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)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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.

© ISO/IEC 2026 – All rights reserved

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.

© ISO/IEC 2026 – All rights reserved

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/.

© ITU 2026

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

			Page
1	Scope		1
2	Normative references		1
3	Terms, definitions and abbreviated terms		1
	3.1	Terms and definitions	1
	3.2	Abbreviated terms	2
4	Overview		2
	4.1	Protection of PII	2
	4.2	Requirement for the protection of PII	2
	4.3	Controls derived from privacy risk assessment	3
	4.4	Selecting controls	3
	4.5	Developing organization specific guidelines	3
	4.6	Life cycle considerations	3
	4.7	Structure of this Specification	4
5	Organizational controls		8
	5.1	Policies for information security	8
	5.2	Information security roles and responsibilities	8
	5.3	Segregation of duties	8
	5.4	Management responsibilities	9
	5.5	Contact with authorities	9
	5.6	Contact with special interest groups	9
	5.7	Threat intelligence	9
	5.8	Information security in project management	9
	5.9	Inventory of information and other associated assets	9
	5.10	Acceptable use of information and other associated assets	10
	5.11	Return of assets	10
	5.12	Classification of information	10
	5.13	Labelling of information	10
	5.14	Information transfer	10
	5.15	Access control	11
	5.16	Identity management	11
	5.17	Authentication information	11
	5.18	Access rights	11
	5.19	Information security in supplier relationships	11
	5.20	Addressing information security within supplier agreements	11
	5.21	Managing information security in the ICT supply chain	12
	5.22	Monitoring, review and change management of supplier services	12
	5.23	Information security for use of cloud services	12
	5.24	Information security incident management planning and preparation	12
	5.25	Assessment and decision on information security events	13
	5.26	Response to information security incidents	13
	5.27	Learning from information security incidents	13
	5.28	Collection of evidence	13

© ISO/IEC 2026 – All rights reserved

5.29 Information security during disruption ... 13
5.30 ICT readiness for business continuity ... 13
5.31 Legal, statutory, regulatory and contractual requirements ... 13
5.32 Intellectual property rights ... 14
5.33 Protection of records ... 14
5.34 Privacy and protection of PII ... 14
5.35 Independent review of information security ... 14
5.36 Conformance with policies, rules and standards for information security ... 14
5.37 Documented operating procedures ... 14
6 People controls ... 15
6.1 Screening ... 15
6.2 Terms and conditions of employment ... 15
6.3 Information security awareness, education and training ... 15
6.4 Disciplinary process ... 15
6.5 Responsibilities after termination or change of employment ... 15
6.6 Confidentiality or non-disclosure agreements ... 15
6.7 Remote working ... 15
6.8 Information security event reporting ... 15
7 Physical controls ... 16
7.1 Physical security perimeters ... 16
7.2 Physical entry ... 16
7.3 Securing offices, rooms and facilities ... 16
7.4 Physical security monitoring ... 16
7.5 Protecting against physical and environmental threats ... 16
7.6 Working in secure areas ... 16
7.7 Clear desk and clear screen ... 16
7.8 Equipment siting and protection ... 16
7.9 Security of assets off-premises ... 16
7.10 Storage media ... 16
7.11 Supporting utilities ... 16
7.12 Cabling security ... 17
7.13 Equipment maintenance ... 17
7.14 Secure disposal or re-use of equipment ... 17
8 Technological controls ... 17
8.1 User endpoint devices ... 17
8.2 Privileged access rights ... 17
8.3 Information access restriction ... 17
8.4 Access to source code ... 17
8.5 Secure authentication ... 18
8.6 Capacity management ... 18
8.7 Protection against malware ... 18
8.8 Management of technical vulnerabilities ... 18
8.9 Configuration management ... 18
8.10 Information deletion ... 18
8.11 Data masking ... 18
8.12 Data leakage prevention ... 18

© ISO/IEC 2026 – All rights reserved

8.13 Information backup 18
8.14 Redundancy of information processing facilities 18
8.15 Logging 18
8.16 Monitoring activities 19
8.17 Clock synchronization 19
8.18 Use of privileged utility programs 19
8.19 Installation of software on operational systems 19
8.20 Networks security 19
8.21 Security of network services 19
8.22 Segregation of networks 19
8.23 Web filtering 19
8.24 Use of cryptography 19
8.25 Secure development life cycle 19
8.26 Application security requirements 19
8.27 Secure system architecture and engineering principles 19
8.28 Secure coding 19
8.29 Security testing in development and acceptance 20
8.30 Outsourced development 20
8.31 Separation of development, test and production environments 20
8.32 Change management 20
8.33 Test information 20
Annex A (normative) – Extended control set for PII protection 21
A.1 General 21
A.2 General policies for the use and protection of PII 21
A.3 Consent and choice 21
A.4 Purpose legitimacy and specification 23
A.5 Collection limitation 25
A.6 Data minimization 25
A.7 Use, retention and disclosure limitation 26
A.8 Accuracy and quality 29
A.9 Openness, transparency and notice 30
A.10 PII principal participation and access 31
A.11 Accountability 33
A.12 Information security 36
A.13 Privacy compliance 36
Annex B (informative) – Correspondence between this Specification and ISO/IEC 29151:2017 38
Bibliography 41

© ISO/IEC 2026 – All rights reserved

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;

© ISO/IEC 2026 – All rights reserved

– individual participation and access;
– accountability;
– information security; and
– privacy compliance.

Figure 1 describes the relationship between this Specification and other International Standards.

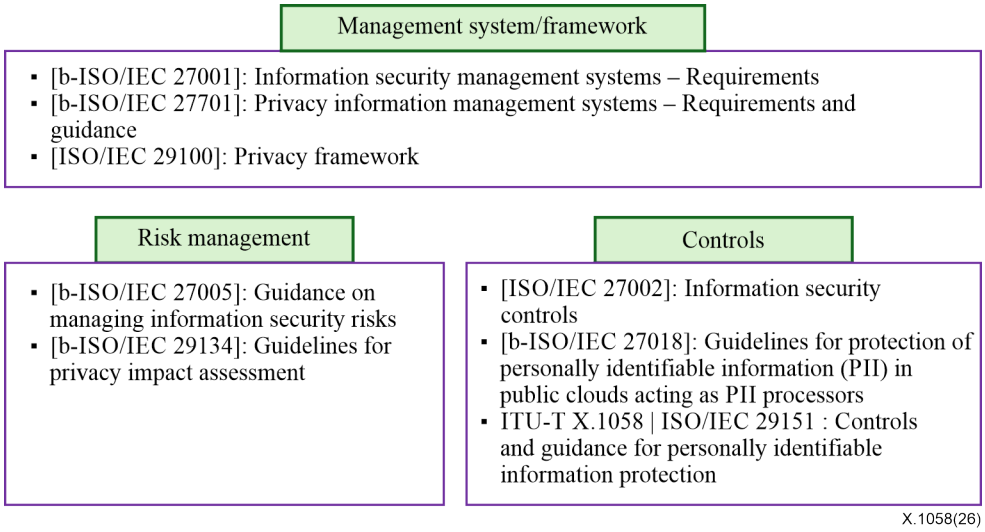


Figure 1 – Relationship between this Specification and other International Standards

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).

© ISO/IEC 2026 – All rights reserved

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.

© ISO/IEC 2026 – All rights reserved

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.

© ISO/IEC 2026 – All rights reserved