International Standard

ISO/IEC 29151

Second edition
2026-07

Information security, cybersecurity and privacy protection — Controls, requirements, and guidance for personally identifiable information protection

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité, exigences et recommandations pour la protection des données à caractère personnel

Reference number
ISO/IEC 29151:2026(en)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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.

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.

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by ITU as X.1058 (2025) and drafted in accordance with its editorial rules, in collaboration with Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*, and in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/CLC/JTC 13, *Cybersecurity and Data Protection*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This second edition cancels and replaces the first edition (ISO/IEC 29151:2017), which has been technically revised.

The main changes are as follows:

— the content of the guidance for security controls in the main text and the privacy controls in Annex A have been aligned with ISO/IEC 27002:2022.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

INTERNATIONAL STANDARD ISO/IEC 29151
RECOMMENDATION ITU-T X.1058

Information security, cybersecurity and privacy protection – Controls, requirements and guidance for personally identifiable information protection

Summary

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.

Recommendation ITU-T X.1058 | International Standard ISO/IEC 29151 specifies controls, purpose and guidance for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of PII. In particular, this Specification specifies requirements and guidance based on ISO/IEC 27002, taking into consideration the controls for processing PII that can be applicable within the context of an organization's information security risk environment(s).

History*

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1058	2017-03-30	17	11.1002/1000/13182
2.0	ITU-T X.1058	2026-02-06	17	11.1002/1000/16527

Keywords

Control, guidance, protection of PII, requirements.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, and information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at https://www.itu.int/ITU-T/ipr/.

CONTENTS

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. Other International Standards that provide guidance or requirements on other aspects of the overall process of protecting PII are as follows:

- ISO/IEC 27001 specifies an information security management system, which is a suitable foundation for protecting any information, including PII.
- ISO/IEC 27002 provides guidelines for organizational, people-related, physical and technological information security controls that can be used for the protection of all kinds of information, including PII.
- ISO/IEC 27005 provides guidance to assist organizations to address information security risks and perform information security risk management activities, specifically information security risk assessment and treatment.
- ISO/IEC 27018 offers guidance to organizations acting as PII processors when offering processing capabilities as cloud services.
- ISO/IEC 27701 specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS).
- ISO/IEC 29100 provides a privacy framework which: specifies a common privacy terminology, defines the actors and their roles in processing personally identifiable information (PII), describes privacy safeguarding considerations, and provides references to known privacy principles for information technology.
- ISO/IEC 29134 provides guidelines for assessing the potential impacts on privacy of a process, information system, programme, software module, device or other initiative which processes personally identifiable information (PII), while ISO/IEC 27001 together with ISO/IEC 27005 provide guidance to perform information security risk management activities.

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

This Specification contains two parts:

- the main body consisting of clauses 1 to 8;
- Annexes A and B.

The structure of this Specification, including the clause titles, reflects the main body of ISO/IEC 27002:2022 for the development of PII-specific extensions.

The title of the subclauses in clauses 5 to 8 mirror those of ISO/IEC 27002:2022, reflecting the fact that this document builds on the guidance in ISO/IEC 27002:2022, adding new controls specific to the protection of PII. Many of the controls in ISO/IEC 27002:2022 do not require 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 27002:2022.

Annex A contains an extended set of PII protection-specific controls. These new PII protection controls, with their associated guidance, are divided into twelve categories, corresponding to the privacy policy and the eleven 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 other International Standards.

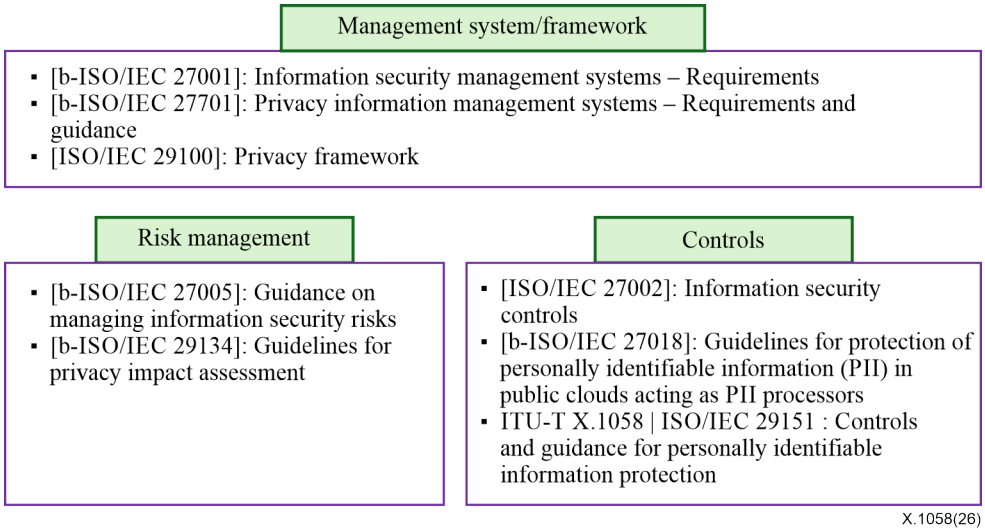

Figure 1 – Relationship between this Specification and other International Standards

This Specification includes guidance based on ISO/IEC 27002. The guidance is adapted as necessary to address the privacy needs 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 can be considered PII in some jurisdictions),
   – within an organization's own processing infrastructure,
   – on a third party's processing platform;
c) for the collection type 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).

Ongoing data collection can contain or yield behavioural, locational and other types of PII. In such cases, it is recommended to use PII protection controls that allow:

– access and collection to be managed based on consent, and
– the PII principal to exercise appropriate control over such access and collection.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information security, cybersecurity and privacy protection – Controls, requirements and guidance for personally identifiable information protection

1 Scope

This Recommendation | International Standard specifies controls, purpose, and guidance 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 requirements and guidance based on ISO/IEC 27002, taking into consideration the controls for processing PII that can 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, in particular, organizations that do not establish or operate a privacy information management system.

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 27002:2022, *Information security, cybersecurity and privacy protection – Information security controls*.
– ISO/IEC 29100:2024, *Information technology – Security techniques – Privacy framework*.

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this Recommendation | International Standard, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27002, ISO/IEC 29100 and the following apply.

ITU, ISO and IEC maintain terminology databases for use in standardization at the following addresses:

– ITU Terms and Definitions at https://www.itu.int/myworkspace/terminology
– ISO Online browsing platform: available at https://www.iso.org/obp
– IEC Electropedia: available at https://www.electropedia.org/

3.1.1 chief privacy officer (CPO): Senior management individual who is accountable for the protection of *personally identifiable information (PII)* (3.1.4) in an *organization* (3.1.3).

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

3.1.3 organization: Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.

NOTE – The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

3.1.4 personally identifiable information (PII): Information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or might be directly or indirectly linked to a natural person.

NOTE – The "natural person" in the definition is the PII principal (3.1.6). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

[SOURCE: ISO/IEC 29100, 3.7]

3.1.5 personally identifiable information controller (PII controller): Privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information (PII)* (3.1.4) other than natural persons who use data for personal purposes.

NOTE – A PII controller sometimes instructs others [e.g., *PII processors* (3.1.7)] to process PII on its behalf while the responsibility for the processing remains with the PII controller.

[SOURCE: ISO/IEC 29100, 3.8]

3.1.6 personally identifiable information principal data subject (PII principal): Natural person to whom the *personally identifiable information (PII)* (3.1.4) relates.

[SOURCE: ISO/IEC 29100, 3.9]

3.1.7 personally identifiable information processor (PII processor): Privacy stakeholder that processes *personally identifiable information (PII)* (3.1.4) on behalf of and in accordance with the instructions of a *PII controller* (3.1.5).

[SOURCE: ISO/IEC 29100, 3.10]

3.1.8 privacy risk assessment, privacy impact assessment: Overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of *personally identifiable information* (3.1.4), framed within an organization's broader risk management framework.

[SOURCE: ISO/IEC 29100, 3.18]

3.2 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

CPO Chief Privacy Officer

PIA Privacy Impact Assessment

PII Personally Identifiable Information

4 Overview

4.1 Protection of PII

This Recommendation | International Standard provides a set of controls for PII protection. The objective of the controls for protection of PII is to enable organizations to put in place a set of controls as part of their overall PII protection programme. Controls can be used in a framework for demonstrating 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 clauses in ISO/IEC 29100.

4.2 Requirement for the protection of PII

An organization should identify its PII protection requirements. ISO/IEC 29100 can be applied to identify PII protection requirements. There are four main factors that apply to PII protection requirements:

- legal and regulatory factors for the safeguarding of the PII principal's privacy and the protection of their PII;
- contractual factors, such as agreements between and among several different actors, company policies and binding corporate rules;
- risk assessment factors, including privacy risk assessment, which covers external and internal context which can be determined through business strategy and objectives; and
- corporate policies: an organization can also choose voluntarily to go beyond the criteria that are derived from previous requirements.

PII protection controls (including information security controls) should be selected on the basis of a risk assessment. The results of a privacy impact assessment (PIA) as specified in ISO/IEC 29134 can help determine, prioritize and implement the appropriate controls for managing risks to the protection of PII and for implementing controls selected to protect against these risks.

A PIA document as defined in ISO/IEC 29134 provides PIA guidance, including advice on privacy risk assessment, privacy risk treatment plan, privacy risk acceptance and privacy risk review.

4.3 Controls derived from privacy risk assessment

Privacy risk assessment helps organizations protect the confidentiality, integrity and availability of PII. Data breach can cause significant harm to both organizations and individuals. Organizations should identify and implement controls to treat the risks identified by the risk impact process. Privacy risk assessment report should describe at least system requirements, system design and operational plans and procedures. ISO/IEC 29134 provides information on what should be documented in a privacy risk assessment.

NOTE – Some jurisdictions require privacy risk assessments depending on the level of the risk of PII processing, the nature of the organization (e.g., government agencies), etc.

4.4 Selecting controls

Controls can be selected from this Specification, including 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.

NOTE – Legal requirements can also apply for selection of controls.

Organizations shall consider the extended control set for PII protection in Annex A for selecting controls to implement the privacy risk treatment option(s) chosen.

The selection and implementation of controls is also dependent upon the organization's role in the provision of infrastructure or services. Many different organizations are 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 apply the controls in this Specification according to 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 according to 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 8, along with implementation guidance. Implementation can be simpler if requirements for the protection of PII have been considered in the design of the organization's information systems, 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 Recommendation | International Standard can be regarded as a starting point for developing organization specific guidelines. Not all the controls and guidance in this Specification are applicable to all organizations.

Furthermore, additional controls and guidelines not included in this Recommendation | International Standard can be required. When other Specifications are developed containing additional guidelines or controls, it can be useful to include cross-references to the clauses in this Specification, where applicable, to facilitate compliance checking for auditors and business partners.

4.6 Life cycle considerations

PII has a natural life cycle, from creation or origination, collection, through to 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 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 information 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.