

Information technology - Online privacy notices and consent (ISO/IEC 29184:2020)

## EESTI STANDARDI EESSÕNA

## NATIONAL FOREWORD

See Eesti standard EVS-EN ISO/IEC 29184:2023 sisaldab Euroopa standardi EN ISO/IEC 29184:2023 ingliskeelset teksti.	This Estonian standard EVS-EN ISO/IEC 29184:2023 consists of the English text of the European standard EN ISO/IEC 29184:2023.
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 05.04.2023.	Date of Availability of the European standard is 05.04.2023.
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 35.030

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 autorikaitse 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 copyright, please contact 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 - Online privacy notices and consent (ISO/IEC 29184:2020)

Technologies de l'information - Déclarations de confidentialité en ligne et les consentements (ISO/IEC 29184:2020)

Informationstechnologie - Online-Datenschutzerklärung und Einwilligung (ISO/IEC 29184:2020)

This European Standard was approved by CEN on 24 March 2023.

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, Türkiye and United Kingdom.



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

## European foreword

The text of ISO/IEC 29184:2020 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 29184:2023 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 2023, and conflicting national standards shall be withdrawn at the latest by October 2023.

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, Türkiye and the United Kingdom.

## Endorsement notice

The text of ISO/IEC 29184:2020 has been approved by CEN-CENELEC as EN ISO/IEC 29184:2023 without any modification.

# Contents

Page

<b>Foreword</b>	<b>v</b>
<b>Introduction</b>	<b>vi</b>
<b>1 Scope</b>	<b>1</b>
<b>2 Normative references</b>	<b>1</b>
<b>3 Terms and definitions</b>	<b>1</b>
<b>4 Symbols and abbreviated terms</b>	<b>2</b>
<b>5 General requirements and recommendations</b>	<b>2</b>
5.1 Overall objective	2
5.2 Notice	2
5.2.1 General	2
5.2.2 Providing notice obligation	2
5.2.3 Appropriate expression	3
5.2.4 Multi-lingual notice	3
5.2.5 Appropriate timing	3
5.2.6 Appropriate locations	4
5.2.7 Appropriate form	4
5.2.8 Ongoing reference	5
5.2.9 Accessibility	5
5.3 Contents of notice	5
5.3.1 General	5
5.3.2 Purpose description	5
5.3.3 Presentation of purpose description	6
5.3.4 Identification of the PII controller	6
5.3.5 PII collection	6
5.3.6 Collection method	7
5.3.7 Timing and location of the PII collection	7
5.3.8 Method of use	8
5.3.9 Geo-location of, and legal jurisdiction over, stored PII	8
5.3.10 Third-party transfer	8
5.3.11 Retention period	9
5.3.12 Participation of PII principal	9
5.3.13 Inquiry and complaint	9
5.3.14 Information about accessing the choices made for consent	10
5.3.15 Basis for processing	10
5.3.16 Risks	10
5.4 Consent	11
5.4.1 General	11
5.4.2 Identification of whether consent is appropriate	11
5.4.3 Informed and freely given consent	11
5.4.4 Providing the information about which account the PII principal is using	12
5.4.5 Independence from other consent	12
5.4.6 Separate consent to necessary and optional elements of PII	13
5.4.7 Frequency	13
5.4.8 Timeliness	13
5.5 Change of conditions	13
5.5.1 General	13
5.5.2 Renewing notice	14
5.5.3 Renewing consent	14
<b>Annex A (informative) User interface example for obtaining the consent of a PII principal on PCs and smartphones</b>	<b>16</b>
<b>Annex B (informative) Example of a consent receipt or consent record (NOTE in 5.4.3)</b>	<b>22</b>

**Bibliography** .....25

This document is a preview generated by EVS

## 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. 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)) or the IEC list of patent declarations received (see <http://patents.iec.ch>).

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](http://www.iso.org/iso/foreword.html).

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

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](http://www.iso.org/members.html).

## Introduction

The wider availability of communication infrastructures like home broadband connections and the global internet, the growth in the use of smartphones and other devices (e.g., wearables) that collect details of individuals' activities, and improvements in information processing capability have enabled much wider-ranging collection and analysis of personal information. Such technological improvements provide a better prospect for more convenient consumer life, new business opportunities, more attractive services and more added value. On the other hand, consumers are becoming increasingly "privacy aware" and are questioning the privacy impact of the collection and use of personally identifiable information (PII) by online services. This criticism is often due to the lack of a clear explanation of how their PII is processed, stored, maintained and managed.

This document specifies controls and associated additional information for organizations:

- to provide the basis for presenting clear, easily understood information to individuals whose PII is collected, about how the organization processes their PII (e.g., when providing services to consumers or under an employment relationship) and
- to obtain consent from the PII principals in a fair, demonstrable, transparent, unambiguous and revocable (withdrawable) manner.

This document provides details on the implementation of two privacy principles from ISO/IEC 29100 (i.e., Principle 1: Consent and choice, Principle 7: Openness, transparency and notice).

# Information technology — Online privacy notices and consent

## 1 Scope

This document specifies controls which shape the content and the structure of online privacy notices as well as the process of asking for consent to collect and process personally identifiable information (PII) from PII principals.

This document is applicable in any online context where a PII controller or any other entity processing PII informs PII principals of processing.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 29100 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

### 3.1

#### **explicit consent**

personally identifiable information (PII) principal's freely given, specific and informed unambiguous agreement to the processing of their PII exercised through an affirmative act indicating such consent by the PII principal

Note 1 to entry: Explicit consent is the result of an opt-in.

Note 2 to entry: Explicit consent can also be referred to as express consent.

EXAMPLE Consent is obtained by asking the PII principal to take a specific action in the context of a notice.

[SOURCE: ISO/IEC 29100:2011, 2.4, modified – The words "exercised through an affirmative act indicating such consent by the PII principal" have been added.]

### 3.2

#### **notice**

information regarding processing of PII

Note 1 to entry: Given to the PII principals through different channels, in a concise, transparent, intelligible and easily accessible form and using clear and plain language.