INTERNATIONAL STANDARD

ISO/IEC 27556

First edition
2022-10

Information security, cybersecurity and privacy protection — User-centric privacy preferences management framework

Sécurité de l'information, cybersécurité et protection de la vie privée — Cadre centré sur l'utilisateur pour le traitement des données à caractère personnel basé sur des préférences relatives au respect de la vie privée

Reference number
ISO/IEC 27556:2022(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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 or www.iec.ch/members_experts/refdocs).

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 https://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. In the IEC, see www.iec.ch/understanding-standards.

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 and www.iec.ch/national-committees.

Introduction

This document describes a user-centric framework for handling personally identifiable information (PII), based on privacy preferences and privacy preference administration within information and communication technology (ICT) systems. ICT systems which handle PII implement privacy control mechanisms. To ensure these mechanisms are implemented effectively in ICT systems, PII is controlled using privacy preferences which are set (directly or indirectly) by the relevant PII principal, including consent information. When PII is processed based upon authorities other than consent, ICT systems can, where appropriate, incorporate mechanisms to improve transparency and adjust PII processing in accordance with the preferences of the PII principal. PII principals can make informed use of a system only when they understand the scope of its privacy implications, which is improved when the actionable privacy control options align in an intuitive way with PII processing undertaken in the ICT system.

Mechanisms that incorporate a PII principal's privacy preferences into machine-readable settings for each PII handling system can be useful. Moreover, such collected PII may be shared or transferred among other service providers according to the PII principal's preferences.

The framework is intended to help organizations include user-centric PII handling mechanisms in their systems following privacy-by-design principles and realize PII handling based on privacy preferences of PII principals. The framework includes components designed to manage privacy preference information, and sub-components that are implemented within that component are defined in this document. However, this document does not specify the content and format of privacy preference information.

This document can be used to:

— design and implement ICT systems that handle PII, or transfer PII between organizations;

— develop PII exchange platforms based on privacy preferences;

— provide privacy preference management services.

Information security, cybersecurity and privacy protection — User-centric privacy preferences management framework

1 Scope

This document provides a user-centric framework for handling personally identifiable information (PII), based on privacy preferences.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
personally identifiable information
PII
information that (a) can be used to identify the *PII principal* (3.2) to whom such information relates, or (b) is or may be directly or indirectly linked to a PII principal

Note 1 to entry: 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 identify that natural person.

[SOURCE: ISO/IEC 29100:2011, 2.9, modified — The word “any” has been removed, “might” has been replaced by “may”.]

3.2
PII principal
natural person to whom the *personally identifiable information* (3.1) relates

Note 1 to entry: Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym “data subject” can also be used instead of the term “PII principal”.

[SOURCE: ISO/IEC 29100:2011, 2.11]

3.3
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information* (3.1) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others (e.g. PII processors) to process personally identifiable information on its behalf while the responsibility for the processing remains with the PII controller.