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

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.

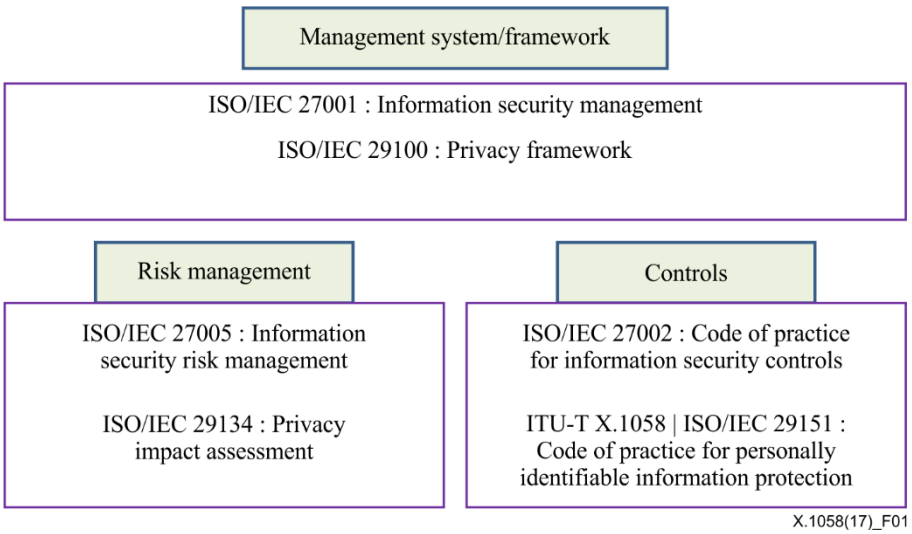

Figure 1 – The relationship of this Specification and the family of ISO/IEC standards

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.