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/IEC 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO/IEC 2021 – All rights reserved

Contents

Page

Foreword ... **v**
Introduction ... **vi**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols and abbreviated terms ... **3**
5 Framework for deletion ... **3**
5.1 General ... 3
5.2 Constraints ... 4
5.3 Clusters of PII ... 4
5.4 Retention period and regular deletion period ... 5
5.4.1 Retention period ... 5
5.4.2 Regular deletion period ... 5
5.4.3 Allocation of clusters of PII ... 6
5.5 Archives and backup copies ... 6
5.6 Standard deletion periods, starting points, deletion rules and deletion classes ... 7
5.7 Special situations ... 7
5.8 Documentation of policies and procedures ... 8
6 Clusters of PII ... **8**
6.1 General ... 8
6.2 Identification ... 9
6.3 Documentation ... 10
7 Specification of deletion periods ... **10**
7.1 Standard and regular deletion periods ... 10
7.2 Regular deletion period specifications ... 11
7.3 Standard deletion period identification ... 11
7.4 Deletion period specifications for special situations ... 12
7.4.1 General ... 12
7.4.2 Modification of data objects ... 12
7.4.3 Need to extend period of active use ... 13
7.4.4 Suspension of the deletion ... 13
7.4.5 Backup copies ... 13
8 Deletion classes ... **14**
8.1 Abstract starting points — abstract deletion rules ... 14
8.2 Matrix of deletion classes ... 15
8.3 Allocation of deletion classes and definition of deletion rules ... 16
9 Requirements for implementation ... **16**
9.1 General ... 16
9.2 Conditions for starting points outside IT systems ... 18
9.3 Requirements for implementation for organization-wide aspects ... 18
9.3.1 General ... 18
9.3.2 Backup ... 18
9.3.3 Logs ... 19
9.3.4 Transmission systems ... 19
9.3.5 Repair, dismantling and disposal of systems and components ... 19
9.3.6 Everyday business life ... 19
9.4 Requirements for implementation for individual IT systems ... 20
9.5 Deletion in regular manual processes ... 21
9.6 Requirements for implementation for PII processor ... 21
9.7 Control deletion in special cases ... 21
9.7.1 Exception management ... 21

© ISO/IEC 2021 – All rights reserved

9.7.2 Further sets of PII 22
10 Responsibilities 22
10.1 General 22
10.2 Documentation 23
10.3 Implementation 24
Bibliography 25

© ISO/IEC 2021 – All rights reserved

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.

© ISO/IEC 2021 – All rights reserved

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.

© ISO/IEC 2021 – All rights reserved

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*

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/

© ISO/IEC 2021 – All rights reserved

3.1
cluster of personally identifiable information
cluster of PII
personally identifiable information which is processed for a consistent functional purpose

Note 1 to entry: Clusters of PII are described independently of the technical representation of data objects. On a regular basis, the clusters of PII also include PII which is not stored electronically.

3.2
data object
element which contains personally identifiable information (PII)

EXAMPLE Examples of elements include files, documents, records or attributes. Concrete data objects include, for example, invoices, contracts, personal files, visitor lists, personnel planning sheets, photos, voice recordings, user accounts, log entries and consent documents.

Note 1 to entry: In the context of this document, data objects usually contain PII and can be combined with other data objects in a *cluster of PII* (3.1). The individual data object can be of varying complexity.

3.3
deletion
process by which personally identifiable information (PII) is changed so that it is no longer present or recognizable and usable and can only be reconstructed with excessive effort

Note 1 to entry: In this document the term deletion has the following synonyms: disposition mechanism, erasure, destruction, destruction of data storage media.

Note 2 to entry: In this document the term deletion refers to the elimination of the bit patterns or comparable practices, not simply marking or moving the data to be hidden. As a result, excessive effort for PII reconstruction is required, considering all the means likely to be used, e.g. available state-of-the-art technology, human and technical resources, costs and time.

Note 3 to entry: For selecting the methods for deletion, a risk-based approach should be taken into account, including sensitivity of PII and potential use of forensic tools. Required measures can change over time depending on the state of the art of technology and other factors.

Note 4 to entry: PII can be also changed by applying an irreversible de-identification technique. Such data often fall out of the scope of privacy legislation. Further guidance on a de-identification technique can be found in ISO/IEC 20889:2018, Clause 11.

3.4
deletion class
combination of a *standard deletion period* (3.7) and an abstract starting point for the period run

Note 1 to entry: All clusters of personally identifiable information (PII) which are subject to the same *deletion period* (3.6) and the same abstract starting point are combined in a deletion class. As opposed to the (specific) *deletion rule* (3.5) for a *cluster of PII* (3.1), the (abstract) deletion class relates only to the abstract starting point and not to a specific condition for the start of the period run (see also Clause 8).

3.5
deletion rule
combination of *deletion period* (3.6) and specific condition for the starting point of the period run

3.6
deletion period
time period after which a specific *cluster of personally identifiable information (PII)* (3.1) should be deleted

Note 1 to entry: As a generic term, the deletion period comprises all deletion periods. This includes the *standard deletion periods* (3.7) and the *regular deletion periods* (3.8), which form special groups. However, the term also includes, for instance, the specific deletion periods for some clusters of PII or deletion periods in special cases. For details, see Clause 7.

© ISO/IEC 2021 – All rights reserved

Note 2 to entry: The deletion period for a cluster of PII extends beyond the end of the *retention period* (3.9), by at least an amount commensurate with the time required to achieve deletion of the relevant *data objects* (3.2).

3.7
standard deletion period
unified deletion period for the personally identifiable information (PII) controller

Note 1 to entry: A standard deletion period is a *deletion period* (3.6) used for several *clusters of PII* (3.1) to standardize several deletion periods lying close to one another (see 7.1).

3.8
regular deletion period
maximum time period after which the *data objects* (3.2) of a *cluster of personally identifiable information (PII)* (3.1) should be deleted if used in regular processing in the processes of the PII controller

Note 1 to entry: For the boundary conditions of period specifications, see 5.4.

3.9
retention period
time period within which the *data objects* (3.2) of the *cluster of personally identifiable information (PII)* (3.1) are required to be available in the PII controller's organization because of functional use or legal retention obligations

Note 1 to entry: A specific cluster of PII typically has the same retention period.

Note 2 to entry: For the boundary conditions of period specifications, see 5.4 and Clause 7.

3.10
legal retention period
time period within which the *data objects* (3.2) of a *cluster of personally identifiable information (PII)* (3.1) are available in the PII controller's organization as required by legal provisions

4 Symbols and abbreviated terms

CD	compact disc
DVD	digital versatile disc
IT	information technology
PII	personally identifiable information
PDF	portable document format
SD	secure digital
USB	universal serial bus

5 Framework for deletion

5.1 General

This document describes how an organization acting as PII controller can establish policies and procedures for deletion of PII. For this, the PII controller should specify:

— which deletion rules apply to which PII;

— how the deletion is implemented using the deletion rules;

— how the deletion rules and the deletion measures are documented;

© ISO/IEC 2021 – All rights reserved