INTERNATIONAL STANDARD

ISO/IEC 29184

First edition
2020-06

Information technology — Online privacy notices and consent

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

Reference number
ISO/IEC 29184:2020(E)

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) 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).

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) 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.

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.

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 this document 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.

5.3.3 Presentation of purpose description

Control

The organization shall specify the purposes related to the collection of each element of PII and appropriate information about the plausible risk of the processing, in an order according to the general assessment of the risk.

NOTE The impact and risk are necessarily obvious.

Additional information

The organization explains how PII will be used in a manner that allows the PII principal to clearly and readily understand the purpose. If the purpose of the use varies among the elements of PII being collected, the organization should clearly mark which purpose applies to which element of PII.

5.3.4 Identification of the PII controller

Control

The organization shall provide the PII principal with the relevant information (e.g. the identity and contact details) about the PII controller.

Additional information

Identification of the PII controller is typically by company name, but can also involve the displaying of company number, head office/operational address and (if appropriate) departmental information.

5.3.5 PII collection

Control

The organization shall provide information that allows PII principals to understand what elements of PII are being collected, even where the collection of the particular elements of PII is obvious.

Additional information

In addition to using generic language such as "We collect your personal information." where appropriate based on the impact determined in the assessment described in 5.3.3, the organization should provide the list of specific elements of PII that are collected (e.g. "We collect your name, address, and telephone number.") even if it is obvious what the collected information is.

To identify what would count as the PII to be listed in the notice, the organization should consult ISO/IEC 29100:2011, 4.4.

The organization should present the actual value of an element of PII to be collected at the time of collection where it is relevant, feasible and practical. Where it is not feasible to do so, the organization may provide a clear example of the element values being collected with the associated name of an element of PII. By doing so, the PII principal can understand what is referred to by the name of an element of PII and what kind of values are going to be collected.

EXAMPLE Instead of referring to "telephone number" organization can state "telephone number (01-234-5678)"

Where the PII controller collects the PII from the PII principal through their devices or identity provider, the actual value can be shown to the PII principal with the notice before being transferred to the PII controller (see A.2.3 for such examples). Showing actual values of elements of PII helps the PII principals to determine if they want to provide them to the PII controller, especially in cases where there are multiple elements of the same type. For example, for a phone number, the PII principal can agree to provide their work telephone number but not their personal mobile number.

Care should be taken to lessen the risk of PII leak through shoulder surfing, etc. Techniques such as masking and drill down should be considered.

If new PII is generated through some kind of processing of PII, showing the actual value before the consent is impossible. In such cases, providing an example value can be desirable. For example, when purchase data from a shop is to be provided, and the PII principal does not have a purchase at the time of consent, there is no actual data available for display. In such a case, it can be desirable to obtain the understanding of the PII principal by showing example purchase data and informing the PII principal what kind of data is going to be collected.

5.3.6 Collection method

Control

The organization shall provide PII principals with clear explanations of the collection methods being used, along with information about any risks associated with particular collection methods.

Additional information

PII can be collected in different ways. For example, PII can be:

a) directly collected from the PII principal, e.g. through a web form;

b) indirectly collected, e.g. from a third party, such as a credit agency;

c) observed by the PII controller, e.g. observing browser fingerprint and accessed web pages;

d) inferred by the PII controller, e.g. profiling the PII principal by analysing the data collected through the methods a) to c).

Based on the impact determined in the assessment described in 5.3.3, if the collection methods are different depending on the element of PII, the organization should inform the PII principal which collection method is applied to each element of PII. When the same collection method is applied to multiple elements of PII, then elements of PII can be grouped together under each collection method. However, if the privacy impact of one or more elements of PII in the group is markedly higher than others according to a general assessment of impact to the corresponding population of PII principals, then it should be communicated separately so that the PII principal becomes aware of this.

NOTE This is to prevent the "hide a tree in a forest" attack where the attacker buries the high-impact elements of PII in benign ones to trick the PII principal into giving consent.

5.3.7 Timing and location of the PII collection

Control

The organization shall explain in the notice generally when and where the PII is collected, although such notice shall not be required in circumstances where PII collection occurs where and when a PII principal undertakes an action such as the explicit submission of information.

Additional information

If PII is not directly collected, the timing and the location of the PII collection may not be obvious to the PII principal. Including this information in the notice helps the PII principal to understand the situation.

Typically, notices should be provided prior to the PII being collected. For example, where PII is being collected on a web-based form, the top of the form can include the privacy notice (or a summary of the notice with a link to the full notice). A second example where there is collection of PII by CCTV in a public area: a notice that "CCTV is in operation" along with details of the PII controller and contact details should be displayed at the entrance to the area covered by the CCTV.

5.3.8 Method of use

Control

The organization shall include in the notice how the PII will be used.

Additional information

PII can be:

— used as is;

— used after some processing (e.g. derivation, inference, de-identification, or combining with other data);

— combined with other data (e.g. geo-localized, via the use of cookies, from third parties);

— used by automated decision-making techniques (e.g. profiling, classification).

If some processing (e.g. de-identification, aggregation) is applied to the PII before use, it is desirable to state what kinds of transformations are being applied.

5.3.9 Geo-location of, and legal jurisdiction over, stored PII

Control

The organization shall specify the geo-location(s) where PII will be stored and processed, and refer to the legal jurisdiction(s) that govern the handling of the data.

Additional information

The organization should determine the appropriate granularity of geographical location(s) (e.g., country, region) taking into consideration all the privacy safeguarding requirements explained in ISO/IEC 29100:2011, 4.5.

5.3.10 Third-party transfer

Control

The organization shall indicate in the notice if the PII will be transferred to a third party in the ordinary course of business.

NOTE 1 Transfer includes PII disclosure/communication.

Additional information

If an organization will transfer PII to a third party, the notice shall include, directly or indirectly:

— to whom the PII will be transferred;

— the geo-location(s) where the PII will be transferred to, and any changes in legal jurisdiction(s) that can arise;

— for what purpose the PII will be transferred;

— the negative impacts on the PII principal, or risks of such impacts caused by the data transfer; and

— the related safeguard for the transfer (e.g., confidentiality and integrity safeguard).

Although the organization needs to identify and provide notice of individual third-party recipients, it may specify a group of recipients using clearly defined criteria where appropriate.

Criteria as specified in 5.3.10 should be clearly defined as part of a purpose specification category or definition.

NOTE 2 Subclause 5.3.10 only applies to third-party transfers and does not apply to a transfer to a PII processor.

5.3.11 Retention period

Control

The organization shall provide information about the retention period and/or disposal schedule of PII that it is collecting.

Additional information

The information concerning the retention period and/or disposal schedule may be in the form of a specified period (e.g. 5 years) from the date of collection or the occurrence of a specific event, or a specified date (e.g. to be disposed of on 1 January 2025). It can also consist of the criteria used to determine that period or schedule.

NOTE An organization can collect PII for multiple purposes. Depending on the purposes, the retention period can differ. As such, the data retention period can also be specified per purpose.

5.3.12 Participation of PII principal

Control

The organization shall provide information about the PII principal's rights (e.g. access, rectification, deletion, objection, restriction, data portability, withdrawal of consent, etc.) to access their PII, as well as their rights to correct or delete their PII.

Additional information

The notice should include, directly or indirectly, the following aspects of the access:

a) what elements of PII the PII principal can request access to and the means by which the PII principal can make such a request;

b) what information the PII principal has to provide to authenticate themselves to an acceptable level before access to any PII is authorized (to avoid the risk of inappropriate disclosure);

c) the timelines within which a request will be acted on;

d) any fees which may be charged for such access, where the charging of such fees is permitted;

e) the means by which PII principals can challenge the accuracy and completeness of the PII and have it amended as appropriate;

f) the circumstances where information will not be altered or deleted and detailing opportunities to indicate the PII principal's objections regarding the correctness of the PII; and

g) when consent is the legal basis, how it can be revoked if the revocation is feasible or required by relevant legislation.

5.3.13 Inquiry and complaint

Control

The organization shall provide information about the contact details for inquiries regarding the processing of PII stated in the notice and about the right to lodge a complaint with a supervisory authority.

Additional information

Contact information consists of but is not limited to telephone numbers, websites, e-mail addresses and physical locations where inquiries can be directed.

5.3.14 Information about accessing the choices made for consent

Control

The organization shall inform the PII principal of where and how to access preserved evidence of choice exercised initially and as subsequently revised by the PII principal (including revocation), along with the date such choices were made.

Additional information

Choice and consent are distinct concepts. Choice is the action made by the PII principal. Unless the basis on which the PII principal made the choice is informed and fair, the choice does not necessarily entail consent. This control is dealing with choice instead of consent to preserve the objective action of the PII principal.

This may be required for future reference. For example, the PII principal may inquire about it to revise the previously given consent. It may also be required in the event of a dispute.

When the notice or the privacy policy referenced in the notice undergoes significant revision, then all such revisions should be preserved.

Organizations, when obtaining the explicit consent as described in 5.4, should provide notice to PII principals so that PII principals can see the content of their consent by any appropriate means, at any time within reasonable limits appropriate to the mechanism provided.

5.3.15 Basis for processing

Control

The organization shall ensure that the notice includes information about the basis under which the PII will be processed.

Additional information

Consent is one possible basis for processing. Other bases such as performance of a contract may be possible.

5.3.16 Risks

Control

The organization should provide specific information about plausible risks to PII principals, where the impact to privacy and likelihood of occurrence (after mitigations are taken into account) are high or those risks cannot be inferred from other information provided to the PII principal.

Additional information

The information provided in notices should generally be sufficient enough that the PII principal can be reasonably expected to identify potential risks to their privacy. The risk should be explicitly communicated:

— where the organization determines a high risk; or

— if a risk cannot be expected from other information provided by the PII principal (in this case, the PII controller should communicate this risk regardless of the likelihood of occurrence).

For those risks that are specifically communicated to the PII principal, this can be done in a separate section or within the corresponding section (e.g. if the plausible highest risks relate to the purpose of processing and particular data types, it can be communicated within those sections, or it can be communicated in a separate section of the notice specific to risks).

In some cases, it can be preferable to improve the other information provided so the risks can be better inferred from this information, e.g. by being more specific on purpose descriptions or elements of PII processed.

NOTE Residual risk to privacy of a PII principal can determined from a risk assessment or privacy impact assessment.

5.4 Consent

5.4.1 General

Objective: To ensure the organization shall obtain consent from the PII principal when consent is the basis for collection of PII in a manner that is fair, demonstrable, transparent, unambiguous and revocable (withdrawable).

5.4.2 Identification of whether consent is appropriate

Control

The organization shall identify the situations where consent or explicit consent is appropriate and shall request consent from PII principals in these situations.

Additional information

Explicit consent may be required, among other things:

— when the organization plans to collect sensitive PII;

— when the organization plans to use sensitive PII already collected for new purposes;

— if the collection or new purposes cause or indicate a particularly high negative impact on the PII principal or a particularly high risk of such an impact.

The organization can be required to obtain consent concerning its PII collection from PII principals by relevant data protection/privacy legislation. Consent can be required, among other things, when the organization plans to collect new PII or when it plans to use PII already collected for new purposes.

Consent is not the only lawful basis for the processing of PII and, thus, not always required. In some jurisdictions, other lawful basis includes:

a) contractual necessity;

b) compliance with legal obligations;

c) vital interest;

d) public interest; and

e) legitimate interests.

5.4.3 Informed and freely given consent

Control

The organization shall provide sufficient details concerning their processing of PII so that the PII principal can give consent to the processing freely, specifically and on a knowledgeable basis, and can easily access, modify and/or withdraw that consent.

Additional information

Details should include the information specified in 5.3.

Consent is only considered to be informed if there is evidence that the PII principal has been provided a clear and understandable notice. Consent needs to be freely given without the PII principal perceiving any form of coercion or compulsion.

Organizations, when obtaining consent, should obtain it through the PII principal's intentional action.

An intentional action is an action which is unambiguously associated with the PII principal's own intention. For example, such user interface actions as clicking a checkbox, pressing a button or sliding a slide bar can be considered as forming an intentional action.

If the screen to display the notice and the screen to perform the action are separated, PII principals can get confused about what they are about to do. Therefore, it is better to display the notice on the same screen as the one obtaining the consent. Where it is not feasible to display the notice and the request for consent on the same screen, organizations should take additional measures (such as a summary of key points from the notice) to ensure that the PII principal clearly understands what they are consenting to.

The modification and withdrawal of the consent should be as easy as it was to give. This can be achieved by providing an account or privacy settings page for the PII principal.

NOTE One possible approach to document the consent is to use consent receipt as explained in Annex B.

5.4.4 Providing the information about which account the PII principal is using

Control

When an organization is collecting consent associated with an account, the organization shall clearly indicate which account of the PII principal it is asking to grant consent.

Additional information

A PII principal may have more than one online account at the PII controller. For example, the PII principal may have browser sessions to a service with both their work account and their private account. Another common example is a case where members of a family are sharing the same PC and the web browser is maintaining the sessions for all of them and the user can select the account from a pull-down menu.

Organizations should display the user account or identity that is being used to give consent in the manner that the PII principal is accustomed to when using the system.

At the outset, the PII controller ensures that the claimed PII principal is verified so that the PII controller can be confident that the PII rightfully relates to that PII principal.

Also note that there are cases where the PII principal has not established an account with the service, but the service is identifying the PII principal with an implicit account that may be linked to an explicit account later.

5.4.5 Independence from other consent

Control

The organization shall obtain consent for matters related to privacy separately from consent for other matters not related to privacy.

Additional information

Consent for use, collection and processing of PII should be clearly differentiated from Terms of Use. Combining privacy-related notice with other matters can obscure the notice and potentially have a negative impact on the comprehensibility of the notice. Organizations should obtain consent through an action independent from consent for any other terms not related to privacy (e.g. contractual terms and conditions).

5.4.6 Separate consent to necessary and optional elements of PII

Control

The organization shall make it possible for the PII principal to recognize the necessary (mandatory) and optional elements of PII for each identified purpose.

Additional information

If the necessary elements of PII are not provided, then the processing cannot proceed, but it is not the case for the optional elements of PII.

The organization should make it possible for the PII principal to provide consent separately on the necessary elements of PII and optional elements of PII.

Where PII is provided for an optional element of PII, it should be taken that consent has been given.

5.4.7 Frequency

Control

The organization shall seek to confirm existing consent or gain the new consent of a PII principal at an appropriate interval.

Additional information

If the organization asks for the consent of the PII principal too often, the PII principal can overlook what the consent is about and start accepting it without really understanding the implication of it. This is sometimes referred to as click training or user de-sensitization. The organization should not seek consent too often to prevent this from happening. An indicator for the considerations made before should be the negative impacts on the PII principal or the risks of such an impact (i.e. the frequency of confirming existing consent or gaining new consent should enable the PII principal to effectively and efficiently react to or prepare for the corresponding impacts or risks).

Typically, re-consent is only required where a change of conditions (see 5.5) exist.

5.4.8 Timeliness

Control

The organization shall obtain the consent of the PII principal in a timely manner.

Additional information

Seeking the consent of the PII principal too early can have practical issues in the choice being given to the consent. The organization should not seek the consent of the PII principal too early.

5.5 Change of conditions

5.5.1 General

Objective: To ensure PII principals have an opportunity to re-consent when significant changes are made in respect to matters regarding initial consent (see 5.4).

5.5.2 Renewing notice

Control

The organization shall inform the PII principal when its contents of notice (see 5.3) are updated

Additional information

Situations, when the organization should inform the PII principal are for example when:

a) the PII controller's contact details change;

b) the contact point details change;

c) recipients or categories of recipients;

d) PII retention period changes.

5.5.3 Renewing consent

Control

The organization shall obtain re-consent from the PII principal when conditions change, and not effect such changes for the PII principal until the re-consent is obtained, especially in circumstances where the PII principal can be negatively impacted.

Additional information

Situations when the PII principal is required to re-consent are, for example, when:

a) the PII controller changes the purpose of use of collected PII to something outside the scope of what was notified to the PII principal at the time PII was collected;

b) there is a substantial organizational change at the PII controller (e.g. change of owner, change of business);

c) the PII controller changes the PII being collected (e.g. the PII being processed changes);

d) the PII controller changes the processing of PII;

e) the PII controller changes the collection method of PII (e.g. the methods used to process the PII change);

f) the PII controller changes matters related to the transfer of PII to a third party (unless the PII principal was previously notified that PII would be provided to a range of third parties and the change made does not expand the scope of transfer);

g) the PII controller extends the retention period or changes the disposal date notified to the PII principal at the time PII was collected;

h) the PII controller changes matters related to disclosure, use and retention period, correction, deletion, third party transfer, or revoking of consent;

i) the PII controller changes the geo-location of data collection.

When organizations should seek consent for changes such as those outlined here, they should consider whether the PII principal has access to a record (of some kind) of their original consent, as well as how much time has elapsed between the original consent and the present. If the PII principal is able to access a record of their prior consent readily and if the elapsed time is not significant, organizations may provide notice of the changes and seek consent for the same. Otherwise, the organization should seek reconfirmation of the original consent in addition to consent to the notified changes.

Where re-consent is requested, and no response is received, it should be assumed that the original consent has been withdrawn.

If a PII principal was notified of a change and that change is going to be made within a notified context, the organization can change without obtaining consent from the PII principal.

In many cases, the consent for an individual PII principal would be obtained at the login time of the PII principal.

Annex A
(informative)

User interface example for obtaining the consent of a PII principal on PCs and smartphones

A.1 General

This annex covers some aspects of the presentation of the notice and the user interface for obtaining consent. The presentation and the consent user interface can vary widely depending on the circumstances and context. For example, the presentations that are suitable for a smart watch and a personal computer can differ greatly. As such, the presentation and the user interface should be optimized in each case and should lead to good practices for each type of case.

In this annex, presentation and user interface aspects of personal computers and smartphones are covered as a starting point for such considerations.

A.2 User interface examples for obtaining initial consent for PCs and smartphones

A.2.1 Identification of which account the PII principal is using

Before organizations can collect PII from the PII principal, they should identify the PII principal explicitly or implicitly. In some cases, the PII principal has established multiple account with the PII controller. In some other cases, the device is shared so that the device can be maintaining multiple sessions to the PII controller's software. In both cases, as described in 5.4.4, it is important to ensure that the PII principal is aware of which account is being used to give consent and select the correct PII principal and account if not.

There are many ways to achieve this. The simplest way is to ask the PII principal for an username and password. Other methods are becoming popular, such as displaying an account selection screen prompting the PII principal to select which account to use for granting consent (see Figure A.1).

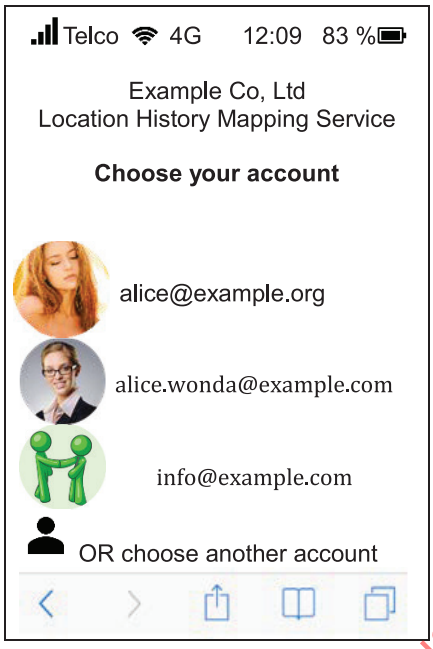

Figure A.1 — Account selection screen

A.2.2 Order of Items to be displayed

When organizations seek consent from PII principals, they should display the chosen item in the order specified in 5.3. The chosen item should be displayed as a headline in a table format for corresponding values. However, in the absence of corresponding value, the row may be omitted. If the screen is too small to fit all the relevant information in a table format, a text format may be used. However, the order of appearance should not be changed.

Displaying items in a fixed order in a table format makes the comparison of different notices easier, helping PII principals to form their decision (see Figure A.2).

EXAMPLE 1

Notice regarding use of PII	
Overview of service	"Where was I" Location history mapping service
Purpose of use	To provide your mobile history to you as a map
PII controller	Example Co., Ltd.
PII to be collected	Email address, GPSLocation, IP Address
Collection method	Data is collected via "Where was I App"
Timing and location of the PII Collection	Data is collected while the application is running and in the background.
Method of use	Collected data are combined to infer the location of the phone that the App is running
Geo-location of stored PII	California, USA
Transfer to third parties	No
Retention period, disposal	To be disposed of after being stored for six months
Your participation and current choices	You may view,update, and delete the stored information and manage information sharing consent options at http://example.com/maps/
Inquiry and complaint	Tel: 03-0000-0000 E-mail: info@example.com Web: https://example.com/info/ Supervising authority: PPC
Lawful basis	Performance of the contract and consent (for email)
Additional risks	Learn about the risks with granting access to the PII at http://example.com/maps/risks/
Notice	A full copy of this notice is available at http://example.com/maps/notice/

Figure A.2 — Notice in a table format

When displaying the notice in a constrained screen such as on a smart phone, organizations can want to omit the item names.

EXAMPLE 2 Item names are omitted (see Figures A.3 and A.4).

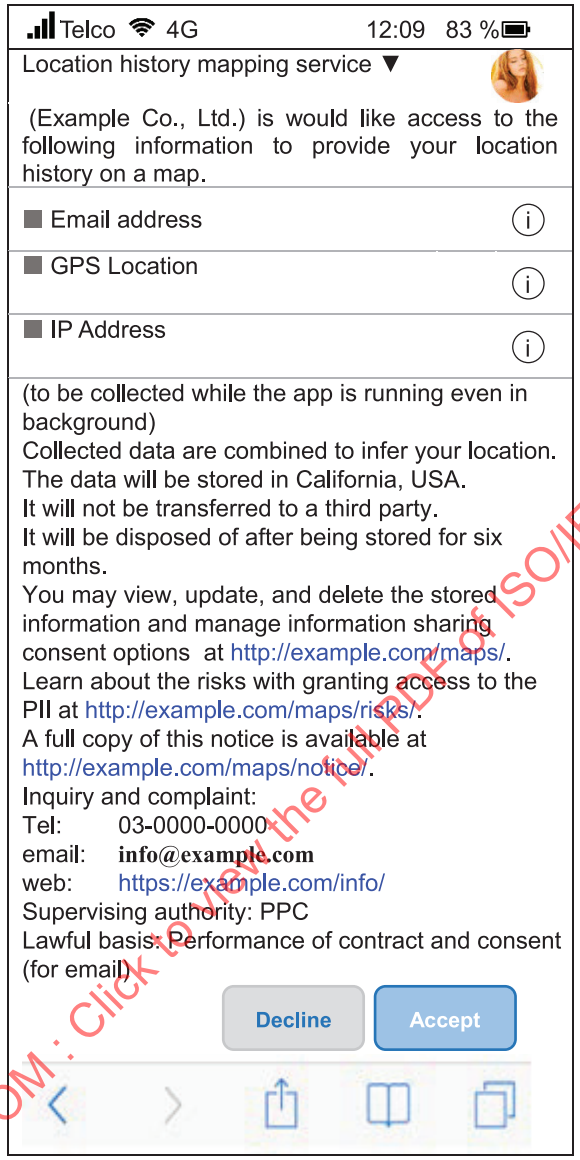

Figure A.3 — Case where the heading is omitted