INTERNATIONAL STANDARD

ISO/IEC 27555

First edition
2021-10

Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion

Sécurité de l’information, cybersécurité et protection de la vie privée — Lignes directrices relatives à la suppression des informations personnellement identifiables

Reference number
ISO/IEC 27555:2021(E)

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 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

Many functional processes and IT applications use personally identifiable information (PII), which is subject to various compliance provisions relating to privacy. Thus, organizations need to ensure that PII is not retained for longer than is necessary and that it is deleted at the appropriate time. This can require organizations to fulfil the rights of PII principals, such as the right to obtain erasure (to be forgotten). ISO/IEC 29100 defines principles of "data minimization" and "use, retention and disclosure limitation" for PII, which can be enforced using deletion as a security control.

PII deletion requires a set of carefully designed, clear and easily understood deletion rules, embodying appropriate retention periods that satisfy the demands of multiple stakeholders. These rules should also conform with requirements originating from codes of practice and other standards. Mechanisms are to be correctly implemented and appropriately operated. In order to ensure the legally compliant deletion of PII, the PII controller needs to develop policies and procedures for deletion that include a set of rules and responsibilities for the processes involved. The chances of success for the development and implementation of these policies and processes can be improved if the PII controller uses a recognized approach to their design and implementation.

This document provides a framework for developing and establishing policies and procedures for PII deletion that can be implemented by an organization. This framework allows for consistent deletion of PII throughout an organization.

Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion

1 Scope

This document contains guidelines for developing and establishing policies and procedures for deletion of personally identifiable information (PII) in organizations by specifying:

- a harmonized terminology for PII deletion;
- an approach for defining deletion rules in an efficient way;
- a description of required documentation;
- a broad definition of roles, responsibilities and processes.

This document is intended to be used by organizations where PII is stored or processed.

This document does not address:

- specific legal provision, as given by national law or specified in contracts;
- specific deletion rules for particular clusters of PII that are defined by PII controllers for processing PII;
- deletion mechanisms;
- reliability, security and suitability of deletion mechanisms;
- specific techniques for de-identification of data.

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 29100:2011, *Information technology — Security techniques — Privacy framework*