INTERNATIONAL STANDARD

ISO/IEC 29100

First edition
2011-12-15

AMENDMENT 1
2018-06

Information technology — Security techniques — Privacy framework

AMENDMENT 1: Clarifications

Technologies de l'information — Techniques de sécurité — Cadre privé

AMENDEMENT 1: Clarifications

Reference number
ISO/IEC 29100:2011/Amd.1:2018(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

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).

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).

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.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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.

Information technology — Security techniques — Privacy framework

AMENDMENT 1: Clarifications

Introduction, third paragraph, first sentence

Replace "international standard" with "document":

> In some jurisdictions, this document's references to privacy safeguarding requirements might be understood as being complementary to legal requirements for the protection of PII.

Introduction, last paragraph

Replace "international standard" with "document":

> Some jurisdictions might require compliance with one or more of the documents referenced in ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 (WG 5 SD2) — *Official Privacy Documents References* [3] or with other applicable laws and regulations, but this document is not intended to be a global model policy, nor a legislative framework.

2.6

Delete the definition of identify:

> 2.6
>
> (withdrawn)

2.7

Delete the definition of identity:

> 2.7
>
> (withdrawn)

2.9

Change the terminological entry as follows:

2.9
personally identifiable information
PII
any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person

NOTE The "natural person" in the definition is the PII principal (2.11). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

2.20

Change the terminological entry as follows:

2.20
privacy impact assessment
PIA
privacy risk assessment
overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of personally identifiable information, framed within an organization's broader risk management framework

[SOURCE: ISO/IEC 29134:2017, 3.7, modified — "privacy risk assessment" has been added as an admitted term.]

4.5, last paragraph, second item of list

Replace with the following to synchronize item text with the text from Figure 1:

— contractual factors such as agreements between and among several different actors, company policies and binding corporate rules;

4.5.2, second paragraph

Replace the paragraph with the following:

In principle, any party that has access to PII should be made aware of its obligations by the respective PII controller(s) in a formalized manner, for example, by entering into third-party agreements. Such agreements are likely to contain a number of privacy safeguarding requirements that recipients of PII will have to take into account. In certain jurisdictions, national and regional authorities might have established legal and contractual instruments that enable the transfer of PII to third parties.

4.5.3, second paragraph

Replace the paragraph with the following:

Many business factors do not have a direct impact on privacy safeguarding requirements as such. The envisaged use of PII is likely to affect an organization's implementation of privacy policies, as well as the choice of privacy controls. However, the organization should not change the privacy principles it subscribes to because of that. For example, offering a certain service might require a service provider to collect additional PII or to allow more of its employees to process certain types of PII. However, a PII controller that has subscribed to the principles contained in this framework should still carefully assess which types of PII are strictly needed to provide the service (principle of collection limitation) and to limit the processing of PII by its employees to that needed in order to fulfil their duties (principle of data minimization).

5.1, first paragraph, first sentence

Replace "states, countries" with "countries":

The privacy principles described in this standard were derived from existing principles developed by a number of countries and international organizations. This framework focuses on the implementation of the privacy principles in ICT systems and the development of privacy management systems to be implemented within the organization's ICT systems. These privacy principles should be used to guide the design, development, and implementation of privacy policies and privacy controls. Additionally, they can be used as a baseline in the monitoring and measurement of performance, benchmarking and auditing aspects of privacy management programs in an organization.

5.5, bullet list

Replace the list with the following:

— minimize the PII which is processed and the number of privacy stakeholders and people to whom PII is disclosed or who are allowed to process it;

— ensure adoption of a "need-to-know" principle (i.e., one should be allowed to process only the PII which is necessary for the conduct of his/her official duties in the framework of the legitimate purpose of the PII processing);

— use or offer as default options, wherever possible, interactions and transactions which do not involve the identification of PII principals, reduce the observability of their behaviour and limit the linkability of the PII collected; and

— securely dispose of PII whenever it is practical to do so, in particular when the purpose for PII processing has expired and where there are no legal requirements to keep it.

5.8, second list, last item

Replace "PII data" with "PII":

— the specified PII retention and disposal requirements.

5.9, list, item 3

Replace “personal data” with “PII”:

— providing any amendment, correction or removal to PII processors and third parties to whom PII had been disclosed, where they are known; and

ICS 35.030

Price based on 4 pages