

**Information technology - Security techniques - Code  
of practice for personally identifiable information  
protection (ISO/IEC 29151:2017)**

## EESTI STANDARDI EESSÕNA

## NATIONAL FOREWORD

See Eesti standard EVS-EN ISO/IEC 29151:2022 sisaldab Euroopa standardi EN ISO/IEC 29151:2022 ingliskeelset teksti.	This Estonian standard EVS-EN ISO/IEC 29151:2022 consists of the English text of the European standard EN ISO/IEC 29151:2022.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 06.04.2022.	Date of Availability of the European standard is 06.04.2022.
Standard on kättesaadav Eesti Standardimis- ja Akrediteerimiskeskusest.	The standard is available from the Estonian Centre for Standardisation and Accreditation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile [standardiosakond@evs.ee](mailto:standardiosakond@evs.ee).

ICS 75.200

**Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardimis- ja Akrediteerimiskeskusele**

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardimis- ja Akrediteerimiskeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autoriõiguse kaitse kohta, võtke palun ühendust Eesti Standardimis- ja Akrediteerimiskeskusega: Koduleht [www.evs.ee](http://www.evs.ee); telefon 605 5050; e-post [info@evs.ee](mailto:info@evs.ee)

**The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation and Accreditation**

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation and Accreditation.

If you have any questions about standards copyright protection, please contact the Estonian Centre for Standardisation and Accreditation: Homepage [www.evs.ee](http://www.evs.ee); phone +372 605 5050; e-mail [info@evs.ee](mailto:info@evs.ee)

English version

**Information technology - Security techniques - Code of  
practice for personally identifiable information protection  
(ISO/IEC 29151:2017)**

Technologies de l'information - Techniques de sécurité  
- Code de bonne pratique pour la protection des  
données à caractère personnel (ISO/IEC 29151:2017)

Informationstechnik - Sicherheitsverfahren - Leitfaden  
für den Schutz personenbezogener Daten (ISO/IEC  
29151:2017)

This European Standard was approved by CEN on 27 March 2022.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



**CEN-CENELEC Management Centre:  
Rue de la Science 23, B-1040 Brussels**

## European foreword

The text of ISO/IEC 29151:2017 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 29151:2022 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by October 2022, and conflicting national standards shall be withdrawn at the latest by October 2022.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

## Endorsement notice

The text of ISO/IEC 29151:2017 has been approved by CEN-CENELEC as EN ISO/IEC 29151:2022 without any modification.

## CONTENTS

	<i>Page</i>
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

	<i>Page</i>
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](http://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](http://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](http://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.

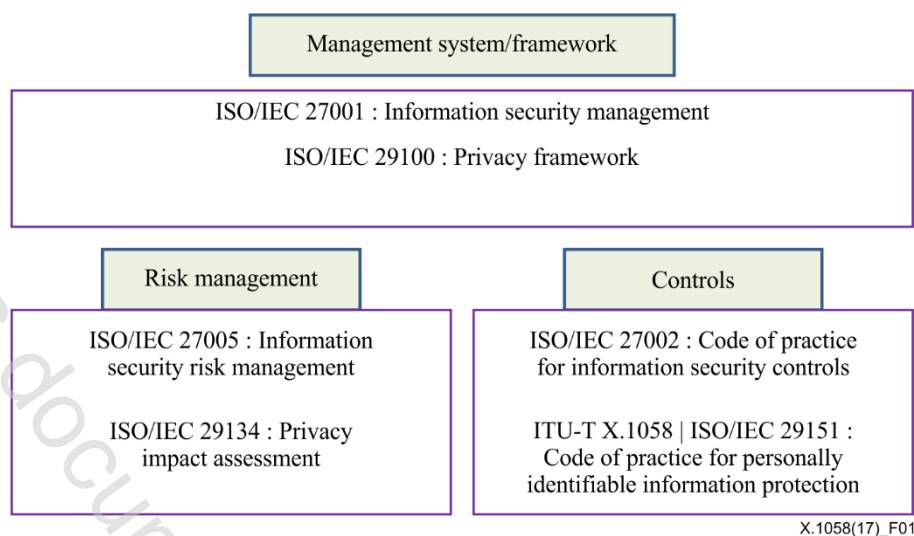
The structure of the main body of this Specification, including the clause titles, reflects the main body of ISO/IEC 27002. The introduction and clauses 1 to 4 provide background on the use of this Specification. Headings for clauses 5 to 18 mirror those of ISO/IEC 27002, reflecting the fact that this 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.

# 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