(b), (18)(1)(c), (18)(1)(d)
7.3.5	(13)(2)(b), (14)(2)(c), (21)(1), (21)(2), (21)(3), (21)(5), (21)(6)

7.3.6	(5)(1)(d), (13)(2)(b), (14)(2)(c), (16), (17)(1)(a), (17)(1)(b), (17)(1)(c), (17)(1)(d), (17)(1)(e), (17)(1)(f), (17)(2)
7.3.7	(19)
7.3.8	(13)(2)(b), (14)(2)(c), (15)(3), (15)(4), (20)(1), (20)(2), (20)(3), (20)(4)
7.3.9	(15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (12)(3), (12)(4), (12)(5), (12)(6)
7.3.10	(13)(2)(f), (14)(2)(g), (15)(1)(h), (22)(1), (22)(3)
7.4.1	(5)(1)(b), (5)(1)(c)
7.4.2	(25)(2)
7.4.3	(5)(1)(d)
7.4.4	(5)(1)(c)
7.4.5	(5)(1)(c), (5)(1)(e), (6)(4)(e), (11)(1), (32)(1)(a)
7.4.6	(5)(1)(c)
7.4.7	(13)(2)(a), (14)(2)(a)
7.4.8	(5)(1)(f)
7.5.1	(15)(2), (44), (45)(1), (45)(2)(a), (45)(2)(b), (45)(2)(c), (45)(3), (45)(4), (45)(5), (45)(6), (45)(7), (45)(8), (45)(9), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (46)(4), (46)(5), (47)(1)(a), (47)(1)(b), (47)(1)(c), (47)(2)(a), (47)(2)(b), (47)(2)(c), (47)(2)(d), (47)(2)(e), (47)(2)(f), (47)(2)(g), (47)(2)(h), (47)(2)(i), (47)(2)(j), (47)(2)(k), (47)(2)(l), (47)(2)(m), (47)(2)(n), (47)(3), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6), (30)(1)(e), (48)
7.5.2	(15)(2), (30)(1)(e)
7.5.3	(30)(1)(e)
7.5.4	(30)(1)(d)
7.5.5	(5)(1)(f)
8.2.1	(28)(3)(f), (28)(3)(e), (28)(9), (35)(1)
8.2.2	(5)(1)(a), (5)(1)(b), (28)(3)(a), (29), (32)(4)
8.2.3	(7)(4)
8.2.4	(28)(3)(h)
8.2.5	(28)(3)(h)
8.2.6	(30)(3), (30)(4), (30)(5), (30)(2)(a), (30)(2)(b)
8.3.1	(15)(3), (17)(2), (28)(3)(e)
8.4.1	(5)(1)(c)
8.4.2	(28)(3)(g), (30)(1)(f)
8.4.3	(5)(1)(f)
8.5.1	(44), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (48), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6)
8.5.2	(30)(2)(c)
8.5.3	(30)(1)(d)

8.5.4	(28)(3)(a)
8.5.5	(48)
8.5.6	(28)(2), (28)(4)
8.5.7	(28)(2), (28)(3)(d)
8.5.8	(28)(2)

1928

1929

1930

1931

1932

Annex D
(informative)

Mapping to ISO/IEC 29100

This table gives an indicative mapping between provisions of this document and the principles from ISO/IEC 21900. It shows in a purely indicative manner how compliance to requirements and controls of this document relates to the general privacy principles specified in 29100.

D.1 Mapping for PII controllers

Privacy Principles of ISO/IEC 29100	***Related Controls for PII controllers***
1. Consent and Choice	A.7.2.1 Identify and document purpose A.7.2.2 Identify lawful basis A.7.2.3 Determine when and how consent is to be obtained A.7.2.4 Obtain and record consent A.7.2.5 Privacy impact assessment A.7.3.2 Determining information for PII principals A.7.3.3 Providing information to PII principals A.7.3.4 Provide mechanism to modify or withdraw consent A.7.3.5 Provide mechanism to object to processing A.7.3.7 PII controllers' obligations and third parties
2. Purpose of legitimacy and specification	A.7.2.1 Identify and document purpose A.7.2.2 Identify lawful basis A.7.2.5 Privacy impact assessment A.7.3.2 Determining information for PII principals A.7.3.3 Providing information to PII principals
3. Collection limitation	A.7.2.5 Privacy impact assessment A.7.4.1 Limit collection
4. Data minimization	A.7.4.2 Limit processing A.7.4.4 PII minimization and de-identification objectives A.7.4.5 PII de-identification and deletion at the end of processing
5. Use, retention and disclosure limitation	A.7.4.4 PII minimization and de-identification objectives A.7.4.5 PII de-identification and deletion at the end of processing A.7.4.6 Temporary files A.7.4.7 Retention A.7.4.8 Disposal A.7.5.4 Records of PII disclosure to third parties
6. Accuracy and quality	A.7.4.3 Accuracy and quality
7. Openness, transparency and notice	A.7.3.2 Determining information for PII principals A.7.3.3 Providing information to PII principals

	A.7.3.8 Providing copy of PII processed
8. Individual participation and access	A.7.3.1 Determining and fulfilling obligations to PII principals A.7.3.3 Providing copy of PII processed A.7.3.6 Access, correction and/or erasure A.7.3.9 Handling requests A.7.3.10 Automated decision making
9. Accountability	A.7.2.6 Contracts with PII processors A.7.2.7 Joint controller A.7.2.8 Records related to processing PII A.7.3.9 Handling requests A.7.5.1 Identify basis for international PII transfer A.7.5.2 Countries and organizations to which PII might be transferred A.7.5.3 Records and transfer of PII
10. Information Security	A.7.2.6 Contracts with PII processors A.7.4.9 PII transmission controls
11. Privacy compliance	A.7.2.5 Privacy impact assessment

D.2 Mapping for PII processors

Privacy Principles of ISO/IEC 29100	***Related Controls for PII processors***
1. Consent and Choice	B.8.2.5 PII controller obligations
2. Purpose of legitimacy and specification	B.8.2.1 Cooperation agreement B.8.2.2 Organization's purposes B.8.2.3 Marketing and advertising use B.8.2.4 Infringing instruction B.8.3.1 Obligations to PII principals
3. Collection limitation	N/A
4. Data minimization	B.8.4.1 Temporary files
5. Use, retention and disclosure limitation	B.8.5.3 Records of PII disclosure to third parties B.8.5.4 Notification of PII disclosure requests B.8.5.5 Legally binding PII disclosures
6. Accuracy and quality	N/A
7. Openness, transparency and notice	B.8.5.6 Disclosure of subcontractors used to process PII B.8.5.7 Engagement of a subcontractor to process PII B.8.5.8 Change of subcontractor to process PII
8. Individual participation and access	N/A
9. Accountability	B.8.2.6 Records related to processing PII B.8.4.2 Return, transfer or disposal of PII B.8.5.1 Identify basis for international PII transfer B.8.5.2 Countries and organizations to which PII might be transferred

10. Information Security	B.8.4.3 PII transmission controls
11. Privacy compliance	B.8.2.5 PII controller obligations

1945

Annex E
(informative)

Mapping to ISO/IEC 27018 and ISO/IEC 29151

This table gives an indicative mapping between provisions of this document and provisions from ISO/IEC 27018 and ISO/IEC 29151. It shows how requirements and controls of this document can have some correspondence with provisions from ISO/IEC 27018 and/or ISO/IEC 29151.

It is purely indicative and it should not be assumed that a given link between provisions means equivalence.

ISO/IEC 27552 sub-clause	ISO/IEC 27018 sub-clause	ISO/IEC 29151 sub-clause
5.2	N/A	N/A
5.3	N/A	N/A
5.4	N/A	A.7.12
5.5	7.2.2	7.2.3, A.7.11.5
5.6	N/A	N/A
5.7	N/A	N/A
5.8	N/A	N/A
6.1	N/A	N/A
6.2	6.1.1	A.7.11.1
6.3	N/A	N/A
6.4	N/A	N/A
6.5.1	N/A	8.2.1
6.5.2	A.7.10.5	8.2.6
6.5.3	A.7.10.4	8.3.4
6.6.1	9.2	N/A
6.6.2	9.2.1, A.7.10.10	9.2.2
6.6.3	A.7.10.9	9.2.3
6.6.4	A.7.10.8	9.2.4
6.7	10.1.1	N/A
6.8.1	11.2.7, A.7.10.13	11.2.8
6.8.2	A.7.10.2	N/A
6.9.1	N/A	12.1.5
6.9.2	12.3.1, A.7.10.3	12.3.2
6.9.3	12.4.1	12.4.2

6.9.4	12.4.2	12.4.3
6.9.5	N/A	N/A
6.9.6	N/A	N/A
6.9.7	N/A	N/A
6.10.1	13.2.1	13.2.2
6.10.2	A.7.10.11	13.2.5
6.11.1	A.7.10.6	N/A
6.11.2	N/A	N/A
6.11.3	N/A	N/A
6.12	N/A	N/A
6.13.1	16.1	N/A
6.14	N/A	N/A
6.15.1	A.7.9.2	N/A
6.15.2	18.2.1	18.2.2, A.7.11.4
6.15.3	N/A	N/A
7.2.1	N/A	A.7.4.2
7.2.2	N/A	A.7.4.1
7.2.3	N/A	N/A
7.2.4	N/A	A.7.3.1
7.2.5	N/A	A.7.11.2
7.2.6	N/A	A.7.11.3
7.2.7	N/A	A.7.7.4
7.2.8	N/A	N/A
7.3.1	N/A	A.7.10.1
7.3.2	N/A	N/A
7.3.3	N/A	A.7.4.2, A.7.9.1, A.7.9.2
7.3.4	N/A	N/A
7.3.5	N/A	N/A
7.3.6	N/A	A.7.10.2
7.3.7	N/A	N/A
7.3.8	N/A	N/A
7.3.9	N/A	N/A
7.3.10	N/A	A.7.10.3
7.4.1	N/A	A.7.5, A.7.6

7.4.2	N/A	N/A
7.4.3	N/A	A.7.8
7.4.4	N/A	N/A
7.4.5	N/A	A.7.7.2
7.4.6	N/A	A.7.6
7.4.7	N/A	A.7.7.1
7.4.8	N/A	N/A
7.4.9	N/A	N/A
7.5.1	N/A	A.7.13.2
7.5.2	N/A	A.7.13.2
7.5.3	N/A	A.7.13.2
7.5.4	N/A	A.7.7.3
8.2.1	N/A	N/A
8.2.2	A.7.2.1	N/A
8.2.3	A.7.2.2	N/A
8.2.4	N/A	N/A
8.2.5	N/A	N/A
8.2.6	N/A	N/A
8.3.1	A.7.1.1	N/A
8.4.1	A.7.4.1	N/A
8.4.2	A.7.9.3	N/A
8.4.3	A.7.11.2	N/A
8.5.1	N/A	N/A
8.5.2	A.7.11.1	N/A
8.5.3	A.7.5.1	N/A
8.5.4	N/A	N/A
8.5.5	A.7.5.2	N/A
8.5.6	A.7.7.1	A.7.7.5
8.5.7	N/A	N/A
8.5.8	N/A	N/A

1954

1955

Annex F
(informative)

Terms and alternative terms

There are laws and regulations in many jurisdictions dealing with the protection of PII. In some cases, these laws and regulations use similar terms, in others, different terms are used having identical or similar meanings. Table 1 gives a list of terms used in this document and indicates terms of an identical or similar meaning used in other jurisdictions.

Table F.1 — Terms and alternative terms

Term as used in this document	Alternate term
Privacy Information Management System (PIMS)	Personal Information Management System (PIMS)
PII principal	Data subject
PII	Personal data
Privacy by design	Data protection by design
Privacy by default	Data protection by default
PII controller	Controller
PII processor	Processor

Annex G
(informative)

How to apply ISO/IEC 27552 to ISO/IEC 27001 and ISO/IEC 27002

G.1 How to apply this standard

This standard is based on ISO/IEC 27001:2013 and ISO/IEC 27002:2013 and extends their requirements and guidance to take into account, in addition to information security, the protection of privacy of PII principals as potentially affected by the processing of PII. That means, where the term "information security" is used in ISO/IEC 27001 or ISO/IEC 27002 "information security and privacy" applies instead.

Table G.1 gives the mapping of the extension of the term information security in order to apply it to this document.

Table L.1 — Mapping of the extension of the term information security by privacy

ISO/IEC 27001	ISO/IEC 27552 (extension)
information security	information security and privacy
information security policy	information security and privacy policy
information security management	information security and privacy information management
information security management system (ISMS)	privacy information management system (PIMS)
information security objectives	information security and privacy objectives
Information security performance	information security and privacy performance
Information security requirements	information security and privacy requirements
information security risk	information security and privacy risk
information security risk assessment	information security and privacy risk assessment
information security risk treatment	information security and privacy risk treatment

Basically, there are three cases for applying this document to protection of privacy of PII principals when processing PII ("privacy"):

1. Application of security standards as is:
   The referring standards apply as it is with the extension of terms as listed above. Therefore, the referring standard is not repeated, but only referred to in respective clauses.

2. Additions to security standards:
The referring standards apply with additional privacy-specific requirements or implementation guidance.

3. Refinement of security standards:
The referring standards are refined by privacy-specific requirements or implementation guidance.

G.2 Example of refinement of security standards

This section describes how the section 5.4.1.2 of this standard is applied to section 6.1.2 of ISO/IEC 27001.

This is the respective section of this document:

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 and privacy risk assessment process(s) to identify risks associated with the loss of confidentiality, integrity and availability, within the scope of PIMS.

The organization shall apply the privacy risk assessment process(s) 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) 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 6.1.2.c) of ISO/IEC 27001:2013, as refined above, were to materialize.

This is referring to the following section from ISO/IEC 27001:2013:

6.1.2 Information security risk assessment

The organization shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria that include:

   1) the risk acceptance criteria; and

   2) criteria for performing information security risk assessments;

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

c) identifies the information security risks:

1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and

2) identify the risk owners;

d) analyses the information security risks:

1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;

2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and

3) determine the levels of risk;

e) evaluates the information security risks:

1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and

2) prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the information security risk assessment process.

This section of ISO/IEC 27001:2013, when taking into account the protection of privacy of PII principals when processing PII would be amended as following:

The organization shall define and apply an information security and privacy risk assessment process that:

a) establishes and maintains information security and privacy risk criteria that include:

1) the risk acceptance criteria; and

2) criteria for performing information security and privacy risk assessments;

b) ensures that repeated information security and privacy risk assessments produce consistent, valid and comparable results;

c) identifies the information security and privacy risks:

1) apply the information security and privacy risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security and privacy information management system; and

2) identify the risk owners;

d) analyses the information security and privacy risks;

1) assess the potential consequences that would result if the risks identified in 6.1.2.c) were to materialize;

2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and

3) determine the levels of risk;

e) evaluates the information security and privacy risks:

1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and

2) prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the information security and privacy risk assessment process.

End of the example

Bibliography

[1] ISO/IEC 19944:2017 *Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use*

[2] ISO/IEC DIS 20899 *Information technology -- Security techniques – Privacy enhancing data de-identification techniques*

[3] ISO/IEC 27005:2011, *Information technology -- Security techniques -- Information security risk management*

[4] ISO/IEC 27018:2014, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[5] ISO/IEC 27035-1:2016, *Information technology — Security techniques — Information security incident management – Part 1: Principles of incident management*

[6] ISO/IEC 29101:2013, *Information technology — Security techniques — Privacy architecture framework*

[7] ISO/IEC 29134:2017, *Information technology — Security techniques — Guidelines for privacy impact assessment*

[8] ISO/IEC 29151:2017, *Information technology — Security techniques — Code of practice for Personally Identifiable Information protection*

[9] ISO/IEC 29184:9999 *Information technology — Security techniques — Guidelines for online privacy notices and consent*

[EDITOR'S NOTE: Check status before FDIS, plus link to 7.2]

Form 8A: Committee decision for DIS

Secretariat: DIN	**ISO/IEC JTC 1/SC 27** **N 19115**
Project number and title: ISO/IEC CD 27552 - Information technology -- Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines	

This form should be sent to the ISO Central Secretariat (http://isotc.iso.org/livelink/si/), together with the draft of the project, by the secretariat of the technical committee or subcommittee concerned.

The accompanying document is submitted for circulation to member body vote:

☒ As a DIS

Consensus has been obtained from the P-members of the committee:

on 2018-10-04

☒ At the meeting of ISO/IEC JTC 1/SC 27. See Resolution number 5. In document N 19100.

☐ By ballot initiated on

Please attach a copy of the ballot results (if applicable)

Listing of the P-members (NWIP, CD or Resolution)

P-members in favour: 30

Australia (SA), Brazil (ABNT), Canada (SCC), China (SAC), Costa Rica (INTECO), Denmark (DS), Finland (SFS), France (AFNOR), Germany (DIN), India (BIS), Iran, Islamic Republic of (ISIRI), Ireland (NSAI), Israel (SII), Kenya (KEBS), Korea, Republic of (KATS), Lebanon (LIBNOR), Mauritius (MSB), Mexico (DGN), Netherlands (NEN), New Zealand (NZSO), Panama (COPANIT), Peru (INACAL), Philippines (BPS), Saint Kitts and Nevis (SKNBS), Slovakia (UNMS SR), South Africa (SABS), Sweden (SIS), Switzerland (SNV), Ukraine (DSTU), United Kingdom (BSI)

P-members voting against: 4 Japan (JISC), Luxembourg (ILNAS), Malaysia (DSM), United States (ANSI)
P-members abstaining: 16 Algeria (IANOR), Argentina (IRAM), Austria (ASI), Belgium (NBN), Côte d'Ivoire (CODINORM), Indonesia (BSN), Italy (UNI), Kazakhstan (KAZMEMST), Poland (PKN), Portugal (IPQ), Romania (ASRO), Russian Federation (GOST R), Singapore (ESG), Spain (UNE), United Arab Emirates (ESMA), Uruguay (UNIT)
P-members who did not vote: 1 Chile (INN)
Remarks: The text for the 2nd CD of ISO/IEC 27552 was circulated as SC 27 N18410. The summary of voting on SC 27 N18410 was presented as SC 27 N18822 for consideration at the Comment Resolution Meeting held during the SC 27/WG week in held in Gjøvik, Norway, during the SC 27/WG week on 2018-09-30/10-04. The dispostions of comments received on SC 27 N18410 (text for 2nd CD) are shown in SC 27 N19114. As per Gjøvik Resolution 5 of the Comment Resolution Meeting (contained in SC 27 N19100) the text for a 1st DIS of ISO/IEC 27552 as presented in SC 27 N19115 was submitted to the ISO Central Secretariat(ITTF) for the 12-week DIS ballot processing on 2018-10-15. The negative National Body votes of United States has been satisfactorily resolved and changed to approval.

I hereby confirm that this draft meets the requirements of Part 2 of the ISO/IEC Directives:		
Secretariat: DIN	**Date:** 2018-10-15	**Name/Signature of TC/SC Secretary:** Passia, Krystyna Mrs

Result of voting

Ballot Information	
Ballot reference	ISO/IEC CD 27552.2 - ISO-IECJTC1-SC27_N18410
Ballot type	CD
Ballot title	Information technology -- Security techniques -- Enhancement to ISO/IEC 27001 for privacy management -- Requirements
Opening date	2018-06-05
Closing date	2018-08-28
Note	2nd CD Registration and Consideration In accordance with resolution 2 (see SC 27 N18431 = WG 5 N1331) of the Comment Resolution Meeting (CRM) held in Wuhan, Hubei Province, China (April 2018) the hereby attached document is circulated for a 12 weeks 2nd CD letter ballot closing by .2018-08-28

Member responses:	
Votes cast (50)	Algeria (IANOR) Argentina (IRAM) Australia (SA) Austria (ASI) Belgium (NBN) Brazil (ABNT) Canada (SCC) China (SAC) Costa Rica (INTECO) Côte d'Ivoire (CODINORM) Denmark (DS) Finland (SFS) France (AFNOR) Germany (DIN) India (BIS) Indonesia (BSN) Iran, Islamic Republic of (ISIRI) Ireland (NSAI) Israel (SII) Italy (UNI) Japan (JISC) Kazakhstan (KAZMEMST) Kenya (KEBS) Korea, Republic of (KATS) Lebanon (LIBNOR) Luxembourg (ILNAS) Malaysia (DSM)

	Mauritius (MSB) Mexico (DGN) Netherlands (NEN) New Zealand (NZSO) Panama (COPANIT) Peru (INACAL) Philippines (BPS) Poland (PKN) Portugal (IPQ) Romania (ASRO) Russian Federation (GOST R) Saint Kitts and Nevis (SKNBS) Singapore (ESG) Slovakia (UNMS SR) South Africa (SABS) Spain (UNE) Sweden (SIS) Switzerland (SNV) Ukraine (DSTU) United Arab Emirates (ESMA) United Kingdom (BSI) United States (ANSI) Uruguay (UNIT)
Comments submitted (1)	SBS - Small Business Standards
Votes not cast (1)	Chile (INN)

Questions:	
Q.1	"Do you approve the circulation of the draft as a DIS?"

Votes by members	Q.1
Algeria (IANOR)	Abstention
Argentina (IRAM)	Abstention
Australia (SA)	Approval
Austria (ASI)	Abstention
Belgium (NBN)	Abstention
Brazil (ABNT)	Approval
Canada (SCC)	Approval with comments
China (SAC)	Approval
Costa Rica (INTECO)	Approval
Côte d'Ivoire (CODINORM)	Abstention
Denmark (DS)	Approval
Finland (SFS)	Approval
France (AFNOR)	Approval with comments

Germany (DIN)	Approval with comments
India (BIS)	Approval
Indonesia (BSN)	Abstention
Iran, Islamic Republic of (ISIRI)	Approval
Ireland (NSAI)	Approval
Israel (SII)	Approval
Italy (UNI)	Abstention
Japan (JISC)	Disapproval
Kazakhstan (KAZMEMST)	Abstention
Kenya (KEBS)	Approval
Korea, Republic of (KATS)	Approval with comments
Lebanon (LIBNOR)	Approval
Luxembourg (ILNAS)	Disapproval
Malaysia (DSM)	Disapproval
Mauritius (MSB)	Approval
Mexico (DGN)	Approval
Netherlands (NEN)	Approval
New Zealand (NZSO)	Approval
Panama (COPANIT)	Approval
Peru (INACAL)	Approval
Philippines (BPS)	Approval
Poland (PKN)	Abstention
Portugal (IPQ)	Abstention
Romania (ASRO)	Abstention
Russian Federation (GOST R)	Abstention
Saint Kitts and Nevis (SKNBS)	Approval
Singapore (ESG)	Abstention
Slovakia (UNMS SR)	Approval
South Africa (SABS)	Approval
Spain (UNE)	Abstention
Sweden (SIS)	Approval with comments

Switzerland (SNV)	Approval
Ukraine (DSTU)	Approval
United Arab Emirates (ESMA)	Abstention
United Kingdom (BSI)	Approval with comments
United States (ANSI)	Disapproval
Uruguay (UNIT)	Abstention

Answers to Q.1: "Do you approve the circulation of the draft as a DIS?"		
24 x	**Approval**	**Australia (SA)** **Brazil (ABNT)** **China (SAC)** **Costa Rica (INTECO)** **Denmark (DS)** **Finland (SFS)** **India (BIS)** **Iran, Islamic Republic of (ISIRI)** **Ireland (NSAI)** **Israel (SII)** **Kenya (KEBS)** **Lebanon (LIBNOR)** **Mauritius (MSB)** **Mexico (DGN)** **Netherlands (NEN)** **New Zealand (NZSO)** **Panama (COPANIT)** **Peru (INACAL)** **Philippines (BPS)** **Saint Kitts and Nevis (SKNBS)** **Slovakia (UNMS SR)** **South Africa (SABS)** **Switzerland (SNV)** **Ukraine (DSTU)**
6 x	**Approval with comments**	**Canada (SCC)** **France (AFNOR)** **Germany (DIN)** **Korea, Republic of (KATS)** **Sweden (SIS)** **United Kingdom (BSI)**
4 x	**Disapproval**	**Japan (JISC)** **Luxembourg (ILNAS)** **Malaysia (DSM)** **United States (ANSI)**
16 x	**Abstention**	**Algeria (IANOR)** **Argentina (IRAM)** **Austria (ASI)** **Belgium (NBN)** **Côte d'Ivoire (CODINORM)** **Indonesia (BSN)**

Italy (UNI) **Kazakhstan (KAZMEMST)** **Poland (PKN)** **Portugal (IPQ)** **Romania (ASRO)** **Russian Federation (GOST R)** **Singapore (ESG)** **Spain (UNE)** **United Arab Emirates (ESMA)** **Uruguay (UNIT)**

Comments from Voters		
Member:	Comment:	Date:
Canada (SCC)	***Comment File***	2018-08-28 21:09:13
France (AFNOR)	***Comment File***	2018-08-21 11:00:43
Germany (DIN)	***Comment File***	2018-08-16 15:47:50
Italy (UNI)	***Comment File***	2018-08-11 17:18:36
Japan (JISC)	***Comment File***	2018-08-24 02:36:36
Korea, Republic of (KATS)	***Comment File***	2018-08-27 03:55:46
Luxembourg (ILNAS)	***Comment File***	2018-08-28 09:41:38
Malaysia (DSM)	***Comment File***	2018-08-21 11:29:11
Sweden (SIS)	***Comment File***	2018-08-27 23:19:24
United Kingdom (BSI)	***Comment File***	2018-08-23 12:31:13
United States (ANSI)	***Comment File***	2018-08-22 17:51:17

Comments from Commenters		
Member:	Comment:	Date:
SBS - Small Business Standards	***Comment File***	2018-08-10 18:16:10