COMMITTEE DRAFT ISO/IEC 1st CD 27552	Reference document: SC 27 N17875
Date: 2017-12-08	**Supersedes document WG 5 N860**

THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.

ISO/IEC JTC 1/SC 27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for comments by: **2018-03-02** Please submit your comments via the online balloting application by the due date indicated.

ISO/IEC 1st CD 27552

Title: Information technology -- Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management — Requirements and guidelines *

**Subject to JTC 1 endorsement of the title change.*

Project: 1.27.125 (ISO/IEC 27552)

Explanatory Report

Status	SC 27 Decision	Reference documents	
		Input	**Output**
NWIP	21st WG 5 meeting, April 2016, Recommendations 8 10, (N16241 = WG 5 N341); 28th SC 27 Plenary, April 2016, Resolution 8 (N16370).	FR ExpContr. (WG 5 N261, N322); IN ExpContr. (WG 5 N33 JP ExpContr. (WG 5 N33 KR ExpContr.(WG 5 N32 (WG 1 N447).	Justifcation study (N16435); NWIP (N16450 = JTC 1 N13069).
ISO/IEC NP 27552 1st WD	22nd WG 5 meeting, Oct. 2016, Recommendations 2, 3, 11, 4410, (N16800 = WG 5 N600).	SoV (N16630)	DoC (N16913 = WG 5 N613); Text f. 1st WD (WG5 N614).
ISO/IEC 27552 2nd WD	23rd WG 5 meeting, April 2017, Recommendations 2, 3 (N17400 = WG 5 N800).	Results of call for com. (WG 5 N704); Art29 WP com. (WG 5 N706); WITDOM com. (WG 5 N732, N733); Dra DoCom. (WG 5 N753); Draft rev text (WG 5 N75	Liaisons to: SC 7 (WG 5 N559 = N16759); DoC (WG 5 N859); Text f. 2nd WD (WG 5 N860).
ISO/IEC 27552 1st CD	24th WG 5 meeting, Oct 30 – Nov 3rd, 2017, Recom-mendations 2, 7, 15 (N17820 = WG 5 N1020).	SoCom 2nd WD (WG 5 N932); Art29 DP WP com (WG 5 N965); WITDOM com (WG 5 N9 N990); Draft DoC (WG 5 Draft revised text (WG 5 N991).	Justification f. title and scope change (N17885 = WG 5 N1085); Liaisons to: Art29 WP com. (WG 5 N1037); WITDOM (WG 5 N1055); DoC (N17874 = WG 5 N1074); Text f. 1st CD (N17875).

1st CD Registration and Consideration

In accordance with resolution 15 (see SC 27 N17820) of the 24th SC 27/WG 5 meeting held in Berlin, Germany, 30th October – 3rd November 2017 the hereby attached document has been registered with the ISO Central Secretariat as 1st Committee Draft (CD) and is being circulated for a 1st CD letter ballot closing by **2018-03-02**

MEDIUM: http://isotc.iso.org/livelink/livelink/open/jtc1sc27

NO. OF PAGES: 2 + 56

Secretariat, ISO/IEC JTC 1/SC27 -
DIN Deutsches Institut fuer Normung e.V., Am DIN-Platz, Burggrafenstr. 6, D-10787 [D-10772 postal] Berlin , Germany
Telephone: + 49 2601-2652; Facsimile: + 49 2601-4-2652; E-mail: krystyna.passia@din.de,
http://www.din.de/go/jtc1sc27

ISO/IEC JTC1/SC 27 N 17875

ISO/IEC JTC1/SC 27/WG 5 N 1075

Date: 2017-12-07

ISO/IEC CD 27552

ISO/IEC TC JTC1/SC 27/WG 5

Secretariat: DIN

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

Techniques de sécurité — Extension d'ISO/IEC 27001 à la gestion de la protection de la vie privée — Exigences

* Subject to JTC 1 endorsement of the title change.

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (20) Preparatory
Document language: E

C:\altes NB\Documents\Project_admin\27552_NP_Enhanc_27001_priv_mgmt\03_01_1st_CD_27552_20171208\N17875_Text_1st_CD_27552_20171208\ISO-IEC_27552_(E) WD2 V4.4.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*.

0 Introduction

0.1 General

Almost every organization processes Personally Identifiable Information (PII). Further, the quantity of PII processed is increasing, as is the number of situations where organizations need to cooperate with other organizations regarding PII processing. Protection of privacy in the context of PII processing 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.

This document defines these additional requirements and guidance for the protection of PII, enabling an organizations' 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 (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 Regulations, however these may need to be interpreted to take into account local laws and regulations.

This document can be used by PII controllers (including those who are joint PII controllers) and PII processors (including those using subcontracted PII processors).

An organization complying with this document will generate documentary evidence of how it handles the processing of PII. Such evidence may 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 standard 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 high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

Security techniques — Enhancement to ISO/IEC 27001 for privacy management — Requirements (*)

1 Scope

This document specifies the 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.

* EDITOR'S NOTE: The updated title and scope are under ballot in parallel to the CD ballot on 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 27000:2014, *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 apply.

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

4 Structure of this document

[EDITORS NOTE: NATIONAL BODIES, PLEASE NOTE THE FOLLOWING AND COMENT AS APPROPRIATE:

Referencing ISO/IEC 27001:2013 and ISO/IEC 27002:2013

During Berlin meeting, our co-editor from WG1 identified two ways to reference ISO/IEC 27001 and ISO/IEC 27002:

a) systematic references of all clauses;

b) references only to the ones which have additional guidance.

In the current draft, b) is the option used. If member bodies would prefer option a), please comment appropriately.

Whilst reducing the page count, it may reduce readability for practitioners.]

4.1 Overview

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

PIMS-specific requirements are given in this document. Compliance with this document is based on adherence to these requirements.

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

PIMS-specific guidance and other information regarding the information security controls in ISO/IEC 27002 and PIMS-specific controls, appropriate to an organization acting as either a PII controller or a PII processor, are given in clause 6.

Additional guidance for PII controllers is given in clause 7, and additional guidance for PII processors is given in clause 8.

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

The following tables give the location of sector-specific guidance in this document in relation to ISO/IEC 27001 and ISO/IEC 27002.

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

Clause number in ISO/IEC 27001:2013	Title	Clause number in this document	Remarks
4	Context of the organization	5.2	Additional requirements
5	Leadership	N/A	No PIMS-specific provision
6	Planning	5.3	Additional requirements
7	Support	N/A	No PIMS-specific provision
8	Operation	N/A	No PIMS-specific provision
9	Performance Evaluation	N/A	No PIMS-specific provision
10	Improvement	N/A	No PIMS-specific provision

Table 2 — Location of sector-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

4.2 Customer

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

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

NOTE such an organization may be a joint controller (see 7.5.5)

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

- a PII processor who has a contract with a PII sub-processor (e.g., the customer of the PII sub-processor).

5 PIMS-specific requirements related to ISO/IEC 27001

5.1 General

All requirements from ISO/IEC 27001:2013, clauses 4 to 10 that do not appear below apply unchanged.

ISO/IEC 27001:2013 requirements in clauses 4 to 10 are interpreted as follows:

a) The term "information security" used in ISO/IEC 27001:2013 shall be extended in this document to include the protection of privacy as potentially affected by PII processing, even where an enhancement or extension of requirements is not specifically indicated.

b) The above provision shall encompass terms compounding “information security” with other terms, such as “information security policy”, “information security objectives”, “information security requirements”, “information security risk assessment”, “information security risk treatment” and “information security management”.

5.2 Context of the organization

5.2.1 Understanding the organization and its context

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

a) The organization shall determine its role as either a PII controller or a PII processor;

NOTE 1 Organizations need to determine external and internal issues that are relevant to its context and that affects its ability to achieve the intended outcome(s) of its PII management, e.g.

- Applicable privacy legislation;
- Applicable regulations;
- Judicial decisions;
- Administrative decisions;
- Collective agreements;
- Contractual requirements.

NOTE 2 Where an organization acts as both a PII controller and a PII processor, separate roles need to be determined; each of which would be the subject of a separate set of controls.

NOTE 3 The role of the organization may be different for each instance of PII processing, 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, clause 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 PII processing.

NOTE 1 Such parties may include PII principals, customers, supervisory authorities, other PII controllers, contracted PII processors and their sub-contractors.

NOTE 2 Requirements relevant to the processing of PII may 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 obligations, some interested parties (e.g. customers, regulatory authorities) may 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 may 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, clause 4.3 is:

a) When determining the scope of the information security management system, the organization shall consider the explicit inclusion of the processing of PII.

NOTE The processing of PII includes all aspects of PII management, including collection and processing, facilitating the rights of PII principals, implementing controls for privacy by design and by default, PII sharing, transfer and disclosure.

5.2.4 Information security management system

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

a) The organization shall establish, implement, maintain and continually improve a PII Management System (PIMS) in accordance with the requirements of ISO/IEC 27001 clauses 4 to 10, augmented by the requirements in clause 5 of this document.

5.3 Planning

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

The organization shall apply the information security and privacy risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability, and with risks related to PII processing for information within the scope of the information security management system.

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

The organization shall assess the potential consequences, including those on the PII principals' privacy, that would result if the risks identified in 6.1.2.c) were to materialize.

A requirement additional to ISO/IEC 27001:2013, clause 6.1.3.c) is:

a) Compare the controls determined in 6.1.3 b) of ISO/IEC 27001:2013 with those in ISO/IEC 27001:2013, Annex A and with Annex A and B of this document to verify that no necessary controls have been omitted.

NOTE: 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 should be considered in the context of both risks to information security as well as risks to privacy related to PII processing.

A requirement additional to ISO/IEC 27001:2013, clause 6.1.3.d) is:

a) 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 or Annex A and B of this document according to the organization's determination of its role (see 5.2.1).

6 PIMS-specific guidance related to ISO/IEC 27002

6.1 General

All clauses, control objectives, controls, implementation guidance and other information from ISO/IEC 27002:2013 that do not appear below apply unchanged.

NOTE Unless otherwise stated in this clause, the same guidance applies for PII controllers and PII processors unless otherwise stated, or where otherwise identified contractually or by certain jurisdictions.

6.2 Information security policies

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

The information security policies should be augmented by 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 customers.

Contractual agreements should clearly allocate responsibilities between the organization, its partners, its subcontractors and its relevant third parties (customers, suppliers, etc.) taking into account the type of service. For example, in a cloud-based deployment, the allocation of responsibility for application layer controls may differ depending on whether the public cloud service provider acting as a PII processor is providing a SaaS service or a PaaS or IaaS service upon which the cloud service customer can build or layer its own applications.

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 PI processor, is subject to the relevant PII protection legislation.

The contract between the organization and its customers shall provide a mechanism for ensuring the organization supports and manages compliance with all applicable legislation, regulation and so on. The contract could call for independently audited compliance, acceptable to the customer (e.g., via the implementation of the relevant controls in this International Standard and in ISO/IEC 27002).

6.3 Organization of information security

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 under the contract.

The organization should appoint a person(s) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding PII processing.

NOTE Some jurisdictions may define circumstances where a data protection officer should be appointed, along with their position and role.

6.4 Human resource security

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 to make relevant staff aware of the possible consequences on the organization (e.g., legal consequences, loss of business and brand or reputational damage), on the staff member (e.g., disciplinary consequences) and on 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 including awareness of incident response routines.

NOTE Organizations need to carry out appropriate periodic training for personnel having permanent or regular access to PII.

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

In some jurisdictions, the organization may be subject to legal sanctions, including substantial fines directly from the local supervisory authority. In some jurisdictions, the use of International Standards such as this document in setting up the contract between the organization and the customer may help establish a basis for contractual sanctions for a breach of security rules and procedures.

6.5 Asset management

6.5.1 Classification of information

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, where such PII is stored and the systems through which it may flow,

6.5.2 Management of removable media

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

The organization should not use portable physical media and portable devices that do not permit encryption, except where it is unavoidable, and document any use of such portable media and devices.

Portable media which are taken outside the physical controls of an organization are prone to loss, damage and inappropriate access. Encrypting portable media adds a level of protection which reduces security risks should the portable media be compromised.

The use of portable physical media and devices that do not support encryption should be avoided, except where it is unavoidable. In those instances, organizations should implement compensating controls (e.g., tamper-evident packaging) to mitigate risks to the PII.

Where removable media is disposed of, secure procedures should be documented and implemented.

6.5.3 Physical media transfer

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

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

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

6.6 Access control

6.6.1 User access management

Additional implementation guidance for 9.2, User access management, of ISO/IEC 27002:2013 is:

In the context of the service categories of the cloud computing reference architecture[1], the customer may be responsible for some or all aspects of access management under the customers control. Where appropriate, the organization should enable the customer to manage access by the customers under their control, such as by providing administrative rights to manage or terminate access.

6.6.2 User registration and de-registration

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

Procedures for user registration and de-registration should address the situation where user access control is compromised, such as the corruption or compromise of passwords or other user registration data (e.g., as a result of inadvertent disclosure).

The organization should not grant de-activated or expired user IDs to other users.

In the context of distributed (e.g. cloud computing) reference architectures, the customer may be responsible for some or all aspects of user ID management for the customers under their control.

NOTE Individual jurisdictions may impose specific requirements regarding the frequency of checks for unused authentication credentials. Organizations operating in these jurisdictions should ensure that they comply with these requirements.

6.6.3 User access provisioning

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

The organization should maintain an up-to-date record of the users or profiles of users who have authorized access to the information system and the PII contained therein.

A user profile should be maintained for all users whose access is authorized by the organization. The profile of a user comprises the set of data about that user, including user ID, necessary to implement the technical controls providing authorized access to the information system and the PII contained therein.

6.6.4 Management of privileged access

Additional implementation guidance for 9.3.2, Management of privileged access, of ISO/IEC 27002:2013 is:

[1] For details of a cloud reference architecture, see ISO/IEC 17789:2014 Information technology – cloud computing – reference architecture

The organization should ensure that, where more than one user has access to stored PII, each has a distinct user ID for identification, authentication and authorization purposes.

Implementing individual user access ID's 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.

6.6.5 Secure log-on procedures

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

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

6.7 Cryptography

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

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 may assist them in applying its own cryptographic protection.

NOTE In some jurisdictions it may be required to apply cryptography to protect particular kinds of PII, such as health data concerning a PII principal, resident registration numbers, passport numbers and driver's licence numbers.

6.8 Physical and environmental security

6.8.1 Secure disposal or re-use of equipment

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 assigned to a customer, any PII previously residing on that storage space is not visible to that customer.

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

No specific guidance is especially appropriate for dealing with all cases in implementing this control. However, as an example, some cloud infrastructure, platforms or applications will return zeroes if the customer attempts to read storage space which has not been overwritten by their own data.

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

6.8.2 Clear desk and clear screen policy

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 legitimate processing purpose.

6.9 Operations security

6.9.1 Separation of development, testing and operational environments

Additional implementation guidance for 12.1.4, Separation of development, testing and operational environments, of ISO/IEC 27002:2013 is:

PII should not be used for testing purposes. Where the use of PII for testing purposes cannot be avoided, a risk assessment should be undertaken. Technical and organizational measures should be implemented to minimize the risks identified.

6.9.2 Information backup

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

The organization should have a procedure for, and a log of, PII restoration efforts.

There may 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 may involve the PII principal).

NOTE 1 The above control guidance makes generic the following requirement which applies in certain legal jurisdictions. The log of PII restoration efforts should contain: the person responsible, a description of the restored PII, and the PII that were restored manually.

Information processing systems based on the cloud computing model introduce additional or alternative mechanisms to traditional non-cloud off-site backups for protecting against loss of data, ensuring continuity of data processing operations, and providing the ability to restore data processing operations after a disruptive event. Multiple copies of data in physically and/or logically diverse locations (which may be within the information processing system itself) should be created or maintained for the backup and/or recovery processes.

PII-specific responsibilities in this respect may lie with the customer. Where the organization explicitly provides backup and restore services to the customer, the organization should provide clear information to the customer about the capabilities of the cloud service with respect to backup and restoration of the customer PII.

NOTE 2 Individual jurisdictions may impose specific requirements regarding the frequency of backups. Organizations operating in these jurisdictions should ensure that they comply with these requirements.

Procedures should be put in place to allow for restoration of data processing operations within a specified, documented period after a disruptive event.

The back-up and recovery procedures should be reviewed at a specified, documented frequency.

NOTE 3 Individual jurisdictions may impose specific requirements regarding the frequency of reviews of backup and recovery procedures. Organizations operating in these jurisdictions should ensure that they comply with these requirements.

The use of subcontractors to store replicated or backup copies of data being processed is covered by the controls in this International Standard applying to sub-contracted PII processing. Where physical media transfers take place, this is also covered by controls in this document.

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

6.9.3 Event logging

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 whether or not PII has been changed (added, modified or deleted) as a result of an event and by whom. Where multiple service providers are involved in providing service from different service categories of the cloud computing reference architecture, there may be varied or shared roles in implementing this guidance. These roles should be clearly defined.

Additionally, for PII processors, the following applies:

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

Where a customer is permitted to access log records controlled by the organization, the organization should ensure that the customer can only access records that relate to that customer's activities, and cannot access any log records which relate to the activities of other customers.

6.9.4 Protection of log information

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, may 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 anonymized within a specified and documented period.

6.10 Communications security

6.10.1 Information transfer policies and procedures

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

Whenever physical media are 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.

6.10.2 Confidentiality or non-disclosure agreements

Additional implementation guidance for 13.2.3, Confidentiality or non-disclosure agreements, of ISO/IEC 27002:2013 is:

The organization should ensure that individuals under its control with access to PII are subject to a confidentiality obligation.

A confidentiality agreement, in whatever form, between the organization, its employees and its agents should ensure that employees and agents do not disclose PII for purposes independent of the instructions of the customer. The obligations of the confidentiality agreement should survive termination of any relevant contract.

6.11 Systems acquisition, development and maintenance

6.11.1 Securing application services on public networks

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 end-to-end prior to transmission.

Untrusted networks include the public internet, as well as third party data transmission facilities such as packet switched networks, “leased line services” and other facilities outside of the operational control of the organization.

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.

In the context of cloud computing reference architecture, where multiple service providers are involved in providing service from different service categories of the reference architecture, there may be varied or shared roles in implementing this guidance.

6.11.2 Secure systems engineering principles

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

Systems or components related to processing PII should be designed to anticipate and facilitate the implementation of controls related to privacy by design and by default. For example, algorithms utilized to de-identify PII should be developed securely and validated to ensure effectiveness.

Any PII processing rules developed to facilitate the protection of PII should be subject to a secure development process, including testing and review.

6.12 Supplier relationships

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

The organization should specify whether PII is being processed and the minimum technical and organizational measures which meet the organization’s information security and PII protection obligations in contracts between themselves and any subcontractor that processes them.

Implementation guidance for PII processors

The organization should specify in contracts with the customer that the PII processor is aware that they are processing PII, and the minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that PII is not processed for any purpose independent of the customer’s instructions. Such measures should not be subject to unilateral reduction by the organization.

If the PII processor sub-contracts any PII processing, the organization should specify in contracts the minimum technical and organizational measures which meet the organization’s information security and PII protection obligations.

6.13 Information security incident management

6.13.1 Management of information security incidents and improvements

Additional implementation guidance for 16.1, Management of information security incidents and improvements, of ISO/IEC 27002:2013 is:

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

An information security event may not necessarily trigger such a review. An information security 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, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks and packet sniffing.

6.13.2 Responsibilities and procedures

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 security 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).

6.13.3 Response to information security incidents

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

Implementation guidance for PII controllers

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, may be required to contain details such as:

- a contact point where more information can be obtained;
- description of and the likely consequences of the breach;
- the measures taken or proposed to be taken by the organization to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

Implementation guidance for PII processors

Provisions covering the notification of a data 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 his obligation to notify relevant authorities. This notification obligation does not extend to a data 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 data breach involving PII.

In the event that a data breach involving PII has occurred, a record should be maintained with 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) and the fact that the incident resulted in loss, disclosure or alteration of PII.

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

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

NOTE There may be other data breaches requiring notification that are not covered here, e.g., collection without consent or other authorization, use for unauthorized purposes, etc."

6.14 Information security aspects of business continuity management

No additional controls

6.15 Compliance

6.15.1 Protection of records

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

The organization should retain copies of its security and privacy policies and operating procedures for a specified, documented period of time (see 7.2.7). This includes retaining copies of previous versions of these documents when they are updated.

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

6.15.2 Independent review of information security

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

In cases where individual customer audits are impractical or may increase risks to security, the organization should make available to prospective 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, which should cover the needs of anticipated users, as selected by the organization should normally be an acceptable method for fulfilling the customer's interest in reviewing the organization's processing operations, provided sufficient transparency is available to the customer.

6.15.3 Technical compliance review

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 polices and standards, the organization should include methods of reviewing those tools and components related to processing PII. This may include:

- Ongoing monitoring to verify that non-permitted processing is not occurring;
- Specific penetration or vulnerability tests (for example, de-identified datasets may 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 ISO/IEC 27002:2013 plus the additions of this clause create the PIMS-specific guidance for PII controllers.

7.2 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.

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

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

The information required to document the purpose for processing PII is determined by the information (see 7.3.2) that is required to be provided to PII principals, including information necessary to obtain consent (see 7.2.3), as well as records of policies and procedures (see 7.2.7).

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

7.2.2 Identify lawful basis

Control

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

Implementation guidance

Some jurisdictions may require the organization to be able to demonstrate that the lawfulness of processing was duly established before the processing. The legal basis for PII processing may include collection of consent from PII principals, legitimate interests from the controller, performance of a contract or any other condition as per applicable laws.

The legitimate interests of the organization may include, for instance, information security objectives, and should be balanced against the PII principals' privacy protection. Some jurisdictions may define restrictions on the processing of special categories of data, or of data from categories of data subjects (e.g. children), which should be considered when establishing the lawful basis of processing.

7.2.3 Determine when and how consent is to be obtained

Control

The organization should determine and document a process for the demonstration of when and how consent is to be 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 may be useful for the organization to correlate the purpose/s for processing with if and how consent must be obtained.

Some jurisdictions may 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, may have additional requirements. The organization should take into account such requirements and document how mechanisms for consent meet those requirements.

Considerations for the design of mechanisms for obtaining consent may include:

- use of plain language;
- ability of user to decline; and/or
- granularity of consent request (e.g., all PII is not bundled under one request).

7.2.4 Obtain and record consent

Control

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

Implementation guidance

The organization should record consent in accordance with the documented requirements in 7.2.3.

Considerations for the design of mechanisms for obtaining and recording consent may include:

- Use of plain language;
- Ability of user to decline;
- Granularity of consent request (e.g. all PII is not bundled under one request).

7.2.5 Privacy impact assessment

Control

The organization should assess the need for a privacy impact assessment when a new or changed PII processing is planned.

Implementation guidance

Some types of processing may result in risks for PII principals such that these risks should be assessed through a privacy impact assessment. Some jurisdictions may define cases for which a privacy impact assessment should be performed. Criteria may include automated decision making which produce legal effects on PII principals, large scale processing of special categories of PII (e.g., 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 be aware of the elements that are necessary for the completion of a privacy impact assessment. These may include a list of the types of PII being processed, where the PII is stored and where it may be transferred. Data flow diagrams and data maps may also be helpful in this context. See 7.2.7 for details of records of PII processing that might inform a privacy impact or other risk assessment.

NOTE Guidance on the assessment of privacy impacts related to the processing of PI can be found in ISO/IEC 29134 Privacy impact assessment – Guidelines.

7.2.6 Contracts with PII processors

Control

The organization 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 (see ISO/IEC 27001, clause 6.1.2) and the scope of the PII processing performed by the PII processor. 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.

7.2.7 Records related to processing PII

Control

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

Implementation guidance

A step in maintaining records of PII processing is for the organization to have an inventory or list of the PII processing activities that it performs. Such an inventory may include the type of processing, the purposes for that processing and any other details deemed necessary by the organization.

In addition, some jurisdictions may require the organization to record information such as:

- the purpose of 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;
- a Privacy Impact Assessment report.

.

7.3 Rights of PII principals

Objective: To provide PII principals with the appropriate information about the processing of their PII, and to enable them to exercise their rights related to the processing.

7.3.1 Determining PII principals rights and enabling exercise

Control

The organization should ensure that the PII principals' rights related to the processing of their PII are complied with, and provide the means to enable them to exercise their rights.

Implementation guidance

PII principals' rights, including the right of access and correction, may vary from one jurisdiction to another.

Organizations should ensure that they provide the appropriate means for PII principals to exercise their rights in an accessible and timely manner.

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

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 be aware of 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 those requirements (information given punctually or permanently accessible, general information about the processing or specific information), the information may take the form of a notice.

Examples of types of information are:

- contact details about the controller or its representative;
- 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 may access, amend, request erasure, receive a copy of their PII, object to the processing and/or withdraw consent;
- information about the processing (purposes, international transfer and related safeguards, retention period, disclosure, etc.);
- information about transfers of PII;
- information about recipients or categories of recipients of PII;
- information about the use of automated decision taking based on the automated processing of PII;
- information about the right to lodge a complaint and how to lodge such a complaint;
- information regarding corrections to PII;
- information regarding the frequency with which information is provided (e.g. “just in time” notification, organization defined frequency, etc.).

NOTE The information which is to be provided to PII principals may be determined by legal obligations.

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 as 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.

NOTE Icons can sometimes be used to give 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 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, but should be consistent with the requirements used for obtaining consent when possible.

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

Additional information

Withdrawal of consent does not affect processing performed before withdrawal.

Implementation guidance for 7.2.4 also applies.

7.3.5 Provide mechanism to object to processing

Control

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

Implementation guidance

The organization should be aware of laws and regulations related to situations for which PII principals may object to processing. The organization should provide information to principals of their ability to object in these situations. Mechanisms to object may vary, but should be consistent with the type of service provided (e.g. online services should provide this capability online).

7.3.6 Sharing the exercising of PII principals' rights

Control

The organization should implement mechanisms to inform third parties with whom the PII has been shared of any modification, withdrawal or objections resulting from the exercising of PII principals' rights.

NOTE: In some jurisdictions, it is a legal requirement to inform these third parties of these results.

Implementation guidance

The organization should take the appropriate steps, bearing in mind the available technology, to inform third parties of any modifications, withdrawals or objections resulting from the exercising of the PII principals' rights.

NOTE Modifications resulting from the exercising of PII principals' rights may include modifications of consent, requests for correction, erasure, or restrictions on processing, withdrawal or objections submitted or requested by the PII principal.

7.3.7 Correction or erasure

Control

The organization should implement mechanisms to facilitate the exercise of PII principals' rights to access, correct and/or erase their PII.

Implementation guidance

Taking into account the purposes of the processing, such mechanisms should enable PII principals to obtain the rectification or erasure without undue delay.

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

NOTE Records generated by the implementation of the control specified in 7.5.3 may help in this regard.

The organization should also consider implementing policies and procedures for situations when there may be a dispute about the accuracy or correction of the data by the PII principal.

Some jurisdictions may impose restrictions on the circumstances under which, and the extent to which, a PII principal may request correction or erasure of their PII held by an organization. Organizations should make themselves aware of, and abide by, any such restrictions as may be applicable.

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, subject to the retention and deletion policy, when requested by the PII principal.

Implementation guidance

The organization should provide a copy of the PII processed in a structured, commonly used, human-readable format. Some jurisdictions may require the organization to provide a copy of the PII being processed in a structured, commonly used, machine-readable format that is acceptable to the requestor.

NOTE In some jurisdictions where, for example, data portability is required, a format acceptable to another PII controller needs to be used.

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

Consistently with the data minimization objective, in cases where the organization is no longer in position to identify the PII principal (e.g. as a result of a de-identification process), this control should not apply as the organization should not seek to (re-)identify the PII principals for the sole reason of implementing this control.

7.3.9 Request management

Control

The organization should have the means to handle the legitimate requests of PII principals.

Implementation guidance

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

NOTE In some jurisdictions, the organization may be able to charge a fee in certain cases (e.g. excessive or repetitive requests).

Request should be handed in the appropriate defined response times (see 7.3.2 for additional guidance on information provided to PII principals).

7.3.10 Automated decision taking

Control

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

Implementation guidance

In some jurisdictions, the PII principals may have specific rights when a decision based solely on automated PII processing significantly affects him or her, such as the right to be notified of the existence of automated decision making, the right to object to such decision, and/or the right to obtain human intervention.

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

7.4 Privacy by design and by default

Objective: To ensure that processes and systems are designed such that the collection and processing (including use, retention, disclosure, disposal, and transmission) are limited to what is necessary for the identified purpose.

7.4.1 Limit collection

Control

PII controllers 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 information that the organization indirectly collects from or about a PII principal (e.g., through web logs, system logs, etc.).

Organizations should document how this is achieved.

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

Processing may include, but is not limited to, using, retention and disclosure of PII.

Limiting use, retention and disclosure needs to be managed by the availability of corporate policies (see 6.2) along with documented procedures for their adoption and compliance. It is important that all those with access to PII are aware of what they are able (and unable) to do with PII.

7.4.3 Define and document PII minimization and de-identification objectives

Control

The organization should define and document the need for the processing of PII without prior de-identification to achieve the identified purpose, or the extent to which the PII de-identification objectives are set, in such a way that the processing of the resulting de-identified PII is sufficient for the identified purpose.

Implementation guidance

The identified purpose (see 7.2.1) may require the processing of the original PII (i.e. PII which has not been masked or modified by any de-identification technique); in which case the PII processing for the identified purpose should be justified.

In other cases, the identified purpose may not require the processing of the original PII; the processing of PII which has been de-identified may suffice to achieve the identified purpose. In such cases, the organization should define the extent to which de-identification can be used, typically based on the extent to which the PII needs to be associated with the PII principal.

For example, the removal of attributes associated with PII principals may be possible while still permitting the achievement of the purpose. In other cases, generalization techniques (such as rounding) or randomization techniques (such as noise addition) may be applied. For further information on de-identification techniques, refer to ISO IEC 20889 “Privacy enhancing de-identification techniques”.

NOTE For Cloud computing, ISO/IEC 19944 provides a definition of data identification qualifiers that may 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.

7.4.4 Comply with data minimization and de-identification use

Control

The organization should identify and document the mechanisms by which data is processed in a timely manner in such a way that the extent to which the data can identify or be associated with PII principals meets the data minimization and de-identification objectives.

Implementation guidance

Mechanisms used to process PII in accordance with implementation of the control specified in 7.4.2 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 ensure PII minimization.

7.4.5 PII de-identification and deletion

Control

The organization should either delete PII or render it in a form which does not permit 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 a policy to process PII to minimize the possibility of identifying PII principals as soon as possible based on the purposes for which the PII is processed, and to erase the PII when no further processing is anticipated. The organization should have mechanisms in place to process the PII in accordance with the policy.

Organizations should process de-identified PII in a manner that minimizes the possibility of re-identification of PII principals. De-identification of PII should take place as soon as possible, depending on the purposes for which the PII was processed. PII controllers should not retain PII for any longer than is strictly necessary for the specified purposes.

NOTE De-identification techniques such as masking, hashing or replacing direct identifiers might be used. Techniques are further described in ISO IEC 20889 (see Bibliography), and other methods for PII removal are described in ISO/IEC 19944 for Cloud computing.

7.4.6 Temporary files

Control

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

Implementation guidance

Information systems may create temporary files in the normal course of their operation. Such files are specific to the system or application, but may 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 may not 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.

PII processing information systems should implement a periodic check that unused temporary files above a specified age are deleted.

7.4.7 Retention

Control

The organization should not retain PII for longer than necessary for the purpose(s) 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 (for example where a business requirement is longer than a legal minimum requirement), 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 mechanisms for the disposal of PII.

Implementation guidance

The choice of PII deletion techniques depends on the context, as techniques differ in their properties such as the physical granularity of PII to be deleted, accessing or processing (e.g., deleting) the metadata, and the latency until the complete result of the deletion operation is achieved.

7.4.9 Collection procedures

Control

The organization should ensure 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

Organizations should implement policies, procedures and mechanisms to minimize inaccuracies in the PII they process. Organizations should also implement processes, procedures and mechanisms to address how the organization will respond to instances of inaccurate PII. These policies, procedures and mechanisms should be well documented (e.g., through technical system configurations, etc.) and should apply throughout the PII lifecycle."

7.4.10 PII transmission controls

Control

The organization should subject PII transmitted using 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.

7.5 PII sharing, transfer, and disclosure

Objective: To ensure that PII is processed (including use, retention, disclosure, disposal, and transmission) in accordance with applicable obligations where third-parties are involved.

7.5.1 Identify basis for PII transfer

Control

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

Implementation guidance

PII transfer may 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 be aware of such requirements, and take them into consideration when documenting the basis for transfer.

7.5.2 Countries and 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 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 legal or regulatory requirements.

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 exercise of future access rights to the PII principals.

Implementation guidance

Recording may include transfers from third parties of PII which has been modified as a result of PII principals exercising their rights, 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 the records are maintained.

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 may 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.

7.5.5 Joint controller

Control

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

Implementation guidance

Roles and responsibilities for PII processing should be determined in a transparent manner and should at least address the issues that are determined by the organization to be required in order to comply with applicable legislation and/or regulation.

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

Important examples of issues to be documented in a joint controller agreement may include (the list is neither definitive nor exhaustive):

- Purpose of PII sharing / joint controller relationship;
- Identity of the organizations (PII controllers) that are part of the joint 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);
- Responsibility in implementing technical and organizational security measures for PII protection;
- Terms of retention and/or disposal of PII;
- Liabilities for failure to comply with the agreement;
- How PII principals may exercise their rights;
- Providing to PII principals information covering the essence of the arrangement between the joint controllers;
- How PII principals may obtain other information they are entitled to receive; and
- A contact point for PII principals to contact the organizations.

NOTE: Joint controllers need to be able to demonstrate transparency in the sharing of PII. Documenting the agreement is one of the measures that would allow accountability in PII sharing.

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.

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 as a PII controller.

Implementation guidance

Where the customer is the PII controller, matters that should be covered in the contract include cooperation wherever relevant by the organization in respect of, for example:

- Privacy by Design and by Default (see 7.4, 8.4);
- Achieving security of processing;
- Notification of personal data breaches to a supervisory authority;
- Communication of personal data breaches to PII principals;
- Conducting Privacy Impact Assessments (PIA); and
- Conducting prior consultations with relevant PII protection authorities.

Some jurisdictions may 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

Instructions may be documented in the contract between the organization and the customer including, but not limited to, the objective and time frame to be achieved by the service.

In order to achieve the customer's purpose, there may be technical reasons why it is appropriate for an 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 may be necessary to allocate specific processing resources depending on certain characteristics of the PII principal. In circumstances where the organization's determination of the processing

method involves the collection and use of PII, the organization should adhere to the relevant privacy principles set forth in ISO/IEC 29100.

The organization should provide the customer with all relevant information, in a timely fashion, to allow the customer to verify the organization's compliance with the purpose specification and limitation principles and 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 express consent and not make providing such consent a condition for receiving the service.

Implementation guidance

Data processors need to comply with the PII controllers contractual requirements, especially where marketing and/or advertising is planned. Further, PII processors 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 an 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 PII controller and/or 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 may depend on the technological context, on the instruction itself, and on the contract between the organization and the customer.

8.2.5 PII controller obligations

Control

The organization should provide a customer who is a PII controller with the information necessary for it to demonstrate compliance with its obligations.

Implementation guidance

Such information might include whether the organization can allow for and contribute 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 for the processing of PII carried out on behalf of a customer who is a PII controller.

Implementation guidance

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

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

8.3 Rights of PII principals

Objective: To provide PII principals with the appropriate information about the processing of their PII, and to enable them to exercise their rights related to the processing.

8.3.1 Obligations to PII principals

Control

The organization should provide the customer with the means to enable it to fulfil its obligation to facilitate the exercise of PII principals' rights.

Implementation guidance

Where the customer is a PII controller, its obligations in this respect may be defined by law, by regulations or by contract. These obligations may 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 the customer is a PII controller and depends on the organization for information or technical measures to facilitate the exercise of PII principals' rights, the relevant information or technical measures should be specified in a contract.

8.4 Privacy by design and by default

Objective: To ensure that processes and systems are designed such that the collection and processing (including use, retention, disclosure, disposal, and transmission) are limited to what is necessary for the identified purpose.

8.4.1 Temporary files

Control

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

Implementation guidance

Implementation guidance on PII erasure is provided in 7.3.7.

Information systems may create temporary files in the normal course of their operation. Such files are specific to the system or application, but may 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 may not 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.

PII processing information systems should implement a periodic check that unused temporary files above a specified age are deleted.

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 and should make its policy for the exercise of this capability available to the customer before entering into a PII processing contract.

Implementation guidance

At some point in time, PII may need to be disposed of in some manner. This may 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), securely deleting or otherwise destroying it, de-identifying it or archiving it.

The organization should provide the information 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.

The policy should cover the retention period for PII before its destruction 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 7.4.7).

8.4.3 PII transmission controls

Control

The organization should subject PII transmitted using 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 may be included in the PII controller – PII processor contract; if so these requirements need to be met. Where no contractual requirements are in place, it may be appropriate to take advice from the PII controller prior to transmission.

8.5 PII sharing, transfer, and disclosure

Objective: To ensure that PII is processed (including use, retention, disclosure, disposal, and transmission) in accordance with applicable obligations where third-parties are involved.

8.5.1 Basis for transfer of PII

Control

The organization should inform the customer in a timely manner of the basis for relevant PII transfers 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

Where specific contractual agreements apply to the international transfer of data, such as Model Contract Clauses, Binding Corporate Rules or Cross Border Privacy Rules, the agreements and the countries, or the circumstances in which such agreements apply, should also be identified.

8.5.2 Countries and 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 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 related legal or regulatory requirements.

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 may 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

Procedures and time periods may be agreed in the data processing contract.

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 disclosure and accept any contractually agreed requests for PII disclosures that are authorized by the corresponding customer.

Implementation guidance

Details relevant to the implementation of control may be agreed in the data processing contract.

Such requests might originate from several sources, including courts, tribunals and administrative authorities. They may 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 relevant customer before use.

Implementation guidance

Provisions for the use of subcontractors to process PII should be transparent 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, but not any business-specific details. The information disclosed should also include the countries and international organisations to which subcontractors may 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.

8.5.7 Engagement of a subcontractor to process PII

Control

The organization should provide a contractual undertaking not to engage a subcontractor to process PII outside of that described in the contract.

Implementation guidance

Where an organization acting as a PII processor subcontracts some or all of the processing of that PII to another organization, then written authorization from the PII controller is required. This can be in the form of appropriate clauses in the PII controller – PII processor agreement, or can be a specific 'one-off' agreement.

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 an organization acting as a PII processor changes the organization with which it subcontracts some or all of the processing of that PII, then written authorization from the PII controller is required for the change. This can be in the form of appropriate clauses in the PII controller – PII processor agreement, or can be a specific 'one-off' agreement.

Annex A
(normative)

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.

NOTE: 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 5.3).

Table A.1 — Control objectives and controls

A.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.		
A.2.1	Identify and document purpose	*Control* The organization shall identify and document the specific purposes for which the PII will be processed.
A.2.2	Identify lawful basis	*Control* The organization shall determine, document and comply with the lawful basis for the processing of PII for the identified purposes.
A.2.3	Determine when and how consent is to be obtained	*Control* The organization shall determine and document a process for the demonstration of when and how consent is to be obtained from PII principals
A.2.4	Obtain and record consent	*Control* The organization shall obtain and record consent from PII principals according to the documented requirements.
A.2.5	Privacy impact assessment	*Control* The organization shall assess the need for a privacy impact assessment when a new or changed PII processing is planned.

A.2.6	Contracts with PII processors	*Control* The organization shall ensure that their contracts with PII processors address the implementation of the appropriate controls in Annex B.
A.2.7	Records related to processing PII	*Control* The organization shall determine and maintain the necessary records in support of demonstrating compliance with its obligations for the processing of PII.
A.3 Rights of PII principals Objective: To provide PII principals with the appropriate information about the processing of their PII, and to enable them to exercise their rights related to the processing.		
A.3.1	Determining PII principals rights and enabling exercise	*Control* The organization shall ensure that the PII principals' rights related to the processing of their PII are complied with, and provide the means to enable them to exercise their rights.
A.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.3.3	Providing information for 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.3.4	Providing mechanism to modify or withdraw consent	*Control* The organization shall provide a mechanism for PII principals to modify or withdraw their consent.
A.3.5	Providing mechanism to object to processing	*Control* The organization shall provide a mechanism for PII principals to object to the processing of their PII.
A.3.6	Sharing the exercising of PII principles' rights	*Control* The organization shall take reasonable steps to inform third parties with whom the PII has been shared of any modification, withdrawal or objections resulting from the exercising of PII principals' rights.

A.3.7	Correction or erasure	*Control* The organization shall implement mechanisms to facilitate the exercise of PII principals' rights to access, correct and/or erase their PII.
A.3.8	Providing copy of PII processed	*Control* The organization shall be able to provide a copy of the PII that is being processed, subject to the retention and deletion policy, when requested by the PII principal.
A.3.9	Request management	*Control* The organization shall have the means to handle the legitimate requests of PII principals.
A.3.10	Automated decision taking	*Control* The organization shall identify and address any obligations, including legal obligations, to the PII principals resulting from decisions based solely on automated processing of PII.
A.4 Privacy by design and by default Objective: To ensure that processes and systems are designed such that the collection and processing (including use, retention, disclosure, disposal, and transmission) are limited to what is necessary for the identified purpose.		
A.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.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.4.3	Define and document PII minimization and de-identification objectives	*Control* The organization shall define and document the need for the processing of PII without prior de-identification to achieve the identified purpose, or the extent to which the PII de-identification objectives are set, in such a way that the processing of the resulting de-identified PII is sufficient for the identified purpose.
A.4.4	Comply with PII minimization and de-identification objectives	*Control* The organization shall identify and document the mechanisms by which PII is processed in a timely manner in such a way that the extent to which the PII can identify or be associated with PII principals meets the PII minimization and de-identification objectives.

A.4.5	PII de-identification and deletion	*Control* The organization shall either delete PII or render it in a form which does not permit identification of PII principals, as soon as the original PII is no longer necessary for the identified purpose(s).
A.4.6	Temporary files	*Control* The organization shall ensure that temporary files and documents created as a result of PII processing are disposed of (e.g., erased or destroyed) following documented procedures within a specified, documented period.
A.4.7	Retention	*Control* The organization shall not retain PII for longer than necessary for the purpose(s) for which the PII is processed.
A.4.8	Disposal	*Control* The organization shall have documented mechanisms for the disposal of PII.
A.4.9	Collection procedures	*Control* The organization shall ensure 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.4.10	PII transmission controls	*Control* The organization shall subject PII transmitted using a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.
A.5 PII sharing, transfer and disclosure Objective: To ensure that PII is processed (including use, retention, disclosure, disposal, and transmission) in accordance with applicable obligations where third-parties are involved.		
A.5.1	Identify basis for PII transfer	*Control* The organization shall identify and document the relevant basis for transfers of PII.
A.5.2	Countries and 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.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 exercise of future access rights to the PII principals.
A.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.
A.5.5	Joint controllers	*Control* The organization shall determine respective roles and responsibilities for PII processing (including security requirements) with any joint PII controller.

Annex B
(normative)

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.

NOTE: 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 5.3).

Table B.1 — Control objectives and controls

B.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.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 as a PII controller.
B.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.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 express consent and not make providing such consent a condition for receiving the service.
B.2.4	Infringing instruction	*Control* The organization shall inform the PII controller and/or the customer if, in its opinion, a processing instruction infringes applicable legislation or regulation.
B.2.5	PII controller obligations	*Control* The organization shall provide a customer who is a PII controller with the information necessary for it to demonstrate compliance with its obligations.

B.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 for the processing of PII carried out on behalf of a customer who is a PII controller.
B.3 Rights of PII principals Objective: To provide PII principals with the appropriate information about the processing of their PII, and to enable them to exercise their rights related to the processing.		
B.3.1	Obligations to PII principals	*Control* The organization shall provide the customer with the means to enable it to fulfil its obligation to facilitate the exercise of PII principals' rights.
B.3.2	Record of processing activities	*Control* The organization shall determine and maintain the necessary records in support of demonstrating compliance with its obligations for the processing of PII carried out on behalf of a customer who is a PII controller.
B.4 Privacy by design and by default Objective: To ensure that processes and systems are designed such that the collection and processing (including use, retention, disclosure, disposal, and transmission) are limited to what is necessary for the identified purpose.		
B.4.1	Temporary files	*Control* The organization shall ensure that temporary files and documents created as a result of PII processing are disposed of (e.g., erased or destroyed) following documented procedures within a specified, documented period.
B.4.2	Return, transfer or disposal of PII	*Control* The organization shall provide a capability for the return, transfer and/or disposal of PII and should make its policy for the exercise of this capability available to the customer before entering into a PII processing contract.
B.4.3	PII transmission controls	*Control* The organization shall subject PII transmitted using a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.
B.5 PII sharing, transfer and disclosure Objective: To ensure that PII is processed (including use, retention, disclosure, disposal, and transmission) in accordance with applicable obligations where third-parties are involved.		

B.5.1	Basis for transfer of PII	*Control* The organization should inform the customer in a timely manner of the basis for relevant PII transfers 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.5.2	Countries and 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.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.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.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 disclosure and accept any contractually agreed requests for PII disclosures that are authorized by the corresponding customer.
B.5.6	Disclosures of subcontractors used to process PII	*Control* The organization shall disclose any use of subcontractors to process PII to the relevant customer before use.
B.5.7	Engagement of a subcontractor to process PII	*Control* The organization shall provide a contractual undertaking not to engage a subcontractor to process PII outside of that described in the contract.
B.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.

Annex C
(informative)

Mapping to the General Data Protection Regulation

[EDITORS NOTE: This Annex is a proposal to map the controls in this document with the EU GDPR. It has been produced for review and comment.]

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

ISO/IEC 27552 clause	GDPR article
5.2.2	(24)(3), (28)(5), (28)(6), (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)
5.2.3	(35)(9), (36)(1), (36)(3)(c), (36)(3)(e), (36)(3)(a), (36)(3)(b), (36)(3)(d), (36)(3)(f), (36)(5)
5.2.4	(32)(2)
5.4.2	(32)(2)
6.2	(24)(2)
6.2	(37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (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), (37)(6)
6.4	(39)(1)(b)
6.5.1	(5)(1)(f), (32)(1)(a)
6.5.2	(5)(1)(f), (32)(1)(a)
6.6.1	(5)(1)(f)
6.6.2	(5)(1)(f)
6.6.3	(5)(1)(f)
6.6.4	(5)(1)(f)
6.7	(32)(1)(a)
6.8.1	(5)(1)(f)
6.8.2	(5)(1)(f)
6.9.1	(5)(1)(f)
6.9.2	(5)(1)(f), (32)(1)(c)
6.9.3	(5)(1)(f)
6.9.4	(5)(1)(f)
6.10.1	(5)(1)(f)

6.10.2	(5)(1)(f), (28)(3)(b)
6.11.1	(5)(1)(f), (32)(1)(a)
6.11.2	(25)(1)
6.11.1.2	(28)(1), (28)(3)(c), (30)(2)(d), (32)(4), (5)(1)(f)
6.13.1	(33)(2)
6.13.2	(5)(1)(f), (33)(1), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(3)(a), (34)(3)(b), (34)(3)(c), (34)(4)
6.13.3	(33)(2), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(2)
6.15.1	(5)(2), (24)(2)
6.15.2	(32)(1)(d), (32)(2)
6.15.3	(32)(1)(d), (32)(2)
A.2.1	(5)(1)(b)
A.2.2	(5)(1)(a), (6)(1)(a), (6)(1)(b) (6)(1)(c), (6)(1)(d), (6)(1)(e), (6)(1)(f), (6)(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), (10), (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)
A.2.3	(8)(1), (8)(2)
A.2.4	(7)(1), (7)(2), (9)(2)(a)
A.2.5	(35)(1), (35)(10), (35)(11), (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)
A.2.6	(5)(2), (28)(3)(e)
A.2.7	(5)(2), (24)(1), (30)(1)(a), (30)(1)(b), (30)(1)(c), (30)(1)(d), (30)(1)(g), (30)(3)
A.3.1	(12)(2)
A.3.10	(12)(3), (12)(4), (12)(5), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h)
A.3.11	(13)(2)(f), (14)(2)(g), (22)(1), (22)(3)
A.3.2	(11)(2), (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)(3), (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)
A.3.3	(11)(2), (12)(1), (13)(3), (21)(4)
A.3.4	(7)(3), (13)(2)(c), (14)(2)(d), (18)(1)(a), (18)(1)(b), (18)(1)(c), (18)(1)(d)
A.3.5	(13)(2)(b), (14)(2)(c), (21)(1), (21)(2), (21)(3), (21)(6)
A.3.6	(19)
A.3.7	(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)
A.3.8	(12)(7), (15)(3), (20)(1)
A.4.1	(5)(1)(b), (5)(1)(c)
A.4.10	(15)(2); (30)(1)(e), (44), (46)(1)
A.4.2	(25)(2)
A.4.3	(5)(1)(c)

A.4.4	(5)(1)(c)
A.4.5	(5)(1)(c), (5)(1)(e), (6)(4)(e), (11)(1), (32)(1)(a)
A.4.6	(5)(1)(c)
A.4.7	(13)(2)(a), (14)(2)(a)
A.4.8	(5)(1)(f)
A.4.9	(5)(1)(d)
A.5.1	(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)(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)
A.5.2	(30)(1)(e)
A.5.3	(30)(1)(e)
A.5.4	(30)(1)(d)
A.5.5	(26)(1), (26)(2), (26)(3)
B.2.1	(28)(3)(e), (28)(3)(f)
B.2.2	(5)(1)(a), (5)(1)(b) (28)(3)(a), (29), (32)(4)
B.2.3	(7)(4)
B.2.4	(28)(3)(h)
B.2.5	(28)(3)(h)
B.2.6	(30)(2)(a), (30)(2)(b), (30)(3)
B.3.1	(15)(3), (17)(2), (28)(3)(e)
B.4.1	(5)(1)(c)
B.4.2	(28)(3)(g), (30)(1)(f)
B.4.3	(46)(1)
B.5.1	(44), (48)
B.5.2	(30)(2)(c)
B.5.3	(28)(3)(a)
B.5.4	(48)
B.5.5	(30)(1)(d)
B.5.6	(28)(2), (28)(4)
B.5.7	(28)(2), (28)(3)(d)
B.5.8	(28)(2)

Annex D
(informative)

Mapping to ISO/IEC 29100

[EDITORS NOTE: This Annex is a proposal to map the controls in this document with ISO/IEC 29100. It has been produced for comment.]

D.1 Mapping for PII controllers

Privacy Principles of ISO/IEC 29100	***Related Controls for PII controllers***
1. Consent and Choice	A.2.1 Identify and document purpose A.2.2 Identify lawful basis A.2.3 Determine when consent is to be obtained A.2.4 Obtain and record consent A.2.5 Privacy impact assessment A.3.2 Determining information for PII principals A.3.3 Providing information to PII principals A.3.4 Provide mechanism to modify or withdraw consent A.3.5 Provide mechanism to object to processing A.3.6 Sharing the exercising of PII principals rights
2. Purpose of legitimacy and specification	A.2.1 Identify and document purpose A.2.2 Identify lawful basis A.2.5 Privacy impact assessment A.3.2 Determining information for PII principals A.3.3 Providing information to PII principals
3. Collection limitation	A.2.5 Privacy impact assessment A.4.1 Limit collection
4. Data minimization	A.4.2 Limit processing A.4.3 Define and document PII minimization and de-identification objectives A.4.4 Comply with PII minimization and de-identification objectives A.4.5 PII de-identification and deletion
5. Use, retention and disclosure limitation	A.4.3 Define and document PII minimization and de-identification objectives A.4.4 Comply with PII minimization and de-identification objectives A.4.5 PII de-identification and deletion A.5.4 Records of PII disclosure to third parties
6. Accuracy and quality	A.4.9 Collection procedures
7. Openness, transparency and notice	A.3.2 Determining information for PII principals A.3.3 Providing information to PII principals
8. Individual participation and access	A.3.1 Determining PII principals rights and enabling exercise A.3.3 Providing copy of PII processed

	A.3.7 Correction or erasure A.3.9 Request management A.3.10 Automated processing
9. Accountability	A.2.6 Contracts with PII processors A.2.7 Records of policies and procedures A.3.9 Support from PII processors A.3.10 Request management A.5.2 Countries to which PII might be transferred A.5.3 Records and transfer of personal data A.5.5 Joint controller
10. Information Security	A.2.6 Contracts with PII processors A.4.10 PII transmission controls
11. Privacy compliance	A.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.2.5 PII controller obligations to PII principals
2. Purpose of legitimacy and specification	B.2.2 Organization's purposes B.2.3 Marketing and advertising use B.2.4 Infringing instruction B.3.2 Record of processing activities
3. Collection limitation	N/A
4. Data minimization	B.4.1 Temporary files
5. Use, retention and disclosure limitation	B.5.3 Notification of PII disclosure requests B.5.4 Legally binding PII disclosures B.5.5 Records of PII disclosure to third parties
6. Accuracy and quality	N/A
7. Openness, transparency and notice	B.5.6 Disclosure of subcontractors used to process PII B.5.7 Engagement of a sub-contractor to process PII B.5.8 Change of subcontractor to process PII
8. Individual participation and access	N/A
9. Accountability	B.2.6 Records of policies and procedures B.4.2 Return, transfer or disposal of PII B.5.1 Basis for transfer of PII B.5.2 Countries and organizations to which PII might be transferred
10. Information Security	N/A
11. Privacy compliance	B.2.5 PII controller obligations

Annex E
(informative)

Mapping to ISO/IEC 27018 and ISO/IEC 29151

[EDITORS NOTE: This Annex is a proposal to map the controls in this document with ISO/IEC 27018 and ISO/IEC 29151. It has been produced for comment.]

ISO/IEC 27552 clause	ISO/IEC 27018 clause	ISO/IEC 29151 clause
5.2.1	N/A	N/A
5.2.2	N/A	N/A
5.2.3	N/A	N/A
5.4.2	N/A	A.12
5.5.3	7.2.2	7.2.3, A.11.5
6.2	6.1.1	A.11.1
6.5.1	N/A	8.2.1
6.5.2	A.10.5	8.2.6
6.5.3	A.10.4	8.3.4
6.6.1	9.2	N/A
6.6.2	9.2.1, A.10.10	9.2.2
6.6.3	A.10.9	9.2.3
6.6.4	A.10.8	9.2.4
6.6.5	9.4.2	9.4.3
6.7	10.1.1	N/A
6.8.1	11.2.7, A.10.13	11.2.8
6.8.2	A.10.2	N/A
6.9.1	N/A	12.1.5
6.9.2	12.3.1, A.10.3	12.3.2
6.9.3	12.4.1	12.4.2
6.9.4	12.4.2	12.4.3
6.10.1	13.2.1	13.2.2
6.10.2	A.10.11	13.2.5
6.11.1	A.10.6	N/A
6.11.2	N/A	N/A
6.13.1	16.1	N/A

6.13.2	16.1.1	16.1.2, A.11.1, A.11.6
6.13.3	A.9.1	N/A
6.15.1	A.9.2	N/A
6.15.2	18.2.1	18.2.2, A.11.4
6.15.3	N/A	N/A
A.2.1	N/A	A.4.2
A.2.2	N/A	A.4.1
A.2.3	N/A	N/A
A.2.4	N/A	A.3.1
A.2.5	N/A	A.11.2
A.2.6	N/A	A.11.3
A.2.7	N/A	N/A
A.3.1	N/A	A.10.1
A.3.2	N/A	N/A
A.3.3	N/A	A.4.2, A.9.1, A.9.2
A.3.4	N/A	N/A
A.3.5	N/A	N/A
A.3.6	N/A	N/A
A.3.7	N/A	A.10.2
A.3.8	N/A	N/A
A.3.9	N/A	N/A
A.3.10	N/A	A.10.3
A.3.11	N/A	N/A
A.4.1	N/A	A.5, A.6
A.4.2	N/A	N/A
A.4.3	N/A	N/A
A.4.4	N/A	N/A
A.4.5	N/A	A.7.2
A.4.6	N/A	A.6
A.4.7	N/A	A.7.1
A.4.8	N/A	N/A
A.4.9	N/A	A.8
A.4.10	N/A	N/A
A.5.1	N/A	A.13.2

A.5.2	N/A	A.13.2
A.5.3	N/A	A.13.2
A.5.4	N/A	A.7.3
A.5.5	N/A	A.7.4
B.2.1	N/A	N/A
B.2.2	A.2.1	N/A
B.2.3	A.2.2	N/A
B.2.4	N/A	N/A
B.2.5	N/A	N/A
B.2.6	N/A	N/A
B.3.1	A.1.1	N/A
B.4.1	A.4.1	N/A
B.4.2	A.9.3	N/A
B.4.3	A.11.2	N/A
B.5.1	N/A	N/A
B.5.2	A.11.1	N/A
B.5.3	A.5.1	N/A
B.5.4	N/A	N/A
B.5.5	A.5.2	N/A
B.5.6	A.7.1	A.7.5
B.5.7	N/A	N/A
B.5.8	N/A	N/A

Bibliography

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

[2] 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*

[3] ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

[4] ISO/IEC 29134:2017, *Information technology — Security techniques — Privacy impact assessment – Guidelines*

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

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

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