FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
29184**

ISO/IEC JTC **1**/SC **27**

Secretariat: DIN

Voting begins on:
2020-03-18

Voting terminates on:
2020-05-13

Information technology — Online privacy notices and consent

Technologies de l'information — Déclarations de confidentialité en ligne et les consentements

Reference number
ISO/IEC FDIS 29184:2020(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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 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 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.

This document was prepared by 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.

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.

3.3
element of PII
category of PII
piece of PII
descriptor for a type of information, or a set of types of information

4 Symbols and abbreviated terms

JSON	JavaScript object notation
PC	personal computer
PII	personally identifiable information
XML	extensible markup language

5 General requirements and recommendations

5.1 Overall objective

The overall objective of the standard is to allow PII Principals to understand and act in accordance with the implications of PII processing, such as the likelihood and severity of any potential impact the processing can have, as well as the direct and/or intended consequences of the processing.

Organizations that wish to demonstrate compliance with this document shall document for each control of Clause 5:

a) whether the control applies;

b) when there are reasons that can justify that the control does not apply, that the justification is documented and validated;

c) how the implementation of the control is verified and validated.

5.2 Notice

5.2.1 General

Objective: To provide notice where it is required, in a language appropriate to PII principals, at a time that permits PII principals to meaningfully exercise consent, at places where it is easy for PII principals to recognize, and with references that provide PII principals with access to supplementary material, including prior notices and their responses.

5.2.2 Providing notice obligation

Control

The organization shall identify situations where providing notice is necessary and shall provide notice that complies with 5.3 to PII principals whenever it is required.

Additional information

The notice should provide all interested parties, including outsiders to the organization, with the organization's privacy practices, as well as other relevant information such as contact details including the identity and registered address of the PII controller, and contact points from which PII principals can obtain additional information (see Annex A).

Displaying a visual notice is one way to provide notice. For accessibility, either screen readers for visual notices or directly audible notices can be appropriate to assist those who are visually impaired. Other forms of notice can also be appropriate (see 5.2.9).

The organization should provide a notice to PII principals. Notice may be required, among other situations, when the organization plans to collect new PII (from the PII principal or from another source) or when it plans to use PII already collected for new purposes.

5.2.3 Appropriate expression

Control

The organization shall provide the notice in a way that is clear and easy to understand for the targeted PII principals. The notice shall be easily legible and in a concise language that a person without any legal or technical training can reasonably comprehend.

Additional information

The notice should be drafted taking into account particular categories or types of PII principals (e.g. disadvantaged societal sub-groups).

5.2.4 Multi-lingual notice

Control

The organization shall provide the notice in the language(s) according to the target principal's language expectations.

Additional information

For example, the organization may present the PII principal with a list of supported languages displayed in the respective languages and allow the PII principal to choose the language. Displaying the name of each language in that language is important, as the PII principal may not be able to recognize it if it is shown in another language.

A web browser has a preference setting for a preferred language, and it may be used for this purpose. However, it may not be a good idea to solely depend on the browser's language preference since the PII principal can be using a shared computer.

5.2.5 Appropriate timing

Control

The organization shall determine and document the appropriate timing (e.g. immediately prior to collecting the PII) for providing notice to the PII principals when the activity in question is relevant to the privacy interests of the PII principals.

Additional information

When an organization provides a PII principal with a notice and then collects the PII at a later point in time, including cases in which data are collected from another source, the timing of the notice and the collection of PII can differ significantly.

The organization should provide notice where the use of PII can have unexpected or significant effects on PII principals. If an organization intends to collect additional PII, it should provide a further notice.

5.2.6 Appropriate locations

Control

The organization shall provide notices in a manner appropriate to the product or service in question so that PII principals can find and access the notices electronically and easily, including at online locations.

Additional information

Appropriate online locations can include, but are not limited to, links on the organization's home pages on its websites or on the landing page, the start-up page of mobile apps, online forms or in captive portals.

In some cases, PII may be processed without prior interaction with the PII principal. From the point of view of the PII principals, it would actually be quite hard to even find out who is processing their data and, thus, it does not help to post the privacy notice only on the organization's website. It is useful to have a place where a PII principal can go and obtain the privacy notices of such organizations. Thus, where applicable and feasible, the organization should consider using a publicly accessible common repository where stakeholders can easily find and access the relevant notices.

5.2.7 Appropriate form

Control

The organization shall determine how the notice is provided and made accessible with respect to the timing of processing.

Additional information

The organization may implement the control using different techniques: layered notices, dashboards, just-in-time notices and icons, and may provide notices in a machine-readable format so that the software which is presenting it to the PII principal can parse it to optimize the user interface and help PII principals make decisions.

If the organization implements the control using a layered notice, the first layer should detail anything unexpected or things that can significantly impact a PII principal, with that impact determined in the assessment described in 5.3.3. The other layers should provide notice of all collection and/or processing activities in order to give the PII principal detailed information of these activities.

Organizations should display the first layer of each notice such that PII principals are able to read it as quickly as possible. It should not span more than a few screens. Given the volume constraints, it may not be possible to display all the contents on one screen. In that case, organizations should display the summary first. In the context of mobile devices and smartphones, for better readability, it would be useful to introduce a "multilayer approach" to notice and consent, showing a short text, with key information and with a link to the "full text" notice/consent.

When organizations display elements of PII to be collected, they should display them by groups with those having the highest potential privacy impact being listed first so that PII principals can clearly recognize the differences.

Organizations should make content, including relevant information omitted from the first or subsequent screens, available for reference by PII principals if they wish.

NOTE In the case of online notification, pop-ups and drill-downs can be used to display content. PII principals can have difficulty in reading a large amount of terms and conditions in a contract, especially when they are about to take a certain action.

Machine-readable notices may be provided in a standardized XML or JSON format. By doing so, it becomes possible for devices to select items appropriately and display graphics and icons where applicable. However, organizations need to note that the PII principal's interpretation of graphical

representation can differ significantly depending on cultural backgrounds. Guidance for the region or culture in question may be created in order to prevent PII principals from getting confused.

5.2.8 Ongoing reference

Control

The organization shall keep and make available the version of the notice presented when the PII principal gave consent, as well as the most recent relevant version for easy reference by that PII principal.

Additional information

Versions of notices should be retained for as long as they are associated with retained PII.

5.2.9 Accessibility

Control

The organization shall provide a notice in an accessible manner that is appropriate to the technologies underlying the online service.

Additional information

Particularly in cases where individuals with accessibility issues are expected to access notices, the notices should enable them to understand the content of the notices. This can involve the need to ensure that the text of the notice can be converted to sound for those individuals with visual issues.

Guidelines such as ISO/IEC 40500 help in designing accessibility.

5.3 Contents of notice

5.3.1 General

Objective: To ensure that the PII principal has sufficient information within the notice to understand how the PII is being processed and what rights the PII principal has.

5.3.2 Purpose description

Control

The organization shall ensure that the notice includes information about the purpose(s) for which the PII will be processed.

Additional information

It is important for PII principals to understand the purposes for the processing of the PII collected so that they can provide meaningful consent. For brevity of the notice, a name or short phrase for each purpose may be used, but it should be possible (e.g. via a hyperlink) to associate that name or phrase with an overview of the purpose sufficient for PII principals to provide meaningful consent.

Care needs to be taken when drafting notices, as the inclusion of too much detail can result in the need to reissue them at frequent intervals.