INTERNATIONAL STANDARD

ISO/IEC 29151

First edition
2017-08

Information technology — Security techniques — Code of practice for personally identifiable information protection

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la protection des données à caractère personnel

Reference number
ISO/IEC 29151:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

CONTENTS

Page

1 Scope 1
2 Normative references 1
3 Definitions and abbreviated terms 1
3.1 Definitions 1
3.2 Abbreviated terms 1
4 Overview 2
4.1 Objective for the protection of PII 2
4.2 Requirement for the protection of PII 2
4.3 Controls 2
4.4 Selecting controls 2
4.5 Developing organization specific guidelines 3
4.6 Life cycle considerations 3
4.7 Structure of this Specification 3
5 Information security policies 4
5.1 Management directions for information security 4
6 Organization of information security 4
6.1 Internal organization 4
6.2 Mobile devices and teleworking 5
7 Human resource security 6
7.1 Prior to employment 6
7.2 During employment 6
7.3 Termination and change of employment 6
8 Asset management 7
8.1 Responsibility for assets 7
8.2 Information classification 7
8.3 Media handling 8
9 Access control 9
9.1 Business requirement of access control 9
9.2 User access management 9
9.3 User responsibilities 10
9.4 System and application access control 10
10 Cryptography 11
10.1 Cryptographic controls 11
11 Physical and environmental security 11
11.1 Secure areas 11
11.2 Equipment 12
12 Operations security 12
12.1 Operational procedures and responsibilities 12
12.2 Protection from malware 13
12.3 Backup 13
12.4 Logging and monitoring 13
12.5 Control of operational software 14
12.6 Technical vulnerability management 14
12.7 Information systems audit considerations 14
13 Communications security 15
13.1 Network security management 15
13.2 Information transfer 15
14 System acquisition, development and maintenance 15
14.1 Security requirements of information systems 15
14.2 Security in development and support processes 16

Page
14.3 Test data ... 16
15 Supplier relationships ... 17
15.1 Information security in supplier relationships ... 17
15.2 Supplier service delivery management ... 18
16 Information security incident management ... 18
16.1 Management of information security incidents and improvements ... 18
17 Information security aspects of business continuity management ... 19
17.1 Information security continuity ... 19
17.2 Redundancies ... 19
18 Compliance ... 20
18.1 Compliance with legal and contractual requirements ... 20
18.2 Information security reviews ... 21
Annex A – Extended control set for PII protection (This annex forms an integral part of this Recommendation | International Standard.) ... 22
A.1 General ... 22
A.2 General policies for the use and protection of PII ... 22
A.3 Consent and choice ... 22
A.4 Purpose legitimacy and specification ... 24
A.5 Collection limitation ... 26
A.6 Data minimization ... 26
A.7 Use, retention and disclosure limitation ... 27
A.8 Accuracy and quality ... 30
A.9 Openness, transparency and notice ... 31
A.10 PII principal participation and access ... 32
A.11 Accountability ... 34
A.12 Information security ... 37
A.13 Privacy compliance ... 37
Bibliography ... 39

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.

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

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

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

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

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.1058.

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, societal expectations for the protection of PII and the security of data relating to individuals are also increasing. A number of countries are augmenting their laws to address the increased number of high profile data breaches.

As the number of PII breaches increases, organizations collecting or processing PII 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. This Specification provides such guidance.

This Specification offers guidance for PII controllers on a broad range of information security and PII protection controls that are commonly applied in many different organizations that deal with protection of PII. The remaining parts of the family of ISO/IEC standards, listed here, provide guidance or requirements on other aspects of the overall process of protecting PII:

- ISO/IEC 27001 specifies an information security management process and associated requirements, which could be used as a basis for the protection of PII.
- ISO/IEC 27002 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls, taking into consideration the organization's information security risk environment(s).
- ISO/IEC 27009 specifies the requirements for the use of ISO/IEC 27001 in any specific sector (field, application area or market sector). It explains how to include requirements additional to those in ISO/IEC 27001, how to refine any of the ISO/IEC 27001 requirements, and how to include controls or control sets in addition to Annex A of ISO/IEC 27001.
- ISO/IEC 27018 offers guidance to organizations acting as PII processors when offering processing capabilities as cloud services.
- ISO/IEC 29134 provides guidelines 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.

Controls should be chosen based on the risks identified as a result of a risk analysis to develop a comprehensive, consistent system of controls. Controls should be adapted to the context of the particular processing of PII.

This Specification contains two parts: 1) the main body consisting of clauses 1 to 18, and 2) a normative annex. This structure reflects normal practice for the development of sector-specific extensions to ISO/IEC 27002.

The structure of the main body of this Specification, including the clause titles, reflects the main body of ISO/IEC 27002. The introduction and clauses 1 to 4 provide background on the use of this Specification. Headings for clauses 5 to 18 mirror those of ISO/IEC 27002, reflecting the fact that this Specification builds on the guidance in ISO/IEC 27002, adding new controls specific to the protection of PII. Many of the controls in ISO/IEC 27002 need no amplification in the context of PII controllers. However, in some cases, additional implementation guidance is needed, and this is given under the appropriate heading (and clause number) from ISO/IEC 27002.

The normative annex contains an extended set of PII protection-specific controls that supplement those given in ISO/IEC 27002. These new PII protection controls, with their associated guidance, are divided into 12 categories, corresponding to the privacy policy and the 11 privacy principles of ISO/IEC 29100:

- consent and choice;
- purpose, legitimacy and specification;
- collection limitation;
- data minimization;
- use, retention and disclosure limitation;
- accuracy and quality;
- openness, transparency and notice;
- individual participation and access;
- accountability;
- information security; and
- privacy compliance.

Figure 1 describes the relationship between this Specification and the family of ISO/IEC standards.

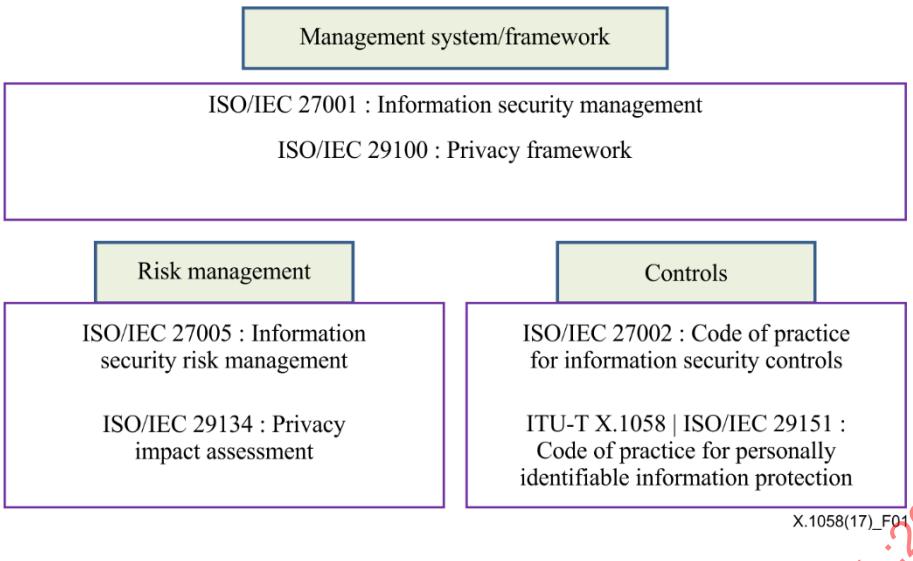

Figure 1 – The relationship of this Specification and the family of ISO/IEC standards

This Specification includes guidelines based on ISO/IEC 27002, and adapts these as necessary to address the privacy safeguarding requirements that arise from the processing of PII:

a) In different processing domains such as:
   - public cloud services,
   - social networking applications,
   - internet-connected devices in the home,
   - search, analysis,
   - targeting of PII for advertising and similar purposes,
   - big data analytics programmes,
   - employment processing,
   - business management in sales and service (enterprise resource planning, customer relationship management);

b) In different locations such as:
   - on a personal processing platform provided to an individual (e.g., smart cards, smart phones and their apps, smart meters, wearable devices),
   - within data transportation and collection networks (e.g., where mobile phone location data is created operationally by network processing, which may be considered PII in some jurisdictions),
   - within an organization's own processing infrastructure,
   - on a third party's processing platform;

c) For the collection characteristic such as:
   - one-time data collection (e.g., on registering for a service),
   - 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 – Ongoing data collection can contain or yield behavioural, locational and other types of PII. In such cases, the use of PII protection controls that allow access and collection to be managed based on consent and that allow the PII principal to exercise appropriate control over such access and collection, need to be considered.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Security techniques – Code of practice for personally identifiable information protection

1 Scope

This Recommendation | International Standard establishes control objectives, controls and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of personally identifiable information (PII).

In particular, this Recommendation | International Standard specifies guidelines based on ISO/IEC 27002, taking into consideration the requirements for processing PII that may be applicable within the context of an organization's information security risk environment(s).

This Recommendation | International Standard is applicable to all types and sizes of organizations acting as PII controllers (as defined in ISO/IEC 29100), including public and private companies, government entities and not-for-profit organizations that process PII.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

- 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 Definitions and abbreviated terms

3.1 Definitions

For the purposes of this Recommendation | International Standard, the terms and definitions that are given in ISO/IEC 27000:2016, ISO/IEC 29100 and the following apply.

The ISO *Online browsing platform*, IEC *Electropedia* and ITU *Terms and definitions* are terminological databases for use in standardization.

3.1.1 chief privacy officer (CPO): Senior management individual who is accountable for the protection of personally identifiable information (PII) in an organization.

3.1.2 de-identification process: Process of removing the association between a set of identifying data and the data principal, using de-identification techniques.

3.2 Abbreviated terms

For the purposes of this Specification, the following abbreviations apply.

BCR	Binding Corporate Rule
CCTV	Closed-Circuit Television
CPO	Chief Privacy Officer
PBD	Privacy By Design
PDA	Personal Digital Assistant
PET	Privacy Enhancing Technology

PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
RFID	Radio Frequency Identification
USB	Universal Serial Bus

4 Overview

4.1 Objective for the protection of PII

This Specification provides a set of controls for PII protection. The objective of the protection of PII is to enable organizations to put in place a set of controls as part of their overall PII protection programme. They can be used in a framework for maintaining and improving compliance with privacy-related laws and regulations, managing privacy risks and meeting the expectations of PII principals, regulators or clients, in accordance with the privacy principles described in ISO/IEC 29100.

4.2 Requirement for the protection of PII

An organization should identify its PII protection requirements. The privacy principles in ISO/IEC 29100 apply to the identification of requirements. There are three main sources of PII protection requirements:

- legal, statutory, regulatory and contractual requirements related to protection of PII including, for example, PII requirements that an organization, its trading partners, contractors and service providers have to comply with;
- assessment of risks (i.e., security risks and privacy risks) to the organization and the PII principal, taking into account the organization's overall business strategy and objectives, through a risk assessment;
- corporate policies: an organization may also choose voluntarily to go beyond the criteria that are derived from previous requirements.

Organizations should also consider the principles (i.e., privacy principles defined in ISO/IEC 29100), objectives and business requirements for processing PII that have been developed to support their operations.

PII protection controls (including security controls) should be selected on the basis of a risk assessment. The results of a privacy impact assessment (PIA), e.g., as specified in ISO/IEC 29134, will help to guide and determine the appropriate treatment action and priorities for managing risks to the protection of PII and for implementing controls selected to protect against these risks.

A PIA specification such as that in ISO/IEC 29134 may provide PIA guidance, including advice on risk assessment, risk treatment plan, risk acceptance and risk review.

4.3 Controls

A privacy risk assessment can assist organizations in identifying the specific risks of privacy breaches resulting from unlawful processing or of cutting the rights of the PII principal involved in an envisaged operation. Organizations should identify and implement controls to treat the risks identified by the risk impact process. The controls and treatments should then be documented, ideally separately in a separate risk register. Certain types of PII processing can warrant specific controls for which the need only becomes apparent once an envisaged operation has been carefully analysed.

4.4 Selecting controls

Controls can be selected from this Specification (which includes by reference the controls from ISO/IEC 27002, creating a combined reference control set). 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 treatment options and the general risk management approach, applied to the organization and, through contractual agreements, to its customers and suppliers, and should also be subject to all applicable national and international legislation and regulations.

The selection and implementation of controls is also dependent upon the organization's role in the provision of infrastructure or services. Many different organizations may be involved in providing infrastructure or services. In some circumstances, selected controls may be unique to a particular organization. In other instances, there may be shared roles in implementing controls. Contractual agreements should clearly specify the PII protection responsibilities of all organizations involved in providing or using the services.

The controls in this Specification can be used as reference for organizations that process PII, and are intended to be applicable for all organizations acting as PII controllers. Organizations acting as PII processors should do so, in accordance with the instructions of the PII controller. PII controllers should ensure that their PII processors are able to implement all the necessary controls included in their PII processing agreement, in accordance with the purpose of PII processing. PII controllers using cloud services as PII processors may review ISO/IEC 27018 to identify relevant controls to implement.

The controls in this Specification are explained in more detail in clauses 5 to 18, 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 (PBD). More information about selecting controls and other risk treatment options can be found in ISO/IEC 29134. Other relevant references are listed in the bibliography.

4.5 Developing organization specific guidelines

This Specification can be regarded as a starting point for developing organization specific guidelines. Not all of the controls and guidance in this Specification are applicable to all organizations.

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

4.6 Life cycle considerations

PII has a natural life cycle, from creation or origination, collection, through storage, use and transfer to its eventual disposal (e.g., secure destruction). The value of, and risks to, PII may vary during its life cycle, but protection of PII remains important to some extent at all stages and in all contexts of its life cycle.

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

4.7 Structure of this Specification

The remainder of this Specification contains two main normative parts.

The first part of this Specification, made up of clauses 5 to 18, contains additional implementation guidance and other information for certain relevant existing controls described in ISO/IEC 27002. The format for this part uses the relevant clause headings and numbering from ISO/IEC 27002 to allow cross-reference to that International Standard.

The second part contains a specific control set for PII protection specified in Annex A. It uses the same format as ISO/IEC 27002, which specifies control objectives (text within a box) followed by one or more controls that can be applied. Control descriptions are structured as follows.

Control

Text under this heading defines the specific control statement to fulfil the control objective.

Implementation guidance for the protection of PII

Text under this heading provides more detailed information to support the implementation of the control and meeting the control objectives. The guidance provided in this Specification may not be entirely suitable or sufficient in all situations and may not fulfil the organization's specific control requirements. Alternative or additional controls, or other forms of risk treatment (avoiding or transferring risks), may therefore be appropriate.

Other information for the protection of PII

Text under this heading provides further information that may need to be considered, such as legal considerations and references to other standards.

5 Information security policies

5.1 Management directions for information security

5.1.1 Introduction

The objective specified in 5.1 of ISO/IEC 27002:2013 applies.

5.1.2 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 include appropriate statements of security measures for the protection of PII. The details about the protection of PII are available in 18.1.4 of ISO/IEC 27002:2013.

When designing, implementing and reviewing information security policy, organizations should consider privacy safeguarding requirements described in ISO/IEC 29100.

Organizations should specify the elements of PII protection not related to security as a separate privacy policy. See the guidance in clause A.2.

5.1.3 Review of the policies for information security

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

6 Organization of information security

6.1 Internal organization

6.1.1 Introduction

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

6.1.2 Information security roles and responsibilities

Control 6.1.1 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

Roles and responsibilities for the protection of PII need to be clearly defined, properly documented and appropriately communicated. Specifically:

a) a clearly identified senior individual [sometimes referred to as the chief privacy officer (CPO)] within the organization should be allocated the accountability for PII protection;

b) a clearly identified individual or individuals (i.e., PII protection function) should be assigned responsibility for coordinating with the information security functions within the organization; and

c) all individuals that are involved with the processing of PII (including users and support staff) should have appropriate PII protection requirements included in their job specifications.

The established PII protection function should work closely with other functions processing PII, the information security function, which implements security requirements that include ones arising from PII protection laws, as well as the legal function, which assists in interpreting laws, regulations and contract terms, and in handling data breaches.

The organization should examine the need for and establish, as appropriate, a cross-functional council or committee comprising senior members from functions that process PII. Protection of PII being a multi-disciplinary function, such a group can help proactively identify opportunities for improvements, identifying new risks and areas for conducting PIAs, planning preventive actions, detection and reaction measures for any breaches, etc. It is recommended that such a group should meet periodically and be chaired by the person responsible for PII protection as identified in a).

The PII controller should require its PII processor(s) to designate a point of contact to address questions regarding the processing of PII under the PII processing contract.

Individuals responsible for PII protection functions should report to a CPO in order to ensure they have sufficient authority to fulfil their responsibilities.

6.1.3 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 should be independent of those for information security. While recognizing the importance of information security for the protection of PII, it is important that duties and area of responsibilities of the security and PII protection be as independent of each other as possible. If necessary or helpful, in the interest of PII protection, coordination and cooperation of those responsible for information security and for PII protection should be facilitated.

Organizations should adopt the principle of segregation of duties when assigning access rights for PII processing, especially any processing identified as high risk.

Access to PII being processed and access to log files concerning that processing should be separate duties.

Access to information concerning the collection of PII in order to respond to requests from PII principals should be segregated from all other forms of access to PII. Access should be limited to those whose duties include responding to PII principal requests.

6.1.4 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

Where applicable, organizations should have procedures in place that specify when and by whom authorities (including data protection authorities) should be contacted, e.g., to report privacy breaches or to report processing details.

6.1.5 Contact with special interest groups

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

6.1.6 Information security in project management

Control 6.1.5 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

Any new project initiation should trigger at least a threshold analysis to determine whether a PIA needs to be conducted. Note that the term project covers all incidents where an organization implements or modifies new or existing technology, product, service, programme, information system, process or project.

Further guidance can be found in the PIA specified in ISO/IEC 29134.

6.2 Mobile devices and teleworking

6.2.1 Introduction

The objective specified in 6.2 of ISO/IEC 27002:2013 applies.

6.2.2 Mobile device policy

Control 6.2.1 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

Organizations should strictly limit access to PII from portable and mobile devices, such as laptops, mobile phones, universal serial bus (USB) devices, and personal digital assistants (PDAs) that may generally be exposed to higher risk than non-portable devices (e.g., desktop computers at the organization's facilities), depending on the risk assessment.

Organizations should strictly limit remote access to PII and in cases where remote access is unavoidable, ensure that the communications for remote access are encrypted, message authenticated and integrity protected.

6.2.3 Teleworking

Control 6.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

7 Human resource security

7.1 Prior to employment

7.1.1 Introduction

The objective specified in 7.1 of ISO/IEC 27002:2013 applies.

7.1.2 Screening

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

7.1.3 Terms and conditions of employment

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

7.2 During employment

7.2.1 Introduction

The objective specified in 7.2 of ISO/IEC 27002:2013 applies.

7.2.2 Management responsibilities

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

7.2.3 Information security awareness, education and training

Control 7.2.2 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

Measures should be put in place to make relevant staff aware of the possible consequences for the PII controller (e.g., legal consequences, loss of business, or brand or reputational damage), for the staff member (e.g., disciplinary consequences) and for the PII principal (e.g., physical, material and emotional consequences) of breaching privacy or security rules and procedures, especially those addressing the processing of PII.

Just as with information security awareness, education and training, organizations should provide for the appropriate training, education and awareness regarding the protection and the processing of PII.

7.2.4 Disciplinary process

Control 7.2.3 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 establish a formal disciplinary policy. This policy in case of privacy breaches should be clearly communicated to affected individuals. Organizations should enforce this policy in all cases of privacy breaches.

7.3 Termination and change of employment

7.3.1 Introduction

The objective specified in 7.3 of ISO/IEC 27002:2013 applies.

7.3.2 Termination or change of employment responsibilities

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

8 Asset management

8.1 Responsibility for assets

8.1.1 Introduction

The objective specified in 8.1 of ISO/IEC 27002:2013 applies.

8.1.2 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 assets using, for example, the information given from the PIA report, if any, as specified in ISO/IEC 29134. This should include the PII assets and all systems that process PII.

When developing and maintaining the inventory, organizations should extract the following information elements from PIAs concerning information systems processing PII. The following list is given as an example – there might be additions or subtractions to the final implemented lists:

a) name of and acronym for each identified system;

b) types of PII processed by those systems;

c) classification (see 8.2.2) of all types of PII, both as individual information elements and as combined in those information systems;

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

e) purpose(s) for collecting the PII;

f) whether PII processing will be outsourced to a PII processor;

g) whether PII is transmitted to other PII controllers, and if so, to whom (or to which group of recipients);

h) retention period of PII;

i) geographical area where the PII was collected or processed; and

j) whether trans-border data transfer is involved.

Organizations should provide regular updates of the PII inventory to the person accountable for protection of PII to support the establishment of appropriate security controls for all new or updated information systems processing PII.

8.1.3 Ownership of assets

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

8.1.4 Acceptable use of assets

Control 8.1.3 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 protect assets supporting PII against unauthorized access, unauthorized modification, unauthorized removal, loss or destruction, or wrong and unlawful processing and so on.

8.1.5 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

8.2.1 Introduction

The objective specified in 8.2 of ISO/IEC 27002:2013 applies.

8.2.2 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

Organizations should classify all information containing PII, using an existing classification category (called an information group in ISO/IEC 27002) or newly created classification categories. New classification categories should include, but are not limited to, general ones such as sensitive and non-sensitive PII. A classification scheme may also include more specific categories such as personal health information (PHI), personal financial information (PFI). If organizations create new classification categories, then levels of protection for those should also be defined. The actual categories used should also depend upon, for example, the requirements defined in relevant data protection legislation and regulations, other legal (e.g., contractual) obligations, the nature and sensitivity of the information, and the risk of harm that might arise in the event of a breach.

Some PII that may be classified non-sensitive in one country may be treated as sensitive elsewhere, depending on the applicable data protection laws.

The classification for an element of PII could need re-evaluation and modification when associated with one or more additional attributes. Appropriate guidelines and procedures should be put in place.

8.2.3 Labelling of Information

Control 8.2.2 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

Where an organization does not classify PII to a classification category, the organization should ensure that people under its control are made aware of the definition of PII and how to recognize whether information is PII.

8.2.4 Handling of assets

Control 8.2.3 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

If organizations allow people under their control to be able to omit the information labelling for the classification category related to PII, organizations should make people under the their control handle all information containing PII as the information of the assigned classification category.

8.3 Media handling

8.3.1 Introduction

The objective specified in 8.3 of ISO/IEC 27002:2013 applies.

8.3.2 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 jurisdictions may require removable media containing PII to be encrypted. Whether or not it is required by law, encryption is recommended to reduce the risk of PII leakage.

If data confidentiality or integrity are important considerations, cryptographic techniques should be used to protect PII on removable media. A risk assessment should be performed to identify the required level of protection, which in turn will help determine the necessary type, strength and quality of cryptographic algorithm to be used.

Additional guidance regarding the use of cryptographic controls is provided in 10.1.

8.3.3 Disposal of media

Control 8.3.2 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

The procedures for secure disposal of media containing PII should be proportional to the sensitivity of the information, as well as the level of impact from inappropriate processing of that information. Some jurisdictions may impose criteria on procedures used to dispose of media containing PII or specific types of PII (e.g., health data, financial data).

8.3.4 Physical media transfer

Control 8.3.3 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

Whenever physical media are used for information transfer, a measure should be put in place to record incoming and outgoing physical media containing PII, including the type of physical media, any identifying numbers (e.g., serial numbers or inventory tag numbers), the authorized sender/recipients, the date and time, the number of physical media, and the types of PII they contain and to detect loss of physical media. The purpose and extent of the transfer, the person responsible for its authorization and the legal/contractual basis for the transfer should also be documented. Explicit reference to the data minimization principle should additionally be considered.

9 Access control

9.1 Business requirement of access control

9.1.1 Introduction

The objective specified in 9.1 of ISO/IEC 27002:2013 applies.

9.1.2 Access control policy

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

9.1.3 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

9.2.1 Introduction

The objective specified in 9.2 of ISO/IEC 27002:2013 applies.

9.2.2 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

Procedures for user registration and de-registration as well as user life cycle management should provide measures to 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).

9.2.3 User access provisioning

Control 9.2.2 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

Organizations should provide users with an appropriate right of access to the information systems processing PII, in accordance with the data minimization principle described in ISO/IEC 29100.

Organizations should restrict access to information systems processing PII to the minimum number of individuals needed to carry out the specified purposes for that processing, in accordance with the data minimization principle described in ISO/IEC 29100.

Organizations should adopt strong authentication methods for particular PII and PII processing (i.e., health data).

9.2.4 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

Large scale processing of PII (e.g., batch queries, batch modification, batch export, batch deletion) increases the risk of a large scale breach. Organizations should take special care when assigning access rights for such privileged operations. In order to prevent the abuse of PII, privileged access rights for PII processing (especially high risk PII processing) should be assigned on a strictly limited basis. They should also be assigned in a way that helps reduce the risk of collusion between two or more individuals. The granting and use of such rights should be recorded in relevant log files. All access approvals should be for a specified period. Organizations should review all such approvals on a regular basis and as appropriate, renew, revoke or expire approvals as appropriate.

9.2.5 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.

9.2.6 Review of user access rights

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

9.2.7 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

9.3.1 Introduction

The objective specified in 9.3 of ISO/IEC 27002:2013 applies.

9.3.2 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

9.4.1 Introduction

The objective specified in 9.4 of ISO/IEC 27002:2013 applies.

9.4.2 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 that enable automated massive retrieval of PII from databases that contain PII, organizations should review the necessity to use such languages when processing PII.

Where the use of query languages is consistent with the protection requirement, organizations should provide technical measures to limit the use of such languages to the minimum necessary to fulfil the specified purpose(s).

This can, for example, mean that access restrictions limit the use of query language to a few predefined sensitive fields of the records.

Where individuals require access to areas for which they normally are not authorized (e.g., the operational area), robust approval mechanisms should be implemented. Organizations should maintain a record of all such approvals.

9.4.3 Secure log-on procedures

Control 9.4.2 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

Where PII principals can request accounts from a PII controller, the PII controller should provide secure log-on procedures for those accounts, depending on the results of a risk analysis.

9.4.4 Password management system

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

9.4.5 Use of privileged utility programs

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

9.4.6 Access control to program source code

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

10 Cryptography

10.1 Cryptographic controls

10.1.1 Introduction

The objective specified in 10.1 of ISO/IEC 27002:2013 applies.

10.1.2 Policy on the use of cryptographic controls

Control 10.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

10.1.3 Key management

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

11 Physical and environmental security

11.1 Secure areas

11.1.1 Introduction

The objective specified in 11.1 of ISO/IEC 27002:2013 applies.

11.1.2 Physical security perimeter

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

11.1.3 Physical entry controls

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

11.1.4 Securing offices, rooms and facilities

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

11.1.5 Protecting against external and environmental threats

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

11.1.6 Working in secure areas

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

11.1.7 Delivery and loading areas

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

11.2 Equipment

11.2.1 Introduction

The objective specified in 11.2 of ISO/IEC 27002:2013 applies.

11.2.2 Equipment siting and protection

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

11.2.3 Supporting utilities

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

11.2.4 Cabling security

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

11.2.5 Equipment maintenance

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

11.2.6 Removal of assets

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

11.2.7 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.

11.2.8 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. The following additional guidance also applies.

Implementation guidance for the protection of PII

For the purposes of secure disposal or re-use, equipment containing storage media that may possibly contain PII should be physically destroyed or the PII should either be destroyed, deleted or overwritten using approved techniques, in accordance with well-defined and documented procedures, to render the original PII unrecoverable rather than simply using the standard delete or format function. For equipment containing storage media that may possibly contain encrypted PII, the controlled destruction of decryption keys or key holders (such as smart cards), may be sufficient.

11.2.9 Unattended user equipment

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

11.2.10 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

12.1.1 Introduction

The objective specified in 12.1 of ISO/IEC 27002:2013 applies.

12.1.2 Documented operating procedures

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

12.1.3 Change management

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

12.1.4 Capacity management

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

12.1.5 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. The following additional guidance also applies.

Implementation guidance for the protection of PII

Development, testing and operational environments should be logically and, where possible, physically separate environments. Appropriate access controls should be implemented to ensure access is limited to properly authorized individuals. If test or development networks or devices require access to the operational network, strong access controls should be implemented.

Organization should assess the risk of using removable media and devices containing PII with wireless capabilities, regardless of the environment in which they will be used.

Where not permitted by law or by explicit consent of the PII principal, PII should not be used for purposes of development and testing without prior anonymization.

12.2 Protection from malware

12.2.1 Introduction

The objective specified in 12.2 of ISO/IEC 27002:2013 applies.

12.2.2 Controls against malware

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

12.3 Backup

12.3.1 Introduction

The objective specified in 12.3 of ISO/IEC 27002:2013 applies.

12.3.2 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

Information systems processing PII should introduce additional or alternative mechanisms, such as off-site backups for protection against loss of PII, ensuring continuity of PII processing operations, and providing the ability to restore PII processing operations after a disruptive event, if only strictly necessary.

NOTE – Some time passes between backup and recovery operations. PII stored in a backup may no longer be up to date when it is accessed in order to be restored. Any operations based on out-of-date PII may lead to incorrect results and pose a privacy risk.

12.4 Logging and monitoring

12.4.1 Introduction

The objective specified in 12.4 of ISO/IEC 27002:2013 applies.

12.4.2 Event logging

Control 12.4.1 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

Where possible, the event log should record which PII was accessed, what was done to the PII (e.g., read, print, add, modify, delete), when and by whom, especially for certain types of PII (e.g., health data). Where multiple service providers are involved in providing a service, there may be varied or shared roles in implementing this guidance.

A process should be put in place to review the event log with a specified, documented periodicity to identify irregularities and propose remediation efforts.

The PII controller should define procedures regarding whether, when and how log information can be made available to or usable by the administrator for purposes such as security monitoring and operational diagnostics.

12.4.3 Protection of log information

Control 12.4.2 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

Log information recorded for purposes such as security monitoring and operational diagnostics may contain PII. Measures, such as access control (see 9.2.3), should be put in place to ensure that logged information is only used for its intended purposes. Measures should be put in place to ensure log file integrity.

12.4.4 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 monitor privileged access (e.g., by system administrators and operators) to PII and any subsequent processing by those individuals. Such monitoring should form part of the overall monitoring of information systems processing PII.

Organizations should define what they consider to be anomalous activity and should implement automated procedures to report such activity to relevant individuals within the organization.

12.4.5 Clock synchronization

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

12.5 Control of operational software

12.5.1 Introduction

The objective specified in 12.5 of ISO/IEC 27002:2013 applies.

12.5.2 Installation of software on operational systems

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

12.6 Technical vulnerability management

12.6.1 Introduction

The objective specified in 12.6 of ISO/IEC 27002:2013 applies.

12.6.2 Management of technical vulnerabilities

Control 12.6.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.6.3 Restrictions on software installation

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

12.7 Information systems audit considerations

12.7.1 Introduction

The objective specified in 12.7 of ISO/IEC 27002:2013 applies.

12.7.2 Information systems audit controls

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

13 Communications security

13.1 Network security management

13.1.1 Introduction

The objective specified in 13.1 of ISO/IEC 27002:2013 applies.

13.1.2 Network controls

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

13.1.3 Security of network services

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

13.1.4 Segregation in networks

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

13.2 Information transfer

13.2.1 Introduction

The objective specified in 13.2 of ISO/IEC 27002:2013 applies.

13.2.2 Information transfer policies and procedures

Control 13.2.1 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

Appropriate measures should be put in place to reduce the risk of PII leakage during information transfer. This is generally solved by implementing encryption and other preliminary measures could include de-identification, masking or obfuscation.

13.2.3 Agreements on information transfer

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

13.2.4 Electronic messaging

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

13.2.5 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

Organizations should specify the conditions under which external processing of PII may take place. These conditions should be part 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

14.1.1 Introduction

The objective specified in 14.1 of ISO/IEC 27002:2013 applies.

14.1.2 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 making significant changes to information systems that process PII, a PIA should be conducted. Guidance on the conduct of PIAs can be found in ISO/IEC 29134. The results of the PIA should be used to determine the controls to treat the risks identified during the PIA process.

14.1.3 Securing application services on public networks

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

14.1.4 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

14.2.1 Introduction

The objective specified in 14.2 of ISO/IEC 27002:2013 applies.

14.2.2 Secure development policy

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

14.2.3 System change control procedures

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

14.2.4 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.

14.2.5 Restrictions on changes to software packages

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

14.2.6 Secure system engineering principles

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

14.2.7 Secure development environment

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

14.2.8 Outsourced development

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

14.2.9 System security testing

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

14.2.10 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

System acceptance testing should also include testing of privacy safeguarding requirements.

14.3 Test data

14.3.1 Introduction

The objective specified in 14.3 of ISO/IEC 27002:2013 applies.

14.3.2 Protection of test data

Control 14.3.1 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

Operational data containing PII should not normally be used for development and testing. The use of real PII in these environments increases the risk of information compromise. Instead, organizations should either use synthetic data or should take steps to "hide" (e.g., mask, obfuscate, de-identify) any real PII in use.

15 Supplier relationships

15.1 Information security in supplier relationships

15.1.1 Introduction

The objective specified in 15.1 of ISO/IEC 27002:2013 applies.

15.1.2 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

In the event that an organization needs to make use of the services of a PII processor, PII processors should be evaluated on the basis of experience, trustworthiness and their ability to meet PII protection requirements as stipulated by applicable legislation, regulation, or in contracts or other legal agreements.

The organization acting as a PII controller should have a written contract with any supplier acting as a PII processor. The contract should clearly allocate roles and responsibilities between the PII controller and the PII processor and should contain appropriate clauses relating to PII protection in order to hold the PII processor accountable for the processing performed.

The PII controller contract should provide at least:

- an appropriate declaration on the scale, nature and purpose of the processing under contract;
- support duties of the PII processor on giving PII principals the ability to access and review their PII and handling any complaints raised by PII principals (see clause A.10);
- other organizational measures to be taken in order to fulfil legal or regulatory requirements;
- authorization of the PII controller to conduct audits on the premises of the PII processor;
- reporting obligations in cases of data breaches, unauthorized processing or other non-performance of contractual terms and condition, including identification of the points of contact in both parties;
- method of instruction from the PII controller to the PII processor;
- measures applying on termination of the contract, especially with regard to the secure deletion of PII on premise or returning of PII and physical media.

The PII controller should ensure that their PII processors do not undertake any further subcontracting of processing (i.e., make use of sub-processors) without prior approval of the PII controller. The PII controller should abide by all relevant legislation and regulations in this regard.

The PII controller should ensure that their PII processors do not process the PII for any purposes other than those specified in the contract or other legal agreement.

The PII controller should ensure that their PII processors securely dispose of PII, in accordance with the PII controller's policies or other direction (e.g., specific agency requirements).

15.1.3 Addressing security within supplier agreements

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

15.1.4 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

15.2.1 Introduction

The objective specified in 15.2 of ISO/IEC 27002:2013 applies.

15.2.2 Monitoring and review of supplier services

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

15.2.3 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

16.1.1 Introduction

The objective specified in 16.1 of ISO/IEC 27002:2013 applies.

16.1.2 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 be capable of providing (and be prepared to provide) an organized and effective response to a privacy incident. Organizations should therefore develop and implement a privacy incident response plan.

An organizational privacy incident response plan should include:

a) the definition of privacy incident and the scope of privacy incident response;

b) 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 should rest with senior management within the organization);

c) clearly defined roles, responsibilities and authorities for all members of the privacy incident response team;

d) procedures for clarifying the legal grounds for cooperation with external organizations (national and international) in the event of a cross-border incident;

e) procedures to ensure prompt reporting by all individuals subject to the internal privacy policy (e.g., employees, contractors) of any privacy incident to information security officials and the individual accountable for PII protection (sometimes referred to as the CPO), in accordance with organizational incident management direction;

f) an incident impact assessment (tasks) to determine the nature and extent of any potential or actual harms to affected individuals (e.g., embarrassment, inconvenience or unfairness) or to the organization;

g) a process to identify measures that need to be taken to mitigate the harms identified above and to reduce the likelihood of their recurrence; and

h) procedures to determine whether notice to affected individuals and other designated entities (e.g., regulators) is required, the timing for such notice and the form of that notice and, where appropriate, to provide that notice.

Organizations may choose to integrate their privacy incident response plans with their security incident response plans or keep them separate. An information security incident should trigger a review by the PII controller, as part of its information security incident management process, to determine if a data breach involving PII has taken place.

An information security event may not trigger such a review. An information security event 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. An information security event will not necessarily result in probable or actual compromise of PII or equipment or facilities processing PII.

16.1.3 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 PII principal cannot be protected without immediate measures.

Jurisdictions may impose specific requirements (e.g., in legislation or regulations) related to the reporting or notification of security incidents involving PII (e.g., unauthorized processing, breach). When a security incident related to PII occurs, the details of the incident, including the organizations' proposed response (the disclosure of which may be subject to certain limitations), should be notified as soon as possible to relevant authorities. These may include data protection authorities, law enforcement agencies and individuals affected by the incident.

Organizations should provide affected PII principals access to appropriate and effective remedies, such as correction or deletion of incorrect information, if a privacy breach has occurred.

16.1.4 Reporting security weaknesses

Control 16.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

16.1.5 Assessment of and decision on information security events

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

16.1.6 Response to information security incidents

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

16.1.7 Learning from information security incidents

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

16.1.8 Collection of evidence

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

17 Information security aspects of business continuity management

17.1 Information security continuity

17.1.1 Introduction

The objective specified in 17.1 of ISO/IEC 27002:2013 applies.

17.1.2 Planning information security continuity

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

17.1.3 Implementing information security continuity

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

17.1.4 Verify, review and evaluate information security continuity

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

17.2 Redundancies

17.2.1 Introduction

The objective specified in 17.2 of ISO/IEC 27002:2013 applies.

17.2.2 Availability of information processing facilities

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

18 Compliance

18.1 Compliance with legal and contractual requirements

18.1.1 Introduction

The objective specified in 18.1 of ISO/IEC 27002:2013 applies.

18.1.2 Identification of applicable legislation and contractual requirements

Control 18.1.1 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 identify the laws and regulations related to PII protection to which they are subject. If these are identified, then organizations should take necessary measures for those requirements. The following cases are examples of such requirements.

a) Where additional protection for certain categories of PII (e.g., national identifier, passport number or credit card numbers) is required, cryptographic techniques such as encryption should be used. The type, strength and quality of the cryptographic algorithm required should be taken. Cryptographic algorithms should only be selected from lists of approved algorithms.

   The security control related to this requirement is specified in 10.1.2.

b) Jurisdictions can impose a minimum frequency of data backup for information including PII as well as a minimum frequency of reviews of backup and recovery procedures.

   The security control related to this requirement is specified in 12.3.2.

Organizations should develop PIAs and implement the resulting privacy treatment plans in order to help ensure that programmes and services related to PII processing comply with privacy safeguarding requirements. Further guidance can be found in ISO/IEC 29134.

Organizations should establish an audit programme to help verify that PII processing complies with relevant privacy safeguarding requirements. The programme should specify the frequency with which audits are to be conducted.

Audits may be conducted by the organization (e.g., through an internal audit component) or they may be conducted by a qualified independent third party.

Other information for the protection of PII

While in many jurisdictions it will be the PII controller who is ultimately responsible for ensuring compliance, all actors involved in the processing of PII should take a proactive approach in identifying relevant privacy safeguarding requirements arising from legal or other factors.

A mechanism to ensure the PII processor supports and manages compliance is provided by the contract between the PII controller and the PII processor. The contract should call for independently audited compliance, acceptable to the PII processor, e.g., via the implementation of the relevant controls in this Specification, ISO/IEC 27002, and ISO/IEC 27018.

18.1.3 Intellectual property rights

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

18.1.4 Protection of records

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

18.1.5 Privacy and protection of personally identifiable information

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

18.1.6 Regulation of cryptographic controls

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

18.2 Information security reviews

18.2.1 Introduction

The objective specified in 18.2 of ISO/IEC 27002:2013 applies.

18.2.2 Independent review of information security

Control 18.2.1 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

If audits by individual interested parties are impractical or may increase risks to security, organizations should make available to prospective interested parties, prior to entering into a contract, independent evidence that information security is implemented and operated in accordance with the PII controller's policies and procedures. A relevant independent audit selected by the PII controller should normally be an acceptable method for fulfilling the interested parties' interest in reviewing the PII controller's processing operations, as long as sufficient transparency is provided.

18.2.3 Compliance with security policies and standards

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

18.2.4 Technical compliance review

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

Annex A

Extended control set for PII protection

(This annex forms an integral part of this Recommendation | International Standard.)

A.1 General

This annex provides definitions for new objectives, new controls and new implementation guidance making up an extended control set to meet the specific requirements for the protection of PII.

The guidance in this Specification builds on that provided in ISO 29100:2011 and assumes that the guidance in ISO 29100:2011 has been implemented.

Clause A.2 describes general policies for the protection of PII while the subsequent clauses reflect the privacy principles described in ISO/IEC 29100.

A.2 General policies for the use and protection of PII

Objective: To provide management direction and support for PII protection in accordance with business requirements and relevant laws and regulations.

Control

Organizations involved in the processing of PII should establish a policy for the use and protection of PII.

Implementation guidance for the protection of PII

The privacy policy should include appropriate statements (in separate privacy policies or as additions to existing policies) concerning support for and commitment to managing compliance with applicable PII protection legislation, contractual requirements and other internal policies.

Privacy and security policies may not cover the same topics, although they are closely related. Both information security policies and privacy policies should address the confidentiality, integrity and availability of information, and in addition privacy policies should address topics such as consent and individual access.

ISO/IEC 29100 provides guidance on implementing a privacy framework. The PII protection policy should:

- be appropriate to the purpose(s) of the organization;
- be transparent about the organization's collection and processing of PII;
- provide the framework for setting objectives for the protection of PII;
- define rules for making decisions in questions of protection of PII;
- define criteria on privacy risk acceptance (see also 6.3.1 of ISO/IEC 29134);
- 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.

A.3 Consent and choice

A.3.1 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 regulations, through the exercise of meaningful, informed and freely given consent.

Control

Organizations should provide the means necessary for PII principals to exercise meaningful, informed, unambiguous and freely given consent except where the PII principal cannot freely refuse consent or where applicable law specifically allows the processing of PII without the principal’s consent.

Implementation guidance for the protection of PII

Organizations should:

a) determine the practical means to be implemented to obtain the consent of the PII principals and analyse the cases where the practical means chosen are no longer operational and determine alternate solutions if necessary, in order to ensure that consent is obtained before any processing begins;

b) provide means, where feasible and appropriate or where legally required, for PII principals to provide consent, in order to ensure that consent is obtained before any processing begins – the processing includes collection, storage, alteration, retrieval, consultation, disclosure, de-identification, anonymization, dissemination or otherwise making available, deletion or destruction of PII;

c) where consent is being provided by a legal agent (e.g., on behalf of child or legally incapacitated persons), store the record of consent;

d) where necessary, inform PII principals of all instances of PII transfer to third parties and provide appropriate means for PII principals to provide their consent to such transfers;

e) obtain consent, where feasible and appropriate or where legally required, from PII principals prior to any new uses or disclosure of previously collected PII, and ensure that consent is obtained before any further processing begins;

f) ensure that the consent is obtained in an informed, transparent manner in terms of the purposes of the processing and ensure that consent is obtained for a specific purpose;

g) achieve awareness and consent, e.g., through updated public notices;

h) provide a mechanism for PII principals to modify the scope of their consent – any modification of consent should be acted upon in a timely manner and processing should be modified or cease, in accordance with the revised consent;

i) ensure that consent adheres to all applicable legal requirements, including where appropriate the requirement for explicit consent for sensitive PII;

j) where appropriate, allow for implied consent, where PII principals have been made clearly aware of the processing and have not objected, as this behaviour may indicate agreement;

k) give prior notification for all processing operations prior to their implementation; and

l) confirm, where needed, the identity of the PII principal or that of a PII principal's authorized agent, submitting consent to processing – the information requested for verification should be kept to the minimum essential for that purpose, should only be retained for as long as necessary for that purpose and should be securely disposed of when no longer required.

Other information for the protection of PII

Subject to applicable law, organizations should obtain consent through opt-in 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. If the consent is collected using electronic media, the organization should determine whether simple opt-in is appropriate or double opt-in is needed.

With opt-out mechanisms, organizations can assume that the PII principal has implicitly consented to the processing of their PII, unless the PII principal takes affirmative action to signal otherwise.

Implied consent is usually inferred by an individual's actions or lack thereof, or their particular circumstances. Example of implied consent: the customer provides the shipping address to the online retailer, and the retailer uses the information strictly for the purpose of delivery of the goods the customer purchased.

Organizations should provide practical means to be implemented to obtain the separate consent of the PII principals when national identification numbers (e.g., social security number, resident registration number, passport number) are collected.

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 the PII principal's choices as far as possible.

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

If the PII was transferred to or from another organization, organizations should establish a process to update their records to mirror content updates and consent changes (e.g., modification, revocation) made by PII principals and to ensure that these updates/changes are passed on to the organizations with whom the PII was shared. Only the minimum amount of information necessary to ensure that the correct records are updated should be collected from the PII principal and shared with other organizations. Organizations should periodically review their processes to ensure that no unnecessary PII is being processed.

A.3.2 Choice

Objective: To present to PII principals, where appropriate and feasible, the choice not to allow the processing of their PII, to refuse or withdraw consent or to oppose a specific type of processing, and to explain to PII principals the implications of granting or refusing consent.

Control

Organizations should provide PII principals with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice with respect to 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.

Implementation guidance for the protection of PII

Organizations should:

a) ensure that PII principals exercising a choice regarding the processing of their PII can do so before any processing takes place;

b) not withhold service from a PII principal who declines to provide PII that is not relevant to that service.

c) where provided for by relevant legislation or regulations, determine the practical means that will be implemented to enable PII principals to exercise their right to object to processing of their PII – PII principals should be given multiple means by which to exercise this right (e.g., by postal mail, e-mail, phone);

d) acknowledge the statement of objection within the time frames specified in applicable law or as defined in organizational policy;

e) analyse the cases where the practical means chosen are no longer operational and identify back-up solutions, if necessary, to allow PII principals to continue to exercise their right to object in a timely manner;

f) ensure that PII is classified, labelled and stored in a manner that facilitates the exercising of the right to object and ensure that PII principals can exercise their right to object in a timely manner and at no cost;

g) confirm the identity of the PII principal, or that of a PII principal's authorized agent, submitting an objection to processing – the information requested for verification should be kept to the minimum essential for that purpose, should only be retained for as long as necessary for that purpose and should be securely disposed of when no longer required;

h) ensure, if legal grounds are required to exercise the right to object, that PII principals exercising their right to object provide reasonable grounds for the objection – any refusal to comply with the objection should detail the reasons why the PII controller does not consider those grounds as legitimate;

i) ensure that all organizations with whom the PII has been shared are made aware of any objections submitted by the PII principal, and that they abide by any valid objections; and

j) where possible, provide PII principals with the ability to object to selected aspects of the PII processing, rather than having to accept or object to the processing in its entirety.

Other information for the protection of PII

In many situations, depending on applicable laws, it may 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 offer a choice to PII principals when collecting their name and address from a public record or a newspaper.

A.4 Purpose legitimacy and specification

A.4.1 Purpose legitimacy

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

Control

Organizations should implement appropriate measures to ensure that PII processing complies with applicable law and relies on a permissible legal ground.

Implementation guidance for the protection of PII

Organizations should:

a) determine whether the proposed processing can be undertaken on the basis of a legal ground other than consent (e.g., law enforcement, public safety, legal obligation or a legitimate interest of the PII controller);

b) determine whether the proposed processing is governed by a legal ground (e.g., law enforcement, public safety or legal obligation) that prohibits PII principals from exercising their choice regarding the processing of their PII;

NOTE – If collection or processing of PII is executed internationally, the need for consent and the proper way to process it can differ over the different legal frameworks that apply.

c) determine the legal authority (ground) that permits the processing of PII, either generally or in support of a specific programme or information system; and

d) incorporate procedures that ensure the processing is in accordance with all applicable regulation and its interpretation by competent authorities. The general context of the processing should be considered when determining the legitimacy of its purpose. This will include the nature of the underlying relationship between the PII controller and the PII principals, scientific and technological developments, and changes in societal and cultural attitudes.

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

If the organization has a works council or trade union, applicable laws may require consultation with such bodies when establishing the legitimacy of a purpose in case of employees.

Programme officials should consult with the individual accountable for PII protection (sometimes referred to as the CPO) or equivalent and legal counsel regarding the authority of any programme or activity to collect PII. The authority to collect PII should be documented.

A.4.2 Purpose specification

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

Control

Organizations should communicate to the PII principal from whom they are going to collect PII, the purpose(s) for which that PII is being collected and the purpose(s) for which the PII will be processed. Such communication should take place at or before the PII is collected and before the PII is processed for any purpose(s) not previously communicated to the PII principal.

Implementation guidance for the protection of PII

Organizations should communicate the purpose(s) to the PII principal before the information is collected or used for the first time for a new purpose, use language for this specification that is both clear and appropriately adapted to the circumstances, and give sufficient explanations for the need to process sensitive PII.

Often, statutory language expressly authorizes specific collections and uses of PII. When statutory language is written broadly and thus subject to interpretation, organizations should ensure, in consultation with the CPO and legal counsel, that there is a clear connection between the general authorization and any specific collection of PII.

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

Organizations should:

a) identify the PII useful only to each business process;

b) separate the PII useful to each process in logical fashion;

c) 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

d) regularly confirm that PII are separated effectively and that recipients and interconnections have not been added.

A.5 Collection limitation

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

Control

Organizations should implement appropriate measures to limit the collection of the type and amount of PII to the minimum elements for the purposes described in the notice (See A.9.1) and to that which is within the bounds of applicable laws and regulations.

Implementation guidance for the protection of PII

Organizations should:

a) limit the collection of PII to the minimum elements identified for the purposes described in the notice (See A.9.1) and for which the PII principal has provided consent;

b) not collect sensitive PII unless collection of sensitive PII is legally authorized or consent is obtained; and

c) limit the amount of information that they collect from or about a PII principal indirectly (e.g., through web logs, system logs).

Organizations should define the purpose(s) for processing PII, identify the PII necessary to achieve that purpose, identify information that does not need to be collected and confirm that only essential information is being collected.

Organizations should carefully consider which PII needs to be collected to realize a particular purpose before proceeding with collection. Organizations should not collect PII indiscriminately.

Organizations should regularly review the purpose(s) for which they are collecting PII to ensure that they are still valid. They should also regularly review the PII they are collecting to ensure that it is still only the minimum essential for the purpose(s).

Organizations should not collect sensitive PII, e.g., national identification number, unless collection of such information is legally authorized or explicit consent is obtained.

Other information for the protection of PII

Some jurisdictions may define certain categories of PII (e.g., racial origin, political opinions or religious or other beliefs, personal data on health, sex life or criminal convictions, and so on) as sensitive. These jurisdictions may impose restrictions or conditions on the collection of this kind of PII and organizations should take these restrictions and conditions into account when deciding which PII to collect.

A.6 Data minimization

Objective: To minimize the PII which is processed to what is strictly necessary for the legitimate interests pursued by the PII controller and to limit the disclosure of PII to a minimum number of privacy stakeholders.

Control

Organizations should implement appropriate measures to minimize the amount of PII being processed to that which is strictly necessary for the legitimate interests of the PII controller (e.g., an organization may seek to increase or extend its business operations in a manner which legitimately increases the amount of PII it processes and stores).

Implementation guidance for the protection of PII

Organizations should:

a) 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;

b) use or offer as default options, wherever possible, interactions and transactions which do not involve the identification of PII principals;

c) limit the linkability of the PII collected;

d) conduct an initial evaluation of PII retained by the organization and establish and follow a schedule for regularly reviewing those to ensure that only PII identified in the notice is collected, and that the PII continues to be necessary to accomplish the current business purposes;

e) restrict the transmission of electronic documents containing PII to a minimum of stakeholders who need them in connection with their work;

f) determine which PII should be anonymized or de-identified based on the context, the form in which the PII is stored (e.g., database fields or excerpts from texts) and the risks identified;

g) de-identify the data that require such de-identification based on the form of the data to be de-identified (e.g., databases and textual records) and the risks identified;

h) delete and dispose of PII whenever the purpose for PII processing has expired, when there are no legal requirements to keep the PII or whenever it is practical to do so; and

i) consider whether, and which, privacy enhancing technologies (PETs) may be used.

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

The PII should be classified into mandatory PII and optional PII for collection. Organizations should collect only the mandatory PII required for providing service and obtain appropriate opt-in consent from PII principals when collecting optional PII. Organizations should not decline to provide service when PII principals decline to give optional PII.

The CPO and legal counsel should challenge programme officials to justify the proposed processing of PII to ensure that it is the minimum necessary for the information system or activity to accomplish the legally authorized purpose.

NOTE 1 – Anonymization, as defined in ISO/IEC 29100, is a process by which PII is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party. Such a process necessarily involves an (irreversible) loss of information. In some cases, simply deleting part of the data can achieve the desired objective.

NOTE 2 –A description of privacy-enhancing data de-identification techniques, to be used to describe and design de-identification measures, in accordance with the privacy principles in ISO/IEC 29100 is planned to form the subject of a future International Standard. As a general rule, in order to conclude that a de-identification process complies with the law, de-identification is carried out by, e.g., deleting or generalizing attributes, together with strong organizational and technical measures.

NOTE 3 – When a PII is processed for a purpose, the extent of the PII processed is minimized so as to only serve the intended purpose, without revealing excessive information about the principal e.g., if the geographical area of a respondent to a traffic-related survey is required, consider collecting only nearby landmarks rather than a precise address.

NOTE 4 – Often during analysis of anonymized data when the output is a small data set, the identity of PII principals can be revealed. Therefore, it is good practice to prevent output when the number of records is less than a threshold number – say 10 records. The threshold needs to be carefully arrived at, based on a data distribution pattern.

Organizations should reduce their privacy and security risks by also reducing their inventory of PII, where appropriate. Organizations should conduct both an initial review and subsequent reviews of their PII holdings to ensure, to the maximum extent practicable, that such data stacks are accurate, relevant, timely, and complete.

Organizations should also be directed to reduce their PII holdings to the minimum necessary for the proper performance of a documented organizational business purpose. Organizations should develop and publicize a schedule for periodic reviews of their data stack to supplement the initial review.

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

A.7 Use, retention and disclosure limitation

A.7.1 Use, retention and disclosure limitation

Objective: To limit the use and disclosure of PII for specific, explicit and legitimate purposes and to retain PII no longer than necessary to fulfil the stated purposes or to abide by applicable laws.

Control

Organizations should implement appropriate measures to limit the processing of PII for legitimate and intended purposes and to retain PII only as long as necessary to fulfil the stated purposes or to abide by applicable laws.

Implementation guidance for the protection of PII

Organizations should:

a) limit the use, retention, and disclosure (including transfer) of PII to that which is necessary in order to fulfil specific, explicit and legitimate purposes; and

b) configure their information systems to record the date when PII is collected, created or updated and when PII is to be deleted or archived under an approved record retention schedule.

Implementation guidance on use for the protection of PII

Organizations should:

a) lock (i.e., archive, secure and exempt from further processing) any PII when the stated purposes have expired but retention is required by applicable laws;

b) use appropriate techniques or methods to ensure secure deletion or destruction of PII (including originals, copies and archived records);

c) use PII only for the purposes agreed with or disclosed to the PII principal before or at the time of collection, and obtain consent when necessary prior to any processing for any new purpose;

d) limit external party access to organizational systems and PII to that which is strictly necessary and which has been formally authorized – if access is really necessary for the business, appropriate approval procedures should be followed;

e) confirm the external party systems that are permitted to connect to organizational systems have implemented appropriate safeguards prior to being allowed to connect;

f) periodically review the safeguards implemented by third parties to ensure that they continue to meet the organization's security requirements – if, as a result of such a review, the safeguards are found to be inadequate, third parties should be disconnected until such time as they demonstrate that adequate safeguards have been restored;

g) implement appropriate access authentication mechanism when PII is accessed through remote interfaces – logs of PII access need to be recorded; and

h) provide notice to inform the public of any changes in PII holdings collected during the security monitoring process.

Implementation guidance on retention for the protection of PII

There may be circumstances in which a legal requirement to retain PII results in the retention of PII beyond that required for specified business purposes.

Organizations should:

a) only retain PII for authorized time period to fulfil the purpose(s) identified in the notice or as required by law and organizations and delete the PII promptly when the retention period expires;

b) where required to retain PII for longer than required for specified business purposes, implement measures such as de-identification to protect the PII;

c) define PII retention periods that are time limited and appropriate to the purpose of the processing;

d) confirm that the information system can detect the expiration of the retention period;

e) ensure that agreed retention periods are implemented and PII disposed of in accordance with the retention periods;

f) develop an automated functionality that deletes PII when its retention period expires – this deletion should occur immediately or as soon as it is practical to do;

g) determine what should be de-identified based on the context, the form in which the PII is stored (including database fields or excerpts from texts) and the risks identified;

h) de-identify the data that require such de-identification based on the form of the data to be de-identified (including databases and textual records) and the risks identified; and

i) choose tools (including partial deletion, hashing, key hashing and index) for the protection of PII if that data cannot be de-identified.

Implementation guidance on disclosure for the protection of PII

Organizations should:

a) not disclose PII to external parties without the prior knowledge and consent of the PII principal, unless such disclosure is otherwise permitted by relevant legislation – knowledge and consent of the PII principal may not be required where disclosure is to internal parties (e.g., employees) who have a need to know; and

b) provide strong protection mechanisms when PII is transferred, including data encryption and integrity protection.

Employee PII should be disposed of (i.e., securely deleted or archived) in accordance with applicable legislation and regulations, as well as in accordance with organizational disposal policies and where appropriate, employee consent.

A.7.2 Secure erasure of temporary files

Objective: To provide technical measures for temporary files to be deleted within the specific period.

Control

Temporary files and documents that may contain PII should be disposed of within a specified, documented period.

Implementation guidance for the protection of PII

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

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

A.7.3 PII disclosure notification

Objective: To ensure the PII processor notifies the PII controller of any legally binding request for disclosure of PII.

Control

The contract between the PII controller and the PII processor should require the PII processor to notify the PII controller, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by law enforcement or other authority, unless such disclosure is otherwise prohibited by law.

Implementation guidance for the protection of PII

Organizations should implement measures (e.g., contractual obligations) to ensure that:

a) PII processors consult the relevant PII controller prior to accepting any legally binding requests for disclosure of PII, unless otherwise prohibited by law; and

b) PII processors accept any contractually agreed requests for PII disclosures, as authorized by the relevant PII controller, unless otherwise prohibited by law.

A.7.4 Recording of PII disclosures

Objective: To ensure that disclosures of PII to third parties are recorded.

Control

Disclosures of PII to third parties should be recorded, including which PII has been disclosed, to whom, at what time and for which purpose.

Implementation guidance for the protection of PII

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

A.7.5 Disclosure of subcontracted PII processing

Objective: To ensure that PII processors disclose any use of subcontractors to the PII controller.

Control

The use of subcontractors by the PII processor to process PII should be disclosed to the PII controller prior to any such use.

Implementation guidance for the protection of PII

Provisions for the use of subcontractors to process PII should be specified in the contract between the PII processor and the PII controller. The contract should specify that subcontractors may only be commissioned with the prior authorization of the PII controller. The PII processor should inform the PII controller in a timely fashion of any intended changes in this regard, so that the PII controller has the ability to object to such changes or to terminate the consent.

Information disclosed should cover the fact that subcontracting is used and the names of relevant subcontractors, but not any business-specific details. The information disclosed should also include the countries in which subcontractors may process data and the means by which subcontractors are obliged to meet or exceed the obligations of the PII processor.

Where public disclosure of subcontractor information is assessed to increase security risk beyond acceptable limits, disclosure should be made under a non-disclosure agreement or on the request of the PII controller. The PII controller should be made aware that information about subcontractors being used is available.

A.8 Accuracy and quality

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

Control

Organizations should implement appropriate measures to ensure that PII collected from a PII principal, either directly or indirectly, is of appropriate quality.

Implementation guidance for the protection of PII

Achieving data quality means that the PII being processed is accurate, of adequate precision, complete, up-to-date, adequate and relevant for the purpose of use.

Organizations should:

a) establish PII collection procedures to help ensure accuracy and quality;

b) collect PII in a manner that any modifications are detectible after it has left the authoritative source;

c) confirm to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of the PII;

d) ensure the reliability of PII collected from a source other than from the PII principal before it is processed;

e) verify, through appropriate means, the validity and correctness of the requests for correction made by the PII principal prior to making any changes to the PII, where it is appropriate to do so;

f) periodically check for, and correct as necessary, any inaccurate or outdated PII used by its programmes or systems; and

g) issue guidelines ensuring and maximizing the accuracy, completeness, adequacy and relevance of disseminated information. 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 the 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 should incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be updated.

To minimize the scope for data inaccuracy, to the extent possible, PII should be entered into information systems directly by the PII principal without the need for another person to transcribe the data. However, in the event that transcription of