



ISO/IEC JTC 1/SC 27 **N14292**

ISO/IEC JTC 1/SC 27/WG 5 **N514292**

REPLACES: N13385, N14166

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: working draft text

TITLE: Text for ISO/IEC 3rd WD 29151 — Information technology — Security techniques — Code of practice for PII protection

SOURCE: Project editor (Heung Youl Youm and B. Kenyon)

DATE: (2014-06-15) re-issued: 2014-06-20

PROJECT: 1.27.105 (ISO/IEC 29151)

STATUS: In accordance with resolution 2 (see SC 27 N14199) of the 17th SC 27/WG 5 Plenary meeting held in Hong Kong, China, on 7th – 11th April 2014 this document is being circulated for STUDY AND COMMENT.

Experts, liaison organizations and National Bodies are kindly requested to send their comments/contributions on the above-mentioned document by **2014-09-24**.

PLEASE submit your comments / contributions on the hereby attached document via the SC 27 e-balloting/commenting website at: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

PLEASE NOTE For comments please use the SC 27 TEMPLATE separately attached to this document.

ACTION: COMM

DUE DATE: 2014-09-24

DISTRIBUTION: P-, O- and L-Members
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-Chair
E. J. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenbergh, WG-Convenors
Heung Youl Youm, B. Kenyon, Project editors

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

NO. OF PAGES: 1 + 54

Information technology — Security techniques — Code of practice for PII protection

Élément introductif — Élément central — Partie 4: Titre de la partie

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.

Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

Secretariat of ISO/IEC JTC 1/SC 27
DIN German Institute for Standardization
DE-10772 Berlin

Tel. + 49 30 2601 2652
Fax + 49 30 2601 4 2652
E-mail krystyna.passia@din.de

Web <http://www.jtc1sc27.din.de/en> (public web site)
<http://isotc.iso.org/isotcportal/index.html> (SC27 documents)

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Contents

	Page
FOREWORD.....	V
INTRODUCTION	VI
1 SCOPE	1
2 NORMATIVE REFERENCES.....	1
3 TERMS AND DEFINITIONS AND ACRONYMS	1
4 OVERVIEW	2
5 INFORMATION SECURITY POLICIES.....	4
6 ORGANIZATION OF INFORMATION SECURITY.....	5
7 HUMAN RESOURCE SECURITY	7
8 ASSET MANAGEMENT	8
9 ACCESS CONTROL	10
10 CRYPTOGRAPHY	12
11 PHYSICAL AND ENVIRONMENTAL SECURITY	12
12 OPERATIONS SECURITY	14
13 COMMUNICATIONS SECURITY	16
14 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE	17
15 SUPPLIER RELATIONSHIPS	19
16 INFORMATION SECURITY INCIDENT MANAGEMENT.....	19
17 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT	21
18 COMPLIANCE	22
19 EXTENDED CONTROL SET FOR PII PROTECTION.....	23
19.1 CONSENT AND CHOICE.....	23
19.2 PURPOSE LEGITIMACY AND SPECIFICATION.....	25
19.3 COLLECTION LIMITATION	27
19.4 DATA MINIMIZATION	28
19.5 USE, RETENTION AND DISCLOSURE LIMITATION.....	29
19.6 ACCURACY AND QUALITY	30
19.7 OPENNESS, TRANSPARENCY AND NOTICE	31
19.8 PII PRINCIPAL PARTICIPATION AND ACCESS.....	33
19.9 ACCOUNTABILITY	35
19.10 INFORMATION SECURITY	38
19.11 PRIVACY COMPLIANCE.....	38

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national 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 and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29151 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, Security techniques.

Introduction

The number of organizations processing personally identifiable information (PII) is increasing, as is the amount of PII that these organizations deal with. At the same time, the societal expectation for the protection of an individual's privacy and for the security of data relating to the individual is increasing too. In a number of countries, legislators and regulators are addressing new requirements for the protection of PII and dealing with high-profile breaches of the existing requirements.

As the numbers of PII breaches increase, the organizations including smaller newcomers (e.g., small and medium enterprises (SMEs)) will increasingly need guidance on how they should protect PII in order to reduce the risk of privacy breaches occurring, and to reduce the impact of breaches on the organization and on the individuals concerned. Therefore, there is a need for guidance on how organizations should protect PII.

This document is not exhaustive. Controls should be chosen based on the risks identified as a result of a risk analysis to develop a comprehensive, consistent system that includes other controls. They should be adapted to the context of the particular processing of PII.

While this International Standard offers guidance on a broad range of information security and privacy controls that are commonly applied in many different organizations that deal with protection of PII, the remaining parts of the ISO/IEC 27000 family of standards provide complementary advice or requirements on other aspects of the overall process of protecting PII:

- ISO/IEC 27001 defines an information security management process and associated requirements, which may be adapted for use as a basis of a privacy/personal information management system.
- ISO/IEC 27009 provides a certification model to follow in setting up and operating a management system, which can be applicable to third-party accredited management systems including privacy/personal information management system.
- ISO/IEC 29134 provides a methodology for identifying, analysing, and assessing privacy risks, while ISO/IEC 27001 together with ISO/IEC 27005 provides a methodology for identifying, analysing, and assessing security risks.

Figure 1 describes the relationship between ISO/IEC 29151 and ISO/IEC 27000 family of international standards.

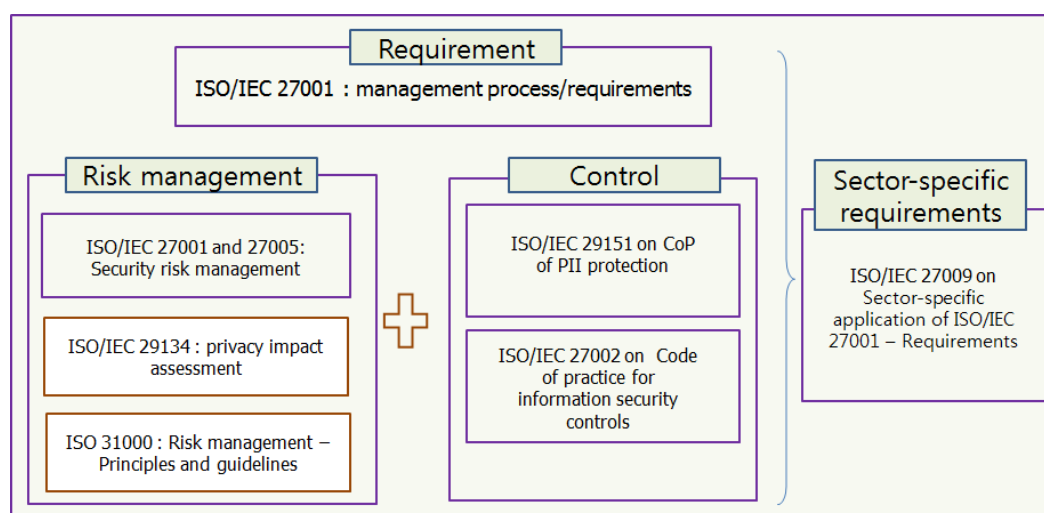


Figure 1- The relationship of ISO/IEC 29151 and ISO/IEC 27000 family of standards

Editor's note: It will be checked if statements in Figure1 are correct at the final stage of this IS.

Although much of this International Standard makes great use of guidelines based on ISO/IEC 27002, these have had to be adapted for personal privacy where PII processing may be undertaken

a) in different processing domains such as :

- domestic processing;
- social networking or public processing;
- product and service provision processing by organisations;
- search, analysis or PII Principal targeting processing by 3rd parties
- big data analytics;
- lawful intervention and law enforcement;
- employment processing,

b) in different locations:

- on a personal processing platform provided to an individual (smart cards, smart phones and their apps, smart meters etc.);
- within data transportation and collection networks e.g. where mobile phone locational data is created operationally by the network processing and that becomes PII;
- within an organisation's own processing infrastructure;
- on a third party's processing platform,

c) under different data collection operational requirements that provide the functionality for the processing purpose:

- one off data collection e.g. on registering for a service online;
- multiple ongoing data collection e.g. frequent health parameter monitoring by sensors on or in an individual's body, multiple data collections using contactless payment cards for payment, smart meter data collection systems and so on.

Note multiple ongoing data collection can contain or yield behavioural, locational and other types of PII. In such cases the use of privacy controls need to be considered that allow access and collection rights to be changed by context and for that change control to be exercised by the individual.

Editor's note: NBs are asked to submit the supporting text regarding the intent of the paragraph above.

Information technology — Security techniques — Code of practice for PII protection

1 Scope

This International Standard establishes commonly accepted control objectives, controls and related guidelines for the treatment of risks that have been identified through a risk analysis process such as the one described in ISO/IEC 29134 - Privacy impact assessment: Methodology.

In particular, this International Standard specifies guidelines as well as privacy controls based on ISO/IEC 27002 in accordance with the privacy principles in ISO/IEC 29100, taking into consideration the regulatory requirements for processing PII which may be applicable within the context of an organization's information security risk environment(s).

This standard does not imply that it is possible to modify ISO/IEC 27001 requirements, but only to identify more specific or additional requirements.

This International Standard is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations, such as PII controllers that collect PII and determine the purposes for which it is processed, and PII processors that process PII on behalf of the PII controller.

Editor's note: The structure of the international standard, especially clause 19, will be revisited when this document is mature.

Editor's note: The generic controls from ISO/IEC 27018 will be considered to be integrated into this Document when ISO/IEC 27018 will be published.

Editor's note: National bodies are asked to provide items to move some items in 27018 to 29151.

2 Normative references

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

ISO/IEC 27000:2012, 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 and definitions and acronyms

For the purposes of this document, the terms and definitions that are given in ISO/IEC 2700:2013 and ISO/IEC 29100:2011 apply.

Editor's note: New terms and definitions will be added, if necessary.

1 In addition, the following acronyms apply.

2 PbD Privacy by Design

3 PFI Personal Financial Information

4 PHI Personal Health Information)

5 PII Personally Identifiable Information

6 PIA Privacy Impact Assessment

7 SME Small and medium enterprise

8 **4 Overview**

9 **4.1 Structure of this standard**

10 This International Standard has a structure similar to that of ISO/IEC 27002. In cases where objectives and
11 controls specified in ISO/IEC 27002 are applicable without a need for any additional information, only a
12 reference is provided to ISO/IEC 27002. Control and implementation guidance specific to the processing of PII
13 is described in Clause 19.

14 In cases where controls need additional guidance specific to the protection of PII, this is given under the
15 heading "Implementation guidance specific to PII protection". Such guidance and information is included in
16 the following categories, as defined in ISO/IEC 27002. Clause numbers and their titles, which have been
17 aligned with the corresponding clause numbers in ISO/IEC 27002, are indicated in the Table 1.

18 Editor's note: Further comments are invited regarding new Clauses on privacy policy (clause 5), Organization
19 of PII protection (clause 6) and PII protection incident management (clause 15).

20 **4.2 Control categories**

21 In line with ISO/IEC 27002, each main control category contains:

- 22 a) a control objective stating what is to be achieved; and
- 23 b) one or more controls that can be applied to achieve the control objective.

24 Control descriptions are structured as follows:

25 Control

26 Defines the specific control statement to satisfy the control objective.

27 Implementation guidance for the protection of PII

28 Provides more detailed information to support the implementation of the control and meeting the control
29 objectives. The guidance may not be entirely suitable or sufficient in all situations, and may not fulfil the
30 organization's specific control requirements. Alternative or additional controls, or other forms of risk treatment
31 (avoiding, transferring or accepting risks), may therefore be appropriate.

32 Other information for the protection of PII

33 Provides further information that may need to be considered, such as legal considerations and references to
34 other standards.

4.3 Requirements for the protection of PII

It is essential that an organization identifies its PII protection requirements. The requirements in ISO/IEC 29100 apply. There are three main sources of PII protection requirements:

- (a) Legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy, and their socio-cultural environment, which are related to privacy;
- (b) Assessing risks (i.e. security risks and privacy risks) to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated;
- (c) Set of principles (i.e. privacy principles described in ISO/IEC 29100), objectives and business requirements for processing PII that an organization has developed to support its operations.

Security and privacy controls need to be selected on the basis of a risk analysis. The results of a risk assessment will help guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

In addition, ISO/IEC 29134 provides privacy risk assessment guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.

4.4 Protection objectives and risk assessment for the protection of PII

4.4.1 Protection objectives for to the protection of PII

The objective of the protection of PII is to enable organizations to put in place, as part of the overall protection, a set of controls for PII protection which provides a framework for maintaining and improving compliance with privacy related laws and regulations, managing privacy risks and enhancing trust of PII principals, regulators or clients, in accordance with the privacy principles described in ISO/IEC 29100.

4.5 Controls for the protection of PII

Organizations should identify and implement controls to treat the risks identified by the risk assessment and treatment process. In addition, the identified and implemented controls should be documented as part of the organization's privacy risk assessment. Certain types of PII processing can warrant specific controls for which the need only becomes apparent once an envisaged operation has been carefully analyzed. A privacy risk assessment can assist organizations in identifying the specific risks of privacy breaches involved in an envisaged operation.

4.6 Selecting controls

Controls can be selected from this International Standard (which includes by reference the controls from ISO/IEC 27002, creating a combined reference control set for the application defined by the scope). If required, controls can also be selected from other control sets, or new controls can be designed to meet specific needs as appropriate.

The selection of controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options, and the general risk management approach applied to the organization and, through contractual agreements, its customers and suppliers, and should also be subject to all relevant national and international legislation and regulations. Where controls from this International Standard are not selected this should be documented with the justification.

Further, the selection and implementation of controls is dependent upon the organization's actual role in the provision of infrastructure or services. Many different organizations may be involved in providing infrastructure and/or services. In some circumstances, selected controls may be unique to a particular organization. In other

instances, there may be shared roles in implementing security controls. Contractual agreements should clearly specify the PII protection responsibilities of all organizations involved in providing or using the services.

The controls in this standard can be considered as guiding principles and applicable for most organizations.

They are explained in more detail below along with implementation guidance. Implementation may be made simpler if requirements for the protection of PII have been considered in the design of the organization's information system, services and operations. Such consideration is an element of the concept that is often called "Privacy by Design". More information about selecting controls and other risk treatment options can be found in ISO/IEC 29134 – Privacy impact assessment - Methodology. Other relevant references are listed in the bibliography

Editor's note: It will be checked if reference 29134 is correct at the final stage of this IS.

4.7 Developing your own guidelines

This International Standard may be regarded as a starting point for developing organization specific guidelines. Not all of the controls and guidance in this guideline may be applicable.

Furthermore, additional controls and guidelines not included in this Recommendation may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this standard where applicable to facilitate compliance checking by auditors and business partners.

4.8 Lifecycle considerations

PII has a natural lifecycle, from creation and origination through storage, processing, use and transmission to its eventual destruction or decay. The value of, and risks to, assets may vary during their lifetime (e.g. unauthorized disclosure or theft of a company's financial accounts is far less significant after they have been formally published) but protection of PII remains important to some extent at all stages.

Information systems have lifecycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained and eventually retired from service and disposed of. PII protection should be taken into account at each of these stages as well. New system developments and changes to existing systems present opportunities for organizations to update and improve security and privacy controls, taking actual incidents and current and projected information security and privacy risks into account.

5 Information Security policies

5.1 Management directions for information security

The objective specified in clause 5.1 of ISO/IEC 27002 applies.

5.1.1 Policies for information security

Control 5.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following additional guidance also applies.

Implementation guidance for the protection of PII

The information security policies should be augmented by a statement (e.g. in a privacy policy) concerning support for and commitment to managing compliance with applicable PII protection legislation and contractual requirements.

The privacy policy in ISO/IEC 29100 apply. Privacy Policy being part of security policy will not be appropriate as security policy is regarding confidentiality, integrity, and availability, whereas privacy has a lot of other principles which have nothing to do with security.

1 When designing, implementing and reviewing security policy, organizations should consider privacy
2 safeguarding requirements.

3 Other information for the protection of PII

4 In some jurisdictions the processing of PII is directly subject to PII protection legislation. Elsewhere, PII
5 protection legislation applies to the PII controller.

6 **5.1.2 Review of the policies for information security**

7 Control 5.1.2 and the associated implementation guidance specified in ISO/IEC 27002 apply.

8 **5.1.3 Policies and review for Privacy**

9 Implementation guidance for the protection of PII

10 The privacy policy should:

- 11 • be appropriate to the purpose of the organization;
- 12 • provide the framework for setting objectives;
- 13 • define rules for making decisions in questions of privacy;
- 14 • define rules on privacy risk acceptance (see also ISO/IEC 29134 clause 5.3.2);
- 15 • include a commitment to satisfy applicable privacy safeguarding requirements;
- 16 • include a commitment to continual improvement;
- 17 • be communicated within the organization; and
- 18 • be available to interested parties, as appropriate.

19 **6 Organization of information security**

20 **6.1 Internal organization**

21 The objective specified in clause 6.1 of ISO/IEC 27002 applies.

22 **6.1.1 Information security roles and responsibilities**

23 Control 6.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002
24 apply. The following additional guidance also applies.

25 Implementation guidance for the protection of PII

26 Areas for which individuals are responsible should be clearly stated. In particular the following should take
27 place:

- 28 (a) A senior individual within the organization should be assigned responsibility for the management, including
29 the protection, of PII. This individual will be responsible for monitoring and ensuring compliance with
30 relevant legislation, regulations and so on. Other individuals within the organization may be designated to
31 assist the senior individual;.

(b) An individual (or individuals) should be assigned responsibility for cooperating with the information security functions within the organization.

The established PII protection function should work closely with other functions processing PII and also information security function which implement security requirements of data privacy laws and legal function which assists in interpreting statutes and in handling data breaches.

The organization should examine the need for and establish as appropriate, a cross-functional council or committee comprising of senior members from functions that process PII. Privacy being a multi-disciplinary function, such council can help in proactively identifying opportunities for improvements, identifying new risks, areas for conducting privacy impact assessments, planning preventive actions for any breaches etc. It is recommended that such council should meet periodically and be chaired and governed by a senior management representative.

6.1.2 Segregation of duties

Control 6.1.2 and the associated implementation guidance specified in ISO/IEC 27002 apply. The following additional guidance also applies.

Implementation guidance for the protection of PII

Duties and area of responsibilities for PII protection function should be independent of those for information security.

Individuals in PII protection function should report to a senior management or member of the board in order to ensure provision of sufficient authority.

6.1.3 Contact with authorities

Control 6.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following additional guidance also applies.

Implementation guidance for the protection of PII

Organizations should also have procedures in place that specify when and by whom authorities (including data protection authority) should be contacted and how identified privacy incidents should be reported.

6.1.4 Contact with special interest groups

Control 6.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

6.1.5 Information security in project management

Control 6.1.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

6.2 Mobile devices and teleworking

The objective specified in clause 6.2 of ISO/IEC 27002 applies.

6.2.1 Mobile device policy

Control 6.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

6.2.2 Teleworking

1 Control 6.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002
2 apply.

3 **7 Human resource security**

4 During the course of employment (from pre-employment screening to termination of employment and beyond),
5 an organization may process PII. This PII shall be adequately protected throughout its lifecycle.

6 **7.1 Prior to employment**

7 The objective specified in clause 7.1 of ISO/IEC 27002 applies.

8 **7.1.1 Screening**

9 Control 7.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002
10 apply.

11 **7.1.2 Terms and conditions of employment**

12 Control 7.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002
13 apply.

14 **7.2 During employment**

15 The objective specified in clause 7.2 of ISO/IEC 27002 applies.

16 **7.2.1 Management responsibilities**

17 Control 7.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002
18 apply.

19 **7.2.2 Information security awareness, education and training**

20 Control 7.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002
21 apply.

22 Editor's note: NBs are asked to provide a supporting text regarding this clause.

23 **7.2.3 Disciplinary process**

24 Control 7.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002
25 apply.

26 **7.3 Termination and change of employment**

27 The objective specified in clause 7.3 of ISO/IEC 27002 applies. The following additional guidance also applies.

28 Implementation guidance for the protection of PII

29 PII of employees should be deleted, stored or archived based on the data retention policy, notice and consent
30 of the employee.

31 **7.3.1 Termination or change of employment responsibilities**

32 Control 7.3.1 and the associated implementation guidance and other information specified in ISO/IEC 27002
33 apply.

8 Asset management

8.1 Responsibility for assets

The objective specified in clause 8.1 of ISO/IEC 27002 applies.

8.1.1 Inventory of assets

Control 8.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following additional guidance also applies.

Implementation guidance for the protection of PII

Organizations should establish, maintain, and update an inventory of asset that contains a list of programs and information systems which process PII.

Organizations should provide regular updates of a PII inventory to the person in charge of the privacy and protection of PII issues to support the establishment of appropriate security controls for all new or updated information system processing PII.

The PII inventory enables organizations to implement effective, administrative, technical and physical security policies and procedures to protect PII consistently.

When developing and maintaining the inventory of PII, organizations may extract the following information elements from Privacy Impact Assessments (PIAs) concerning information systems processing PII:

(a) the name and acronym for each identified system;

(b) the types of PII processed by those systems;

(c) the classification or level of sensitivity of all types of PII, both as individual information elements and as combined in those information systems;

(d) the level of potential risks, to the PII principal and the organization, of any breach of PII;

(e) the purpose of collecting the PII;

(f) whether PII processing will be outsourced to a vendor; and

(g) whether trans-border data transfer is involved.

In the course of updating the PII inventory, organizations should take steps to identify data that if linked to other available information could create PII.

8.1.2 Ownership of assets

Control 8.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.1.3 Acceptable use of assets

Control 8.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. .

8.1.4 Return of assets

Control 8.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.2 Information classification

The objective specified in clause 8.2 of ISO/IEC 27002 applies.

8.2.1 Classification of information

Control 8.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following additional guidance also applies.

Implementation guidance for the protection of PII

Data classification should appropriately include the categories of PII. PII can be classified as sensitive, non-sensitive, personal health information (PHI), personal financial information (PFI), etc.

Organizations should classify PII depending on their importance into sensitive PII and non-sensitive PII in accordance with value, legal or contractual requirement, criticality, and severity which should be defined in the privacy policy of an organization or contractual agreement. Sensitive PII should be clearly identified.

Same PII that may be classified non-sensitive in one country may be treated sensitive in a different part of the world due to applicable data privacy laws.

NOTE- The classification for a PII could change when associated with one or more other values.

8.2.2 Labelling of Information

Control 8.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.2.3 Handling of assets

Control 8.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.3 Media handling

The objective specified in clause 8.3 of ISO/IEC 27002 applies.

8.3.1 Management of removable media

Control 8.3.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following additional guidance also applies.

Implementation guidance for the protection of PII

Some laws in certain jurisdictions may require portable media containing PII to be encrypted. In any case, encryption is recommended to avoid breach notification obligations.

8.3.2 Disposal of media

Control 8.3.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.3.3 Physical media transfer

Control 8.3.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9 Access control

9.1 Business requirement of access control

The objective specified in clause 9.1 of ISO/IEC 27002 applies.

9.1.1 Access control policy

Control 9.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.1.2 Access to networks and network services

Control 9.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.2 User access management

The objective specified in clause 9.2 of ISO/IEC 27002 applies.

9.2.1 User registration and de-registration

Control 9.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following additional guidance also applies.

Implementation guidance for the protection of PII

Organization should provide appropriate right of access to the information systems processing PII as well as other sensitive data to the minimum number of individuals.

9.2.2 User access provisioning

Control 9.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.2.3 Management of privileged access rights

Control 9.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following additional guidance also applies.

Implementation guidance for the protection of PII

Organizations should give special care about assigning privileged access rights of massive PII processing operation to personnel, taking into account high risks PII processing may cause undetected massive breach of PII from massive batch PII processing operations, i.e. batch query, batch modification, batch export, and batch deletion of PII.

Organizations should assign privileged access right of performing high risk PII processing operations to at least two or more personnel to prevent the abuse of PII.

Organizations should assign privileged access right of PII processing operation to different personnel.

9.2.4 Management of secret authentication information of users

Control 9.2.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.2.5 Review of user access rights

Control 9.2.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.2.6 Removal or adjustment of access rights

Control 9.2.6 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.3 User responsibilities

The objective specified in clause 9.3 of ISO/IEC 27002 applies.

9.3.1 Use of secret authentication information

Control 9.3.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.4 System and application access control

The objective specified in clause 9.4 of ISO/IEC 27002 applies.

9.4.1 Information access restriction

Control 9.4.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following additional guidance also applies.

Implementation guidance for the protection of PII

Before allowing individuals such as operators and administrators to use Query languages, which enables automatic retrieval of PII from database, organization should review the validity of the use of Query language to the PII processing systems.

In the case where the use of Query language is compliant with the protection requirement, organizations should provide a technical mean of limiting the use of Query language to the agreed extent.

1 It can, for example, mean that restrictions of access control limit the use of query language to a few predefined
2 sensitive fields or the records.

3 **9.4.2 Secure log-on procedures**

4 Control 9.4.2 and the associated implementation guidance and other information specified in ISO/IEC 27002
5 apply.

6 **9.4.3 Password management system**

7 Control 9.4.3 and the associated implementation guidance and other information specified in ISO/IEC 27002
8 apply.

9 **9.4.4 Use of privileged utility programs**

10 Control 9.4.4 and the associated implementation guidance and other information specified in ISO/IEC 27002
11 apply.

12 **9.4.5 Access control to program source code**

13 Control 9.4.5 and the associated implementation guidance and other information specified in ISO/IEC 27002
14 apply.

15 **10 Cryptography**

16 **10.1 Cryptographic controls**

17 The objective specified in clause 10.1 of ISO/IEC 27002 applies.

18 **10.1.1 Policy on the use of cryptographic controls**

19 Control 10.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002
20 apply. The following additional guidance also applies.

21 Implementation guidance for the protection of PII

22 When being stored in the database, PII, e.g. national identifier, passport number or credit card number should
23 be encrypted.

24 **10.1.2 Key management**

25 Control 10.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002
26 apply.

27 **11 Physical and environmental security**

28 **11.1 Secure areas**

29 The objective specified in clause 11.1 of ISO/IEC 27002 applies.

30 **11.1.1 Physical security perimeter**

1 Control 11.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002
2 apply.

3 **11.1.2 Physical entry controls**

4 Control 11.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002
5 apply.

6 **11.1.3 Securing offices, rooms and facilities**

7 Control 11.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002
8 apply.

9 **11.1.4 Protecting against external and environmental threats**

10 Control 11.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002
11 apply.

12 **11.1.5 Working in secure areas**

13 Control 11.1.5 and the associated implementation guidance and other information specified in ISO/IEC 27002
14 apply.

15 **11.1.6 Delivery and loading areas**

16 Control 11.1.6 and the associated implementation guidance and other information specified in ISO/IEC 27002
17 apply.

18 **11.2 Equipment**

19 The objective specified in clause 11.2 of ISO/IEC 27002 applies.

20 **11.2.1 Equipment siting and protection**

21 Control 11.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002
22 apply.

23 **11.2.2 Supporting utilities**

24 Control 11.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002
25 apply.

26 **11.2.3 Cabling security**

27 Control 11.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002
28 apply.

29 **11.2.4 Equipment maintenance**

30 Control 11.2.4 and the associated implementation guidance and other information specified in ISO/IEC 27002
31 apply.

32 **11.2.5 Removal of assets**

Control 11.2.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2.6 Security of equipment and assets off-premises

Control 11.2.6 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2.7 Secure disposal or re-use of equipment

Control 11.2.7 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

Editor's note: NBs are asked to provide a supporting text regarding using the text in 27018 for this clause.

11.2.8 Unattended user equipment

Control 11.2.8 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2.9 Clear desk and clear screen policy

Control 11.2.9 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12 Operations security

12.1 Operational procedures and responsibilities

The objective specified in clause 12.1 of ISO/IEC 27002 applies.

12.1.1 Documented operating procedures

Control 12.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.1.2 Change management

Control 12.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.1.3 Capacity management

Control 12.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.1.4 Separation of development, testing and operational environments

Control 12.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

Editor's note: NBs are asked to provide a supporting text regarding this clause.

12.2 Protection from malware

The objective specified in clause 12.2 of ISO/IEC 27002 applies.

12.2.1 Controls against malware

Control 12.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.3 Backup

The objective specified in clause 12.3 of ISO/IEC 27002 applies.

12.3.1 Information backup

Control 12.3.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following additional guidance also applies.

Implementation guidance for the protection of PII

Backup systems should ensure timely availability of PII for PII subject access requests in the event of PII non-availability in primary storage.

Backup systems should have provision to facilitate deletion of PII as per organizational data retention policies.

12.4 Logging and monitoring

The objective specified in clause 12.4 of ISO/IEC 27002 applies.

12.4.1 Event logging

Control 12.4.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.4.2 Protection of log information

Control 12.4.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.4.3 Administrator and operator logs

Control 12.4.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following additional guidance also applies.

Implementation guidance for the protection of PII

Organizations should deal with monitoring logs of administrators and operators processing PII. Automated reporting procedures should be defined and implemented as part of the monitoring of information systems processing of PII.

12.4.4 Clock synchronisation

Control 12.4.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.5 Control of operational software

The objective specified in clause 12.5 of ISO/IEC 27002 applies.

12.5.1 Installation of software on operational systems

1 Control 12.5.1 and the associated implementation guidance and other information specified in ISO/IEC 27002
2 apply.

3 **12.6 Technical vulnerability management**

4 The objective specified in clause 12.6 of ISO/IEC 27002 applies.

5 **12.6.1 Management of technical vulnerabilities**

6 Control 12.5.1 and the associated implementation guidance and other information specified in ISO/IEC 27002
7 apply.

8 **12.6.2 Restrictions on software installation**

9 Control 12.6.2 and the associated implementation guidance and other information specified in ISO/IEC 27002
10 apply.

11 **12.7 Information systems audit considerations**

12 The objective specified in clause 12.7 of ISO/IEC 27002 applies.

13 **12.7.1 Information systems audit controls**

14 Control 12.7.1 and the associated implementation guidance and other information specified in ISO/IEC 27002
15 apply.

16 **13 Communications security**

17 **13.1 Network security management**

18 The objective specified in clause 13.1 of ISO/IEC 27002 applies.

19 **13.1.1 Network controls**

20 Control 13.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002
21 apply.

22 **13.1.2 Security of network services**

23 Control 13.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002
24 apply.

25 **13.1.3 Segregation in networks**

26 Control 13.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002
27 apply.

28 **13.2 Information transfer**

29 The objective specified in clause 13.2 of ISO/IEC 27002 applies.

30 **13.2.1 Information transfer policies and procedures**

31 Control 13.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002
32 apply.

33 **13.2.2 Agreements on information transfer**

Control 13.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

13.2.3 Electronic messaging

Control 13.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

13.2.4 Confidentiality or non-disclosure agreements

Control 13.2.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following additional guidance also applies.

Implementation guidance for the protection of PII

When identifying requirements for confidentiality or non-disclosure agreements with respect to the processing of PII, organizations should specify the conditions under which that processing may take place. These conditions should be the subject of an appropriate agreement (e.g., contract, confidentiality or non-disclosure agreement).

14 System acquisition, development and maintenance

14.1 Security requirements of information systems

The objective specified in clause 14.1 of ISO/IEC 27002 applies.

14.1.1 Information security requirements analysis and specification

Control 14.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following additional guidance also applies.

Implementation guidance for the protection of PII

When developing or changing information system related to PII processing, PIA (privacy impact assessment) should be conducted according to ISO/IEC 29134. The result of PIA should be used to develop controls to implement PbD (privacy by design) principle. Organizations should use documented and repeatable process for conducting, reviewing, and approving PIA.

14.1.2 Securing application services on public networks

Control 14.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.1.3 Protecting application services transactions

Control 14.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2 Security in development and support processes

The objective specified in clause 14.2 of ISO/IEC 27002 applies.

14.2.1 Secure development policy

Control 14.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2.2 System change control procedures

Control 14.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2.3 Technical review of applications after operating platform changes

Control 14.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2.4 Restrictions on changes to software packages

Control 14.2.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2.5 Secure system engineering principles

Control 14.2.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2.6 Secure development environment

Control 14.2.6 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2.7 Outsourced development

Control 14.2.7 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2.8 System security testing

Control 14.2.8 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2.9 System acceptance testing

Control 14.2.9 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following additional guidance also applies.

Implementation guidance for the protection of PII

Before an automated system for the processing of PII is released to production, a preliminary check should be carried out to determine special risks to the rights of PII principals, such as the processing of sensitive data (e.g., about race, ethnic origin, political orientation and religion beliefs).

14.3 Test data

The objective specified in clause 14.3 of ISO/IEC 27002 applies.

14.3.1 Protection of test data

Control 14.3.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

15 Supplier relationships

15.1 Information security in supplier relationships

The objective specified in clause 15.1 of ISO/IEC 27002 applies.

15.1.1 Information security policy for supplier relationships

Control 15.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following additional guidance also applies.

Implementation guidance for the protection of PII

Vendor should be shortlisted based on capability to meet data privacy requirements as stipulated by contracts or applicable regulations.

Appropriate Data Privacy clauses should be part of the vendor contract in order to make supplier accountable to protect PII.

Before sub-processing any further or transferring data to a different country, the vendor needs to take prior approval of PII controller organization.

Vendor should not undertake any processing other than that agreed.

Vendor should delete PII as per PII controllers' retention policy.

15.1.2 Addressing security within supplier agreements

Control 15.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

15.1.3 Information and communication technology supply chain

Control 15.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

15.2 Supplier service delivery management

The objective specified in clause 15.2 of ISO/IEC 27002 applies.

15.2.1 Monitoring and review of supplier services

Control 15.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

15.2.2 Managing changes to supplier services

Control 15.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

16 Information security incident management

16.1 Management of information security incidents and improvements

The objective specified in clause 16.1 of ISO/IEC 27002 applies.

16.1.1 Responsibilities and procedures

Control 16.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following additional guidance also applies.

Implementation guidance for the protection of PII

Organizations should develop and implement a privacy incident response plan.

Organizations should provide an organized and effective response to privacy incident in accordance with the privacy incident response plan of an organization.

Organizations should establish procedures to clarify a legal ground, cooperation with external international organizations, and remedy, in case where a cross-border incident occurs.

An organizational Privacy Incident Response Plan includes:

(a) the establishment of a cross-functional Privacy Incident Response Team that develops, implements, tests, executes and reviews the Privacy Incident response Plan (approval of the plan rests with senior management within the organization);

(b) a process to determine whether notice to affected individuals is required and, where appropriate, to provide that notice;

(c) a privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks;

(d) officers or personnel who handle incidents and allow them to make decisions immediately; and

(e) internal procedures to ensure prompt reporting by employees and contractors of any privacy incident to information security officials and the Chief Privacy Officer (CPO), consistent with organizational incident management structures.

Organizations may choose to integrate Privacy Incident Response Plans with Security Incident Response Plans, or keep the plans separate.

16.1.2 Reporting information security events

Control 16.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following additional guidance also applies.

Implementation guidance for the protection of PII

When PII is compromised, the rights and interests of the person cannot be protected without immediate countermeasures.

When a security incident related to PII (e.g. PII leakage) happens, the details of the incident including the organization's proposed response (which may be subject to certain limitations), should be notified to relevant authorities (e.g., data protection authorities, law enforcement) and affected individuals as soon as possible, in accordance with relevant legislation, regulation, applicable PII breach notification requirements or organizational policy.

1 Organization should provide affected PII principals access to appropriate and effective remedies, such as
2 rectification, expungement or restitution if a privacy breach has occurred.

3 **16.1.3 Reporting security weaknesses**

4 Control 16.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002
5 apply. The following additional guidance also applies.

6 **16.1.4 Assessment of and decision on information security events**

7 Control 16.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002
8 apply.

9 **16.1.5 Response to information security incidents**

10 Control 16.1.5 and the associated implementation guidance and other information specified in ISO/IEC 27002
11 apply.

12 **16.1.6 Learning from information security incidents**

13 Control 16.1.6 and the associated implementation guidance and other information specified in ISO/IEC 27002
14 apply.

15 **16.1.7 Collection of evidence**

16 Control 16.1.7 and the associated implementation guidance and other information specified in ISO/IEC 27002
17 apply.

18 **17 Information security aspects of business continuity management**

19 **17.1 Information security continuity**

20 The objective specified in clause 17.1 of ISO/IEC 27002 applies.

21 **17.1.1 Planning information security continuity**

22 Control 17.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002
23 apply.

24 **17.1.2 Implementing information security continuity**

25 Control 17.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002
26 apply.

27 **17.1.3 Verify, review and evaluate information security continuity**

28 Control 17.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002
29 apply.

30 **17.2 Redundancies**

31 The objective specified in clause 17.2 of ISO/IEC 27002 applies.

32 **17.2.1 Availability of information processing facilities**

1 Control 17.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002
2 apply.

3 **18 Compliance**

4 **18.1 Compliance with legal and contractual requirements**

5 The objective specified in clause 18.1 of ISO/IEC 27002 applies.

6 **18.1.1 Identification of applicable legislation and contractual requirements**

7 Control 18.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002
8 apply. The following additional guidance also applies.

9 Implementation guidance for the protection of PII

10 Organization should identify the laws and regulations related to PII protection.

11 Organization should establish the acceptable risk level and implement appropriate measures to treat those
12 risks.

13 Organizations should verify that the processing of PII meet privacy safeguarding requirements by periodically
14 conducting an internal audits or a trusted third-party audit.

15 Organizations should have an internal audit or an independent audit in place, which demonstrates that it
16 meets compliance requirements from relevant privacy law and regulations, privacy policies and procedures
17 specified by an organization.

18 Organizations should develop and implement privacy risk assessments in order to ensure that programme and
19 services related to PII processing comply with privacy safeguarding requirements.

20 **18.1.2 Intellectual property rights**

21 Control 18.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002
22 apply.

23 **18.1.3 Protection of records**

24 Control 18.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002
25 apply.

26 **18.1.4 Privacy and protection of personally identifiable information**

27 Control 18.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002
28 apply.

29 **18.1.5 Regulation of cryptographic controls**

30 Control 18.1.5 and the associated implementation guidance and other information specified in ISO/IEC 27002
31 apply.

32 **18.2 Information security reviews**

33 The objective specified in clause 18.2 of ISO/IEC 27002 applies.

34 **18.2.1 Independent review of information security**

Control 18.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

18.2.2 Compliance with security policies and standards

Control 18.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

18.2.3 Technical compliance review

Control 18.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

19 Extended control set for PII protection

This clause provides definitions for new objectives, new controls and new implementation guidance making up an extended control set to meet the specific requirements for Privacy management related to the processing of PII applying to any processing of PII.

Editor's note: NBs are asked to provide further supporting texts in terms of a comparison of this IS and 29100 in terms of this PII protection specific control and an appropriate reference to the guidance in ISO/IEC 29100:2011.

Editor's note: NBs are asked to provide further supporting texts in terms of making concise the control statements, reducing the number of controls and moving potential controls to the implementation guidelines in clause 19. 19.1 Consent and choice

19.1.1 Consent

Objective: To make PII principals active participants in the decision-making process regarding the processing of their PII except as otherwise limited by legislation and regulation.

Controls

[Organizations should provide the means necessary for PII principals to exercise meaningful, informed consent.] or

[Organizations should:

- (a) ensure that the option of opt-in consent is preferred;
- (b) provide means, where feasible and appropriate, for PII principals to authorize the collection, use, maintenance, transfer, and sharing of PII prior to its collection;
- (c) provide a process to permit a PII principle to modify or withdraw consent for the processing of PII;
- (d) obtain consent, where feasible and appropriate, from PII principals prior to any new uses or disclosure of previously collected PII;
- (e) ensure that PII principals are aware of consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII, where feasible and appropriate;
- (f) determine whether the processing relies on a legal basis other than consent (including legal obligation, protection of life, public service mission, contract or measures taken with the individual and legitimate interest);
- (g) determine the practical means to be implemented to obtain the consent of the PII principals;
- (h) ensure that consent is obtained before any processing begins;

- (i) analyse the cases where the practical means chosen are no longer operational and determine emergency solutions, if necessary, In order to ensure that consent is obtained before any processing begins;.
- (j) ensure that consent is obtained freely;
- (k) confirm that an alternative exists that is not overly restrictive (it must provide a choice) and that no hierarchical relationship exists (for example, between an employee and his/her employer), in order ensure that consent is obtained freely;
- (l) ensure that the consent is obtained in an informed, transparent manner in terms of the purposes of the processing;
- (m) ensure that consent is obtained for a specific purpose;
- (n) set out each party's obligations in an explicit written agreement accepted by both parties, When subcontracting is involved.]

Implementation guidance

Organizations should:

- (a) obtain the opt-in consent of the PII principal for collecting or otherwise processing sensitive PII except where applicable law allows the processing of sensitive PII without the PII principal's consent;
- (b) achieve awareness and consent, for example, through updated public notices;
- (c) obtain consent from a legal agent when obtaining it from a child and store the record of consent from a legal agent;
- (d) provide implied consent which is the least preferred method and should be used in limited circumstances, where PII principals' behaviour or failure to object indicates agreement with the collection or use of PII; and
- (e) allow PII principals to limit the types of PII they provide and subsequent uses of that PII, depending upon the nature of the program or information system.

Other information

This control also recognizes, through the introductory words "where feasible and appropriate", that there are certain cases where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice.

Organization may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that PII principals take affirmative action to allow organizations to collect or use PII.

Organizations may provide, for example, PII principals' itemized choices as to whether they wish to be contacted for any of a variety of purposes. In this situation, organizations construct consent mechanisms to ensure that the organizational operations comply with PII principal choices.

Organizations may provide to the PII principals notice of consent which should be clearly worded and displayed clearly and conspicuously, regardless of means of conveyance.

Consent may be electronic or in hard copy depending on applicable regulatory requirement and practical considerations

19.1.2 Choice

Objective: To present PII principals the choice whether or not to allow the processing of their PII, and explain to PII principals the implications of granting or withholding consent.

Controls

Organizations should:

- (a) provide to the PII principal the choice whether or not to allow the processing of their PII except where the PII principal cannot freely withhold consent or where applicable law specifically allows the processing of PII without the PII principal's consent;
- (b) allow the PII principals to exercise choice which is freely given, specific and on a knowledgeable basis;
- (c) provide appropriate means for PII principals to understand consequences of decisions to approve or decline the authorization of the collection, use, transferring, and retention of PII;
- (d) confirm that the processing is not covered by a legal exception (legal requirement or exclusion noted in the act establishing the processing) that prohibits the PII principal from objecting to the processing;
- (e) determine the practical means that will be implemented to allow PII principals to exercise the right to object. They must be able to exercise this right as quickly as possible, within a period not to exceed time limit specified in the organization's policy, e.g. two months, in a form similar to the form used for the processing (by regular mail and/or by email). In addition, the process must not discourage PII principals from objecting and must not involve any cost to them;
- (f) ensure that the right to object may always be exercised and that the PII collected and processed actually allow the exercise of the right to object;
- (g) analyse the cases where the practical means chosen are no longer operational and identify back-up solutions, if necessary, in order to do the above item;
- (h) ensure that the interested party is able to express his or her choice prior to the final validation of his or her responses;
- (i) confirm that the right to object may be exercised before the PII principals provide final validation of their responses or before the collection is completed, in order to do the above item;
- (j) confirm that requests to exercise the right to object submitted on site provided for verification of the identity of the PII principals submitting requests and the identity of the PII principals they may appoint as their representative;
- (k) confirm that requests to exercise the right to object submitted by regular mail are signed and accompanied by a photocopy of a piece of identification (which should not be retained unless proof must be kept) and that they specify a reply-to address;
- (l) confirm that requests to exercise the right to object submitted by email (using an encrypted channel if transmitted via the Internet) include a digitized piece of identification (which should not be retained unless proof must be kept and, in that case, in black and white, low definition and as an encrypted file);
- (m) ensure that PII principals exercising their right to object provide legitimate grounds and that those grounds are evaluated (except in the case of marketing and processing for the purpose of health research);
- (n) ensure that all recipients of the processing are notified of the objections submitted by the PII principals;
- (o) provide a mechanism allowing PII principals to express their opposition by telephone, in case of processing via telephone;
- (p) Provide a choice of parts of notice instead of to overall notice, when there are multiple parts of privacy notice; and
- (q) allow an objection to be expressed by pressing a telephone button, in order to do the above item.

Consideration should be given to see that the consent is sought at an upstream stage when the choice is maximal. For instance, when certain sensitive information is required to be collected from an employee, and the PII is mandatory, organizations should inform and seek consent from the employee during the time offer is made so that they take informed decision on accepting employment offer.

Implementation guidance

In many situations it would not be necessary or practicable to provide a mechanism to exercise choice when collecting publicly available information. For example, it would not be necessary to provide a mechanism to exercise choice to PII principals when collecting their name and address from a public record or a newspaper.

19.2 Purpose legitimacy and specification

19.2.1 Purpose legitimacy

Objective: To ensure that the purpose of processing of PII complies with applicable laws and relies on a permissible legal ground.

1 Controls

2 Organizations should:

- 3 (a) determine the legal authority (ground) that permits the collection, use, maintenance, and sharing of PII,
- 4 either generally or in support of a specific program or information system;
- 5 (b) incorporate procedures which ensure that: processing of PII is lawfully; and
- 6 (c) delete and dispose of PII whenever the purpose for PII processing has expired, there are no legal
- 7 requirements to keep the PII or whenever it is practical to do so.

8 Implementation guidance

9 Organizations should develop procedures which ensure that processing of PII is not carried out in a way which
10 breaches or potentially breaches any legal obligations, including statutory provisions, common law or
11 contractual terms.

12 If the organization has a works council or trade union, data privacy laws may require consultation with such
13 bodies before establishing the legitimacy of a purpose in case of employees.

14 Before collecting PII in connection with an information system or program, the organization should determine
15 whether the collection of PII is legally authorized. Program officials should consult with the Chief Privacy
16 Officer (CPO) and legal counsel regarding the authority of any program or activity to collect PII. The authority
17 to collect PII should be documented.

18 **19.2.2 Purpose specification**

Objective: To specify the purposes for which PII are collected not later than at the time of PII collection and the subsequent use limited to the fulfilment of original purposes.

19 Controls

20 Organizations should:

- 21 (a) communicate the purpose(s) to the PII principal before the time the information is collected or used for the
- 22 first time for a new purpose, use language for this specification which is both clear and appropriately
- 23 adapted to the circumstances, and give sufficient explanations for the need to process sensitive PII;
- 24 (b) describe the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices;
- 25 (c) communicate the purpose(s) to the PII principal before the time the information is collected or used for the
- 26 first time for a new purpose; and
- 27 (d) use language for this specification which is both clear and appropriately adapted to the circumstances,
- 28 and give sufficient explanations for the need to process sensitive PII.

29 Implementation guidance

30 Often, statutory language expressly authorizes specific collections and uses of PII. When statutory language is
31 written broadly and thus subject to interpretation, organizations should ensure, in consultation with the Chief
32 Privacy Officer (CPO) and legal counsel, that there is a close nexus between the general authorization and
33 any specific collection of PII.

34 Once the specific purposes have been identified, the purposes should be clearly described in the related
35 privacy compliance documentation or forms organizations should use to collect PII. Further, in order to avoid
36 unauthorized collections or uses of PII, personnel who handle PII should receive training on the organizational
37 authorities for collecting.

19.3 Collection limitation

19.3.1 Collection limitation

Objective: To limit the collection of PII to that which is within the bounds of applicable law and strictly necessary for the specified purpose(s).

Controls

Organizations should:

- (a) limit the collection of PII to the minimum elements identified for the purposes described in the notice and for which the PII principal has provided consent;
- (b) not collect sensitive PII unless collection of sensitive PII is legally authorized and an opt-in consent is obtained;
- (c) not collect PII that is not necessary to provide the service or benefit to the PII principal as a mandatory requirement even with consent. Consequence of not providing such non-mandatory information should not be treated as a pre-requisite to providing a service or benefit to PII principal; and
- (d) collect PII not only applicable for information obtained from PII principal with his or her knowledge but also for information that an organization may collect or generate during the course of business, such as IP address of a person browsing a site, work logs from a computer provided to an employee to measure performance, etc.

Implementation guidance

The collection of PII is consistent with a purpose authorized by law or regulation.

Organizations should not collect PII indiscriminately. Both the amount and the type of PII collected should be limited to that which is necessary to fulfill the (legitimate) purpose(s) specified by the PII controller.

Organizations should carefully consider what PII will be needed to realize a particular purpose before proceeding with the collection of PII. Organizations should document the type of PII collected, as well as, their justification for doing so as part of their information-handling policies and practices.

Organizations should confirm that the PII is sufficient, relevant and not excessive with regard to the intended purpose; otherwise, organizations should not collect the PII.

In order to do that, organizations should define the purpose of the processing, identify the PII necessary to achieve that purpose, demonstrate why each category of PII is critical and, last, rule out any PII that does not prevent the purpose from being achieved; if necessary, review the purpose if the PII are necessary for something other than the initial intended purpose.

Organizations should confirm that the PII do not reveal (directly or indirectly) racial or ethnic origin, political, philosophical or religious views, trade union membership, health information, financial information and information about an individual that reveals unique identity or information on an PII principal's sex life and do not collect them if they do, except under exceptional circumstances (for example, with consent, in the public interest) and except when legally required or permitted.

Organizations should confirm that the PII do not relate to offenses, criminal convictions or security measures and do not collect them if they do, except under exceptional circumstances (for example, in dealing with the courts or court officers).

Organizations should prevent the collection of additional PII.

In order to do that, only fields that relate to the PII defined should be created and may be entered in a PII base. No additional field may be added (do not include a "free text field"). Check regularly to ensure that no additional PII is collected in relation to the PII initially identified.

19.4 Data minimization

19.4.1 Minimization

Objective: To minimize the PII which is processed and the number of privacy stakeholders and people to whom PII is disclosed or who have access to it.

Controls

Organizations should:

- (a) identify the minimum PII elements (e.g., name, address, date of birth) that are relevant and necessary to accomplish the legally authorized purpose of collection;
- (b) minimize the number of privacy stakeholders and people to whom PII is disclosed or who have access to it;
- (c) ensure adoption of a "need-to-know" principle, i.e. one should be given access only to the PII which is necessary for the conduct of his/her official duties in the framework of the legitimate purpose of the PII processing;
- (d) use or offer as default options, wherever possible, that interactions and transactions which do not involve the identification of PII principals;
- (e) reduce the observability of their behaviour and limit the linkability of the PII collected;
- (f) conduct an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings periodically to ensure that only PII identified in the notice is collected, and that the PII continues to be necessary to accomplish the legally authorized purpose;
- (g) restrict the transmission of electronic documents containing PII to the PII principals who need them in connection with their work;
- (h) use a secure deletion tool for electronic documents and a degaussing device for storage units that use magnetic technologies, in order to do that above;
- (i) determine what must be anonymized based on the context, the form in which the PII are stored (including database fields or excerpts from texts) and the risks identified;
- (j) permanently anonymize the data that require such anonymization based on the form of the data to be anonymized (including databases and textual records) and the risks identified;
- (k) choose tools (including partial deletion, hashing, key hashing and index) that most closely meet the functional needs, If that data cannot be anonymized permanently; and
- (l) perform irreversible anonymization of PII where possible., In case of databases.

Notes :

- "True" anonymization necessarily involves an (irreversible) loss of information. In some cases, simply deleting or blacking-out part of the data may achieve the desired objective.
- In this pseudonymization process, data lose their identifying characteristics (in direct fashion). The data remain linked to the same person across multiple data records and information systems without revealing the PII principal's identity. It may be performed with or without the possibility of re-identifying names or identities (reversible or irreversible pseudonymization).
- It is still possible to correlate anonymized PII, so a PII principal may be re-identified based on partial information when PII is anonymized but not deleted. Original data can be linked to anonymized data when secrecy is compromised and the original data is not sufficiently complex.
- As a general rule, in order to conclude that an "anonymization process" complies with the law, true anonymization must be carried out by deleting data or performing a "pseudonymization," together with strong organizational and technical guarantees, particularly by using keyed-hash functions.
- When a PII is collected or used for a purpose, the extent of detail must be minimal to only serve the intended purpose but not reveal excessive information about the principal. E.g., if it is required to know which geographical area a respondent on traffic related survey comes from, one need not seek the entire address and instead should only collect nearest landmark. Likewise if an employer wishes to provide date of birth to other employees for the purpose of birthday wishes, it is enough to disclose day and month with consent, rather than entire information including year to prevent age from being revealed..

1 Implementation guidance

2 The minimum set of PII elements required to support a specific organization business process may be a
3 subset of the PII the organization is authorized to collect.

4 The PII should be classified into mandatory PII and optional PII for collection. Organization should collect only
5 mandatory PII required for providing service and obtain opt-in consent from PII principals when collecting
6 optional PII. Organization should not decline providing service when PII principals decline giving optional PII.

7 Program officials should consult with the Chief Privacy Officer (CPO) and legal counsel to identify the
8 minimum PII elements required by the information system or activity to accomplish the legally authorized
9 purpose.

10 Other information for the protection of PII

11 Organizations can further reduce their privacy and security risks by also reducing their inventory of PII, where
12 appropriate. Organizations are required to conduct both an initial review and subsequent reviews of their
13 holdings of all PII and ensure, to the maximum extent practicable, that such holdings are accurate, relevant,
14 timely, and complete.

15 Organizations are also directed to reduce their holdings to the minimum necessary for the proper performance
16 of a documented organizational business purpose. Organizations are required to develop and publicize, either
17 through a notice, a schedule for periodic reviews of their holdings to supplement the initial review.

18 By performing periodic evaluations, organizations reduce risk, ensure that they are collecting only the data
19 specified in the notice, and ensure that the data collected is still relevant and necessary.

20 **19.5 Use, retention and disclosure limitation**

21 **19.5.1 Use, retention and disclosure limitation**

Objective: To limit the use, retention, disposal and disclosure of PII for specific, explicit and legitimate purposes.

22 Controls

23 Organizations should:

- 24 (a) limit the use, retention, disposal, and disclosure (including transfer) of PII to that which is necessary in
25 order to fulfil specific, explicit and legitimate purposes;
- 26 (b) retain PII for authorized time period to fulfil the purpose(s) identified in the notice or as required by law
27 and organizations and delete the PII promptly when the retention period expires;
- 28 (c) dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage in a manner
29 that prevents loss, theft, misuse, or unauthorized access;
- 30 (d) lock (i.e. archiving, securing and exempting the PII from further processing) any PII when and for as long
31 as the stated purposes have expired, but where retention is required by applicable laws.
- 32 (e) use appropriate techniques or methods to ensure secure deletion or destruction of PII (including originals,
33 copies, and archived records);
- 34 (f) configure its information systems to record the date PII is collected, created, or updated and when PII is
35 to be deleted or archived under an approved record retention schedule;
- 36 (g) define PII retention periods that are time-limited and appropriate to the purpose of the processing;
- 37 (h) confirm that the processing can detect the expiration of the retention period; . determine and
38 communicate to the PII principal prior to availing a benefit or service to the extent possible the purpose of
39 processing PII that this absolutely necessary since seeking consent subsequently may be considered
40 unfair, and may be too late for principal to opt-out;
- 41 (i) use PII only for the purpose agreed with or stated to data principal during collection, and obtain consent in
42 advance to commencement of processing in case of any new purpose of processing consent.
- 43 (j) not disclose PII to any recipients within the organization or outside without knowledge or consent of data
44 principal unless legally permitted under exceptions;

- (k) ensure the secure deletion of PII when the retention period expires;
- (l) If the risks are low, PII may simply be deleted; if the risks are high, secure deletion tools should be used; and
- (m) develop an automated functionality that erases PII when their retention period expires.

Implementation guidance

Organization should:

- (a) reduce the types of PII held (e.g., delete social security numbers if their use is no longer needed), shortens the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time;
- (b) provide notice to inform the public of any changes in holdings of PII collected during the security monitoring process;
- (c) ensure an adequate level of protection where PII is transferred or processed across the border;
- (d) develop and publicizes a schedule for periodic reviews of their holdings of PII collected during the security monitoring process to supplement the initial review;
- (e) retain PII collected for monitoring as long as it is necessary to fulfil the purpose(s) identified in the notice or as required by law;
- (f) dispose of PII collected for monitoring when it is no longer necessary to retain it;
- (g) retain PII collected for meeting data retention requirements for only as long as is necessary to fulfil the purpose(s) identified in the notice or as required by legal requirement; and
- (h) appropriately dispose of PII collected for meeting data retention requirements when it is no longer necessary to retain it.

19.6 Accuracy and quality

19.6.1 Data quality

Objective: To ensure that the PII processed is accurate, complete, up-to-date, adequate and relevant for the purpose of use.

Controls

Organizations should:

- (a) confirm to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of PII;
- (b) ensure the reliability of PII collected from a source other than from the PII principal before it is processed;
- (c) verify, through appropriate means, the validity and correctness of the claims made by the PII principal prior to making any changes to the PII, where it is appropriate to do so;
- (d) establish PII collection procedures to help ensure accuracy and quality;
- (e) collects PII directly from the PII principal to the greatest extent practicable;
- (f) check for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems periodically; and
- (g) issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

Implementation guidance

Organizations should take reasonable steps to confirm the accuracy of PII. Such steps may include, for example, editing and validating addresses as they are collected or entered into information systems using automated address verification look-up application programming interfaces (APIs).

When PII is of a sufficiently sensitive nature (e.g., when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit), organizations incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be updated.

Other information

The types of measures taken to protect data quality may be based on the nature and context of the PII, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of PII that is used to make determinations about the rights, benefits, or privileges of PII principals under federal programs may be more comprehensive than those used to validate less sensitive PII. Additional steps may be necessary to validate PII that is obtained from sources other than PII principals or the authorized representatives of PII principals.

To minimize the scope for data inaccuracy, to the extent possible, PII should be provided into information systems directly by the PII principal without the need for another person to manually log into a system. But in the event manual logging is unavoidable, organization may consider providing an update to the PII principal to provide an opportunity to check and confirm if there is any error in the PII logged into system. This helps in timely correction before any consequential damage results from processing inaccurate data..

19.6.2 Data integrity

Objective: To establish control mechanisms to periodically check the accuracy and quality of collected and stored PII.

Controls

Organizations document processes to ensure the integrity of PII through existing security controls.

19.7 Openness, transparency and notice

19.7.1 Privacy notice

Objective: To include in notices the fact that PII is being processed.

Controls

Organizations should:

- (a) provide PII principals appropriate notice of the purposes of the PII collection or technology use and a means for PII principals to consent to the activity in order to obtain consent;
- (b) include in notices the fact that PII is being processed, the purpose for which this is done, the types of privacy stakeholders to whom the PII might be disclosed, and the identity of the PII controller including information on how to contact the PII controller;
- (c) provide effective notice to the public and to PII principals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII; (ii) authority for collecting PII; (iii) the choices, if any, PII principals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;
- (d) give notice to the PII principals when major changes in the PII handling procedures occur;
- (e) provide the tailored public notice and consent mechanisms to meet operational needs;
- (f) revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change;
- (g) confirm that the processing is not covered by an exception and is not subject to the specific conditions set forth by law (e.g. electronic communications networks user, statistics, anonymization, national security, defense, public safety, enforcement of criminal sentences, security measures, prevention, research, findings and prosecution of criminal offenses);

- (h) determine the practical means that will be implemented to inform the PII principals;
 - (i) ensure that the notification is complete, clear and appropriate to the target audience based on the nature of the PII and the practical means chosen;
 - (j) present the information in clear language that can be understood by a person who is not familiar with information technologies or the Internet;
 - (k) ensure that the notification is provided by the time the PII is collected;
 - (l) ensure that the PII cannot be collected without providing this information;
 - (m) determine alternative solutions in the event that the practical means are no longer operational;
 - (n) provide a means by which to show that notification was provided, if possible; and
 - (o) post this information on a sign that all employees must see or require that a notice or document be signed or initialled.
- Notice should be conspicuous and provided to the extent possible without the need for principal to request, for example in the company website or physically displayed at the points of collection.

19.7.2 Openness and transparency

Objective: To provide PII principals with clear and easily accessible information about the PII controller's policies, procedures and practices with respect to the handling of PII.

Controls

Organizations should:

- (a) provide to PII principals a clear and easily accessible means to give information about the PII controller's policies, procedures and practices with respect to the handling of PII; and
- (b) disclose the choices and means offered by the PII controller to PII principals for the purposes of limiting the processing of, and for accessing, correcting and removing their information.

Implementation guidance

Organizations should describe:

- (a) the PII the organization collects and the purpose(s) for which it collects that information;
- (b) how the organization uses PII internally;
- (c) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing,
- (d) whether PII principals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent;
- (e) how long the PII will be retained;
- (f) whether the organization on-sells or forwards data for processing by data analytics organizations and the details applicable to PII risks;
- (g) how PII principals may obtain access to PII for the purpose of having it amended or corrected, where appropriate; and
- (h) how the PII will be protected.

19.7.3 Dissemination of privacy program information

Objective: To provide PII principals with access to information about its privacy activities.

Controls

Organizations should:

- (a) ensure that the public has access to information about its privacy activities and is able to communicate with its Chief Privacy Officer (CPO); and
- (b) ensure that its privacy practices are publicly available through organizational websites or otherwise.

Implementation guidance

Organizations should employ different mechanisms for informing the public about their privacy practices including, but not limited to, Privacy Impact Assessments (PIAs), privacy reports, publicly available web pages, email distributions, blogs, and periodic publications (e.g., quarterly newsletters). Organizations also employ publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

19.8 PII principal participation and access

19.8.1 PII principal access

Objective: To give PII principals the ability to access and review their PII.

Controls

Organizations should:

- (a) provide PII principals the ability to have access to their PII (PII) maintained in its system(s) in order to determine whether to have the PII corrected or amended, as appropriate;
- (b) allow PII principals to challenge the accuracy and completeness of the PII and have it amended, corrected or removed as appropriate and possible in the specific context;
- (c) establish procedures to enable PII principals to exercise these rights in a simple, fast and efficient way, which does not entail undue delay or cost, e.g., within a period not to exceed time limit specified in the organization's policy, in accordance with national legislation, in a form similar to the form used for the processing (by regular mail and/or by email);
- (d) publish rules and regulations governing how PII principals may request access to records maintained in its system;
- (e) confirm that the processing is not subject to an exception (such as PII processed for statistical or research purposes when there is no risk of a privacy breach and the PII are retained only as long as necessary for these purposes or for reasons of national security, defense or public safety);
- (f) determine the practical means that will be implemented to allow the exercise of the direct access right. Individuals must be able to exercise this right as quickly as possible, within a period not to exceed two months, in a form similar to the form used for the processing (by regular mail and/or by email). In addition, the process must not discourage the PII principals and they must not incur expenses that exceed copying costs;
- (g) establish a process to inform PII principals submitting requests about the status of their request and the necessary processing (for example, by regular mail or email, noting that the request has been received and the date by which they can expect to receive a response). In the case of stored archives, there may be some leeway regarding the response date if the PII controller informs the PII principal submitting the request of the problems and has provided a reasonable response time;
- (h) ensure that the right of access can always be exercised;
- (i) analyze the cases in which the practical means chosen are no longer operational and identify back-up solutions, if necessary;
- (j) confirm that requests to exercise the right of access submitted on site provide the identity of the PII principals submitting requests and the identity of the PII principals they may appoint as their representative;

- (k) confirm that requests to exercise the right of access submitted by regular mail are signed and accompanied by a photocopy of a piece of identification (which should not be retained unless proof must be kept) and that they specify a reply-to address;
- (l) confirm that requests to exercise the right of access submitted by email (using an encrypted channel if transmitted via the Internet) are accompanied by a digitized piece of identification (which should not be retained unless proof must be kept and, in that case, in black and white, low definition and as an encrypted file);
- (m) ensure that all information that PII principals may request can be provided while still protecting the PII of third parties; and
- (n) communicate in privacy notice if it wishes to levy a small fee for a principal to access personal data, as permitted by law in case of some countries.

Implementation guidance

Access affords PII principals the ability to review PII about them held within organizational systems of records. Access includes timely, simplified, and inexpensive access to data. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors.

Other information

The pre-condition for giving PII principals the ability to access and review their PII is that their identity is first authenticated with an appropriate level of assurance and such access is not prohibited by applicable law.

19.8.2 Redress and participation

Objective: To provide any amendment, correction or removal to PII processors and third parties to whom personal data had been disclosed, where they are known

Controls

Organizations should:

- (a) provide a process and a means for PII principals to have inaccurate PII maintained by the organization corrected or amended, as appropriate;
- (b) establish a process and a means for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information sharing partners and, where feasible and appropriate;
- (c) confirm that the processing is not covered by an exception (national security, defense or public safety);
- (d) provide PII principals with being able to exercise this right as quickly as possible, within a period not to exceed time limit specified in the organization's policy, in accordance with national legislation, e.g. two months, in a form similar to the form used for the processing (by regular mail and/or by email). In addition, the process must not discourage the PII principals and must not involve any cost to them;
- (e) ensure that the right to correct may always be exercised;
- (f) analyze the cases in which the practical means chosen are no longer operational and identify back-up solutions, if necessary;
- (g) ensure that the identity of PII principals submitting requests will be verified;
- (h) should confirm that requests to exercise the right to correct submitted via postal mail are signed and accompanied by a photocopy of a piece of identification (which shall not be retained unless proof must be kept), and that requests submitted via email (using an encrypted channel if transmitted via the Internet) are accompanied by a digitized piece of identification (which should not be retained unless proof must be kept and, in that case, in black and white, low definition and as an encrypted file) and that requests specify a reply-to address and confirm the identity of PII principals submitting requests on site and of PII principals they may appoint as their representatives or of heirs of a deceased PII principal;
- (i) ensure the accuracy of the corrections requested;
- (j) ensure that the PII principals submitting requests receive confirmation;

- (k) ensure that the third parties to whom the PII may have been sent are informed of the corrections made;
- (l) provide a way for PII principals to access the areas of interest in their profile and a way to modify them. The PII principal's identity may be authenticated based on the information used to access his or her account or on the cookie (or equivalent) on his or her computer, in case of on-line advertising;
- (m) In case of partitioning PII, organizations should identify the PII useful only to each business process;
- (n) provide PII principals with access only to the PII they need. For example, do not provide the statistics department with access to first and last names;
- (o) separate the PII useful to each process in logical fashion;
- (p) manage the different access rights according to the business processes (including payroll management, vacation request management and career advancement) and establish a dedicated IT environment for systems that process the most sensitive PII; and
- (q) regularly confirm that PII are partitioned effectively and that recipients and interconnections have not been added.

19.8.3 Complaint management

Objective: To set up efficient internal complaint handling and redress procedures for use by PII principals.

Controls

Organizations should:

- (a) implement a complaint management process and maintain a contact for receiving and responding to complaints, concerns, or questions from PII principals about the organizational privacy practices; and
- (b) follow the pre-defined breach handling process which will include risk assessment to determine the impact based on which regulations in certain countries may require notification to principals and in some cases to information commissioners in the event of a PII breach, which could include violation of any data privacy principles apart from compromise on security.

Implementation guidance

Organizations should provide complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints (including contact information for the Chief Privacy Officer (CPO) or other official designated to receive complaints), and are easy to use.

Organizational complaint management processes include tracking mechanisms to ensure that all complaints received are reviewed and appropriately addressed in a timely manner.

Other information

Complaints, concerns, and questions from PII principals can serve as a valuable source of external input that ultimately improves operational models, uses of technology, data collection practices, and privacy and security safeguards.

19.9 Accountability

Editor's note: NBs are asked to provide further supporting texts in terms of behaving as a control but as a requirement to the management system instead in clause 19.9.1 and 19.9.2.

19.9.1 Governance

Objective: To assign to a specified PII principal within the organization the task of implementing the privacy-related policies, procedures and practices.

Controls

Organizations should:

- (a) appoint a Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems;
- (b) provide a process to monitor privacy laws and policy for changes that affect the privacy program;
- (c) allocate sufficient budget and human resource to implement and operate the organization-wide privacy program;
- (d) develop a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;
- (e) develop, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII;
- (f) update privacy plan, policies, and procedures periodically; and
- (g) monitor periodically the performance of organization on data privacy and senior management representative or member of the board, should govern it with visibility into aspects such as quantitative metrics, risks and breaches. While such review may be need based, it must be also periodic without the need for any triggers.

19.9.2 Privacy risk assessment

Objective: To establish a privacy risk assessment process.

Controls

Organizations should establish a privacy risk assessment process that assesses privacy risk to PII principals resulting from the collection, sharing, storing, transmitting, and use of PII.

The methodology of privacy risks assessment in ISO/IEC 29134 applies.

Implementation guidance

Organizations should consider threats to PII when performing privacy risk assessment.

19.9.3 Privacy requirement for contractors and service providers

Objective: To ensure that the third party recipient will be bound to provide an equivalent level of privacy protection through contractual or other means such as mandatory internal policies.

Controls

Organizations should:

- (a) document security and privacy requirements that contractors implement in the service level agreement;
- (b) monitor and audit the implementation of those requirements by contractors;
- (c) provide a means to check for an adequate level of protection of contractors in accordance with organization's privacy policy;
- (d) establish privacy roles and responsibilities for contractors and service providers; and
- (e) include privacy requirements in contracts and other acquisition-related documents.

Implementation guidance

1 Organizations should provide a means to monitor and audit privacy controls and privacy policy of contractors
2 periodically to ensure effective implementation of requirements specified in the service level agreement.

3 Other information

4 Contractors and service providers include, but are not limited to, service bureaus, information providers,
5 information processors, and other organizations providing information system development, information
6 technology services, and other outsourced applications. Organizations consult with legal counsel, the Chief
7 Privacy Officer (CPO), and contracting officers about applicable laws, directives, policies, or regulations that
8 may impact implementation of this control.

9 **19.9.4 Privacy monitoring and auditing**

Objective: To monitor and audit privacy controls and internal privacy policy.

10 Controls

11 Organizations should:

- 12 (a) provide a means to monitor and audit privacy controls and internal privacy policy periodically to ensure
13 effective implementation;
- 14 (b) document and communicate as appropriate all privacy-related policies, procedures and practices; and
- 15 (c) perform audits by qualified individuals independent of responsibility to ensure PII protection in the
16 organization.

17 **19.9.5 Privacy awareness and training**

Objective: To provide suitable training for the personnel of the PII controller who will have access to PII.

18 Controls

19 Organizations should:

- 20 (a) develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that
21 personnel understand privacy responsibilities and procedures;
- 22 (b) create mechanisms to keep the personnel within Data Privacy function updated on developments in the
23 regulatory, contractual and technological environment that could impact privacy compliance of the
24 organization;
- 25 (c) administer basic privacy training periodically and targeted, role-based privacy training for personnel
26 having responsibility for PII or for activities that involve PII periodically; and
- 27 (d) ensure that personnel certify (manually or electronically) acceptance of responsibilities for privacy
28 requirements periodically..

29 **19.9.6 Privacy reporting**

Objective: To develop, disseminate, and update privacy reports.

30 Controls

31 Organizations should develop, disseminate, and update reports to demonstrate accountability with specific
32 statutory and regulatory privacy program mandates, and to senior management and other personnel with
33 responsibility for monitoring privacy program progress and compliance;

Other information

Through external and internal privacy reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting also helps organizations determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, identify vulnerabilities and gaps in policy and implementation, and identify success models.

19.9.8 Continuous Improvement of PII management systems, corrective and preventive actions (using approaches such as PDCA cycle)

Editor's note: NBs are asked to provide a supporting text regarding this clause.

19.10 Information security

Control and the associated implementation guidance and other information specified from Clause 5 to Clause 18 in this International Standard apply.

Due diligence should be taken when designing and implementing security controls so that they do not impinge on privacy.

Security requirements are sometimes prescribed by certain data privacy laws in which case the same must be communicated to the data security function for implementation.

19.11 Privacy compliance

19.11.1 compliance

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to privacy and of any privacy requirements.

Control

Organizations should:

- (a) regularly inspect PII processing operations to ensure that they comply with law as well as the effectiveness and appropriateness of planned measures;
- (b) perform checks of the most sensitive processing operations and of operations which are the subject of PII breaches or complaints;
- (c) perform random checks so that all operations are inspected on a regular basis. Have a third party perform occasional audits;
- (d) have a third party to perform occasional audits, particularly of the most sensitive processing operations, etc;
- (e) set data protection objectives and define indicators for determining whether these objectives are met;
- (f) have a map of PII processing operations and the associated risks.
- (g) give prior notification for all processing operations prior to their implementation, etc.;
- (h) regularly assess data protection; and
- (i) present the controller with an annual map of risks to all processing operations, an annual assessment of compliance with the data protection policy, a progress report on planned actions, etc.

19.11.2 Cross border data transfer restrictions in certain jurisdictions

Editor's note: NBs are asked to provide a supporting text regarding this clause.

Annex A (informative)

The relationship of the Clauses of this International Standard with the 29100 privacy principles

This Annex describes the relationship of the clauses of this International Standard with the 29100 privacy principles.

29151 clause# (Those in below are just copied from 1stWD 29151, but those should be copied from the latest 27002 in the later.)	29100 privacy principles																		
	1. Consent and choice		2. Purpose legitimacy and specification		3. Collection limitation	4. Data minimization	5. Use, retention and disclosure limitation			6. Accuracy and quality		7. Openness, transparency and notice			8. Individual participation and access		9. Accountability	10. Information security	11. Privacy compliance
	Consent	Choice	Purpose legitimacy	Purpose specification	Collection limitation	Data minimization	Use limitation	Retention limitation	Disclosure limitation	Accuracy	Quality	Openness	Transparency	Notice	Individual participation	Individual access	Accountability	Information security	Privacy compliance
5. Information security policies																		X	
6. Organization of information security																		X	
7. Human resource security																		X	
8. Asset management																		X	
9. Access control																		X	
10. Cryptography																		X	
11. Physical and environmental security																		X	
12. Operations security																		X	
13. Communications security																		X	
14. System acquisition, development and maintenance																		X	
15. Supplier relationships																		X	
16. Information security incident management																		X	
17. Information security aspects of business continuity management																		X	
18. Compliance																			X

Characters of X are to be marked as like shown in the right side columns

Figure A-1- The relationship of the Clauses of this International Standard with the 29100 privacy principles

Editor's note: NBs are asked to providing the supporting text regarding Figure A-1.

Annex B (informative)

List of specific controls/guidances in DIS 27018 (SC27 N13507) and/or in 2nd WD 29151 (SC27 N13385)

This Annex describes the list of specific controls/guidance in DIS 27018 (SC27 N13507) and/or in 2nd WD 29151 (SC27 N13385).

clause	subclause	specific control/guidance in DIS 27018	specific control/guidance in WD 29151
5 Information security policies	5.1.1 Policies for information security	[guidance] The information security policies should be augmented by a privacy policy containing a statement concerning support for and commitment to managing compliance with applicable PII protection legislation and the contractual terms agreed between the cloud PII processor and its clients (cloud service customers). Contractual agreements should clearly allocate responsibilities between the cloud PII processor, its subcontractors and the cloud service customer, taking into account the type of cloud service in question (e.g. a service provided at the IaaS, the PaaS, or the SaaS layer of the cloud computing reference architecture). For example, the allocation of responsibility for application layer controls may differ depending on whether the cloud PII processor is providing a SaaS service or rather is providing a PaaS or IaaS service upon which the cloud service customer can build or layer its own proprietary applications.	[guidance] The security policy should : be appropriate to the purpose of the organization; provide the framework for setting objectives; define rules for making decisions in questions of privacy; define rules on privacy risk acceptance include a commitment to satisfy applicable privacy safeguarding requirements; include a commitment to continual improvement; be communicated within the organization; and be available to interested parties, as appropriate.
6 Organization of information security	6.1.1 Information security roles and responsibilities	[guidance] The cloud PII processor should designate a point of contact for use by the cloud service customer regarding	[guidance] Areas for which individuals are responsible should be stated. In particular the following should take place:: a) establishment of role for cooperation with information security functions by designating officers and/or personnel who are responsible for monitoring and managing compliance of policies and regulations related with personally identifiable information protection in personally identifiable information handling departments. b) An individual should be appointed to take overall responsibility for protection and management of personally identifiable information. The organization should designate someone for being in charge of the privacy and protection of PII issues.
7 Human resources security	7.2.2 Information security awareness, education and training	[guidance] Measures should be put in place to make relevant staff aware of the possible consequences on the cloud PII processor (for example, legal consequences, loss of business and brand or reputational damage), on the staff member (for example disciplinary consequences) and on the PII principal (for example physical, material and emotional consequences) of breaching privacy or security rules and procedures, especially those addressing the handling of PII.	(none)

8 Asset management	8.1.1 Inventory of assets	(none)	<p>[guidance] The personally identifiable information inventory enables organizations to implement effective, administrative, technical, and physical security policies and procedures to protect personally identifiable information consistently, and to treat risks of personally identifiable information exposure.</p> <p>When developing and maintaining the inventory of PII, organizations may extract the following information elements from Privacy Impact Assessments (PIAs) of information systems containing personally identifiable information: (i) the name and acronym for each system identified; (ii) the types of personally identifiable information contained in that system; (iii) classification or level of sensitivity of all types of personally identifiable information, as combined in that information system; and (iv) level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected PII principals, as well as the financial or reputational risks to organizations, if personally identifiable information is exposed. Organizations should take due care in updating the inventories by identifying linkable data that could create PII.</p>
	8.2.1 Classification of information	(none)	[guidance] Organizations should classify PII into sensitive PII and non-sensitive PII in accordance with value, legal requirement, criticality, and severity which are defined in the privacy policy of an organization.
9 Access control	9.2 User access management	<p>[guidance] In the context of the layers of the cloud computing reference architecture, the cloud service customer may be responsible for some or all aspects of access management for cloud service users under its control. Where appropriate, the cloud PII processor should enable the cloud service customer to manage access by cloud service users under the cloud service customer's control, such as by providing administrative rights to manage or terminate access.</p>	(none)
	9.2.1 User registration and de- registration	[guidance] Procedures for user registration and de-registration should address a compromise of user access control such as the corruption or compromise of passwords or other user registration data, e.g. as a result of inadvertent disclosure.	[guidance] Checking that access rights to the PII processing system are granted to the minimum number of entities needed for processing PII.
	9.4.1 Information access restriction	(none)	<p>[guidance] Before permitting the use of query languages in the context of processing of PIIs, it should be checked if this is compatible with the protection requirements of the information. When it is principally compliant, the following provision should be observed:</p> <p>The system should have a technical mean which limits the use of query language to the agreed extent.</p> <p>This can for example mean that access control restrictions limit its use to a few predefined sensitive fields or the records. Programming techniques must be used to prevent bypassing of the filter.</p>
10 Cryptography		(none)	(none)

11 Operations security	11.2.7 Secure disposal or re-use of equipment	[guidance] For the purposes of secure disposal or re-use, equipment containing storage media that may possibly contain PII should be treated as though it does.	(none)
12 Operations security	12.1.4 Separation of development, testing and operation environments	[guidance] 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.	(none)
	12.3.1 Information backup	[guidance] Information processing systems based on the cloud computing model introduce additional or alternative mechanisms to 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 purposes of backup and/or recovery.	(none)
	12.4.1 Event logging	[guidance] A process should be put in place to verify the event log with a specified, documented periodicity, to identify irregularities and propose remediation efforts. Where possible, the event log 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 at different layers of the cloud computing reference architecture, there may be varied or shared roles in implementing this guidance. The cloud PII processor should define procedures regarding if, when and how log information can be made available to or usable by the cloud service customer. These procedures should be made available to the cloud service customer.	(none)
	12.4.2 Protection of log information	[guidance] Log information recorded for purposes such as security monitoring and operational diagnostics may contain PII. Measures, such as controlling access (see 9.2.3), should be put in place designed to ensure that logged information is only used for its intended purposes.	(none)
	12.4.3 Administration and operator logs	(none)	[guidance] Automated reporting procedures should be defined and implemented as part of the monitoring activities in the processing of PII.
13 Communications security	13.2.1 Information transfer policies and procedures	[guidance] 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, the number of physical media, and the types of PII they contain.	(none)

	13.2.4 Confidentiality or non- disclosure agreements	(none)	[guidance] When organizations are identifying requirements for confidentiality or non-disclosure agreements, the following should be considered: the purpose of PII for which the PII is to be processed; and the use of subcontract (i.e. confidentiality agreement with PII processor).
14 Communica- tions security	14.2.9 System acceptance testing	(none)	[guidance] Before an automated system for the processing of PII is released to production, a preliminary check should be carried out to determine special risks to the rights of PII principals, such as the processing of sensitive data (e.g., about race, ethnic origin, political orientation and religion beliefs).
16 Information security incident management	16.1 Management of information security incidents and improvements	[guidance] In the context of the whole cloud computing reference architecture, there may be shared roles in the management of information security incidents and making improvements. There may be a need for the cloud PII processor to cooperate with the cloud service customer in implementing the controls in this subclause.	(none)
	16.1.1 Responsibilitie s and procedures	[guidance] An information security incident should trigger a review by the cloud PII processor, as part of its information security incident management process, to determine if a data breach involving PII has taken place (see A.9.1). An information security event should 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 cloud PII processor'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.	[guidance] An organizational Privacy Incident Response Plan includes: (i) the establishment of a cross-functional Privacy Incident Response Team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan; (ii) a process to determine whether notice to affected individuals is required and, where appropriate, to provide that notice; (iii) a privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks; and (iv) internal procedures to ensure prompt reporting by employees and contractors of any privacy incident to information security officials and the Chief Privacy Officer (CPO), consistent with organizational incident management structures. Organizations may choose to integrate Privacy Incident Response Plans with Security Incident Response Plans, or keep the plans separate.
	16.1.2 Reporting information security events	(none)	[guidance] When PII is compromised, the rights and interests of the person cannot be protected without immediate countermeasures. Organization should appoint the officers or personnel who handle incidents and allow them to make decisions immediately. When a security incident related to PII (e.g. PII leakage) happens, the details and handling procedures of the incident should be notified to the affected data subjects as well as data protection authorities as soon as possible, where appropriate according to organizational policy. Organization should provide affected PII principals access to appropriate and effective sanctions and/or remedies, such as rectification, expungement or restitution if a privacy breach has occurred. In addition, organizations may provide procedures for compensation for situations where it will be difficult or impossible to bring the natural person's privacy status back to an original position.

	16.1.3 Reporting security weaknesses	(none)	[guidance] When a security weakness related to PII (e.g. PII leakage) happens, the details and handling procedures of the incident should be notified to the affected data subjects as well as data protection.
17 Information security aspects of business continuity management		(none)	(none)
18 Compliance	18.2.1 Independent review of information security	[guidance] In cases where individual cloud service customer audits are impractical or may increase risks to security (see 0.1), the cloud PII processor should make available to prospective cloud service customers, prior to entering into a contract, independent evidence that information security is implemented and operated in accordance with the cloud PII processor's policies and procedures. A relevant independent audit as selected by the cloud PII processor should normally be an acceptable method for fulfilling the cloud service customer's interest in reviewing the cloud PII processor's processing operations, provided sufficient transparency is provided.	(none)
A.1 Consent and choice	A.1.1 Obligation to co-operate regarding PII principals' rights	The cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct, and/or erase PII pertaining to them.	(19.1 Consent and choice)
A.2 Purpose legitimacy and specification	A.2.1 Cloud PII processor's purpose	PII to be processed under a data processing contract should not be processed for any purpose independent of the instructions of the cloud service customer.	(19.2 Purpose legitimacy and specification)
	A.2.2 Cloud PII processor's commercial use	PII processed under a data processing contract should not be used by the cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.	
A.3 Collection limitation	A.3.1	(none)	(19.3 Collection limitation)
A.4 Data minimization	A.4.1 Secure erasure of temporary files	Temporary files and documents should be erased or destroyed within a specified, documented period.	(19.4 Data minimization)
A.5 Use, retention and disclosure limitation	A.5.1 PII disclosure notification	The contract between the cloud PII processor and the cloud service customer should require the cloud PII processor to notify the cloud service customer of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.	(19.5 Use, retention and disclosure limitation)
	A.5.2 Recording of PII disclosures	Disclosures of PII should be recorded, including what PII has been disclosed, to whom, at what time.	

A.6 Accuracy and quality		(none)	(19.6 Accuracy and quality)
A.7 Openness, transparency and notices	A.7.1 Disclosure of sub-contracted PII processing	The use of sub-contractors by the PII processor to process PII should be disclosed before their use to the relevant cloud service customers.	(19.7 Openness, transparency and notices)
A.8 Individual participation and access		(none)	(19.8 Individual participation and access)
A.9 Account-ability	A.9.1 Notification of a data breach involving PII	The cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII, or unauthorized access to processing equipment or facilities resulting in loss, disclosure, or alteration of PII.	(19.9 Account-ability)
	A.9.2 Retention period for administrative security policies and guidelines	Records of security policies and operating procedures should be retained for a specified, documented period upon replacement (including updating).	
	A.9.3 PII return, transfer and disposal	The cloud PII processor should have a policy in respect of the return, transfer, and/or destruction of PII and should make this policy available to the cloud service customer.	
A.10 Information security	A.10.1 Confidentiality or non-disclosure agreements	Individuals under the cloud PII processor's control with access to PII should be subject to a confidentiality obligation.	(19.10 Information security: none)
	A.10.2 Restriction of the creation of hardcopy material	The creation of hardcopy material displaying PII should be restricted.	
	A.10.3 Control and logging of data restoration	There should be a procedure for, and a log of, data restoration efforts.	
	A.10.4 Protecting data on storage media leaving the premises	PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).	
	A.10.5 Use of unencrypted storage media and devices	Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented.	

	A.10.6 Encryption of PII transmitted over public data-transmission networks	PII that is transmitted over public data-transmission networks should be encrypted prior to transmission.	
	A.10.7 Secure disposal of hardcopy materials	Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.	
	A.10.8 Unique use of user IDs	If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes.	
	A.10.9 Records of authorized users	An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained.	
	A.10.10 User ID management	De-activated or expired user IDs should not be granted to other individuals.	
	A.10.11 Data processing contract measures	Data processing contracts between the cloud service customer and the cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data is not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the cloud PII processor.	
	A.10.112 Sub-contracted PII processing	Data processing contracts between the cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor.	
	A.10.113 Access to data on pre-used data storage space	The cloud PII processor should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to the cloud service customer.	
A.11 Privacy compliance	A.11.1 Geographical location of PII	The cloud PII processor should specify and document the countries in which PII might possibly be stored.	(19.11 Privacy compliance)
	A.11.2 Intended destination of PII	PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.	

1

Bibliography

- 2 [1] NIST Special Publication 800-53 Appendix J, Security and Privacy Controls for Federal Information
3 Systems and Organizations, July, 2011
- 4 [2] NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable
5 Information (PII), NIST, April 2010.
- 6 [3] European Commission, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 2011
- 7 [4] KCS, Personal Information Management System, December, 2011.
- 8 [5] BSI 10012, Specification for a personal information management system