DRAFT INTERNATIONAL STANDARD
ISO/IEC DIS 27555

ISO/IEC JTC **1**/SC **27** Secretariat: **DIN**

Voting begins on:
2020-12-08

Voting terminates on:
2021-03-02

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

ICS: 35.030

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 27555:2020(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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 27555 was prepared by Technical Committee ISO/TC JTC1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

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 is deleted at the appropriate time. This also may require organizations to fulfill PII principals' rights such as right to obtain the erasure (to be forgotten). ISO/IEC 29100 defines principles of “data minimization” and “use, retention and disclosure limitation” for personally identifiable information (PII) which can be enforced using deletion as a security control.

PII deletion requires a set of carefully-designed, clear and simple to understand, deletion rules, embodying appropriate retention periods that satisfy the demands of multiple stakeholders. Those rules should also comply with requirements originating from regulations, code of practice and other standards. Mechanisms are correctly to be implemented and to be operated properly. In order to ensure the legally compliant deletion of PII, the PII controller needs to develop policies and procedures for deletion that includes 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 an approved 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 to accomplish 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 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, and
- a broad definition of roles, responsibilities and processes.

This document is intended to be used by organizations where PII are being 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 as are to be defined by PII controllers for processing PII,
- deletion mechanisms,
- security 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, *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
cluster of PII
PII 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 contain PII

EXAMPLE Such elements are for instance files, documents, records or attributes. Concrete data objects can be e.g. invoices, contracts, personal files, visitor lists, personnel planning sheets, photos, voice recordings, user accounts, log entries, consent documents, and so on.

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. The individual data object can be of varying complexity.

3.3
deletion
process by which PII is changed in a manner 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 covers all such 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 will be required, considering all the means likely reasonably to be used, e.g. available state of the art of technology, human and technical resources, costs and time.

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

Note 4 to entry: PII can be also changed applying irreversible de-identification technique. Such data often fall out of privacy legislation. Further guidance on a de-identification technique can be found in ISO/IEC 20889:2018–11 (1st edition) — Privacy enhancing data de-identification terminology and classification of techniques.

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

Note 1 to entry: All clusters of PII which are subject to the same deletion period and the same abstract starting point are combined in a deletion class. As opposed to the (specific) deletion rule for a cluster of PII, 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 and specific condition for the starting point of the period run

3.6
deletion period
time period after which a specific cluster of PII should be deleted

Note 1 to entry: As a generic term, the deletion period comprises all deletion periods. This includes the standard deletion periods and the regular deletion periods, 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.

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

3.7
standard deletion period

unified deletion periods for the PII controller

Note 1 to entry: A standard deletion period is a deletion period used for several clusters of PII 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 of a cluster of PII 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 of cluster of PII is required to be available in the PII controller’s organization because of the 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 of a cluster of PII are available in the PII controller’s organization as required by legal provisions

4 Symbols and abbreviated terms

CRM	Customer Relationship Management
DMS	Document Management system
IT	Information Technology
PII	Personally Identifiable Information

5 A 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;
- the manner in which the deletion rules and the deletion measures are documented; and
- who is responsible for the deletion rules, deletion processes and their documentation.

To establish deletion policies and procedures the following steps are recommended:

- select a minimum number of standard deletion periods which form the basis of deletion classes;
- base deletion classes on the standard deletion periods identified;
- allocate each cluster of PII to a deletion class.

- identify and document deletion processes;
- implement deletion processes for each cluster of PII.

The number and complexity of the deletion classes should be kept to a minimum within the context of the relevant compliance requirements.

5.2 Legal, regulatory and contractual requirements

The PII controller should ensure their policies and procedures to meet compliance and contractual requirements are relevant to the PII in their possession.

Where the organization is performing the role of a PII processor, they should ensure deletion rules are implemented in accordance with the relevant PII controller instructions.

Where compliance and/or contractual requirements state that PII should be deleted when it is no longer required for the defined purpose the principles contained in ISO/IEC 29100: (a) “Use, retention and disclosure limitation” and (b) “Data minimization”, should be considered when designing the deletion processes.

EXAMPLE The deletion rule for the cluster of PII named “Accounting data” could be 10 years after the end of the financial year in which the accounting entry was made in the balance sheet.

Compliance and/or contractual requirements can require special measures, particularly where clusters of PII are retained only to fulfil retention obligations. In this case, restricting the processing of the clusters of PII concerned may be required.

5.3 Clusters of PII

Clusters of PII should be named individually and unambiguously and according to their functional purposes. Each cluster of PII should be allocated one deletion rule (see 6.2.)

EXAMPLE For a telecommunications provider, customer data, location data, traffic data, billing data, itemized bill data, etc. could be the names of clusters of PII.

The same PII can be part of more than one cluster of PII because of two cases:

- clusters of PII contain one or more data objects. Some attributes like name or address can occur in several data objects in the same or different clusters of PII, e.g. in the customer master data, an invoice and a letter to the customer. Deletion is applied usually on the data object as a whole (and not on single attributes within the data object.)
- copies of a data object can be part of different clusters of PII.

EXAMPLE Assume an invoice documents materials and actions performed to repair an engine. With functional processes three copies of the document are stored in different clusters of PII: “Bookkeeping data” (deleted 11 years after payment), “engine documentation file” to document the history and parts of the engine (deleted 5 years after destruction of the engine) and “supplier file” to document the history of the relationship and operations with the supplier (deleted 15 years after receiving the data object.)

PII should not be deleted upon individual case decisions only, but in accordance with appropriate deletion rules wheresoever possible. Therefore, the PII controller should develop deletion rules in accordance with their deletion policy. Every deletion rule should include a definition of the deletion period and when the deletion period begins (starting point.)

5.4 Retention period and regular deletion period

5.4.1 Retention period

The period of time for which a cluster of PII is retained, based on its functional purposes (which might include retention period complying with legal and statutory obligations), is its retention period. This time period includes the time period in which a cluster of PII is actively used in functional processes, in accordance with compliance and/or contractual purposes and in accordance with the organizations long term storage requirements.

EXAMPLE The legal retention obligations for clusters of PII include, for example, the provisions of tax laws for trade letters and accounting documents. Functional purposes include, for example, guarantee commitments and potential equipment recall actions.

5.4.2 Regular deletion period

Clusters of PII should not be deleted until the end of its defined retention period, unless specific approvals have been obtained.

Legal obligations may grant a leeway after retention period to perform deletion. This leeway can be used to apply a process and mechanisms for deletion in accordance with organizational and technical conditions. The combination of the retention period and the maximum time period for the deletion process is defined as the regular deletion period. The PII controller should estimate the maximum time period that is acceptable for the deletion process.

Each deletion rule should be applied by deleting data objects within a cluster of PII in all systems and all other storage places including physical documents. This includes the deletion of clusters of PII processed by any PII processors contracted by the PII controller.

Figure 1 shows an example of how to derive a regular deletion period based on the lifecycle of an order. The retention period and regular deletion period for the order starts with the formation of the contract. The active use of the contract ends with the receipt of payment. After that, the contract is still retained for possible warranty cases and as a trade letter.

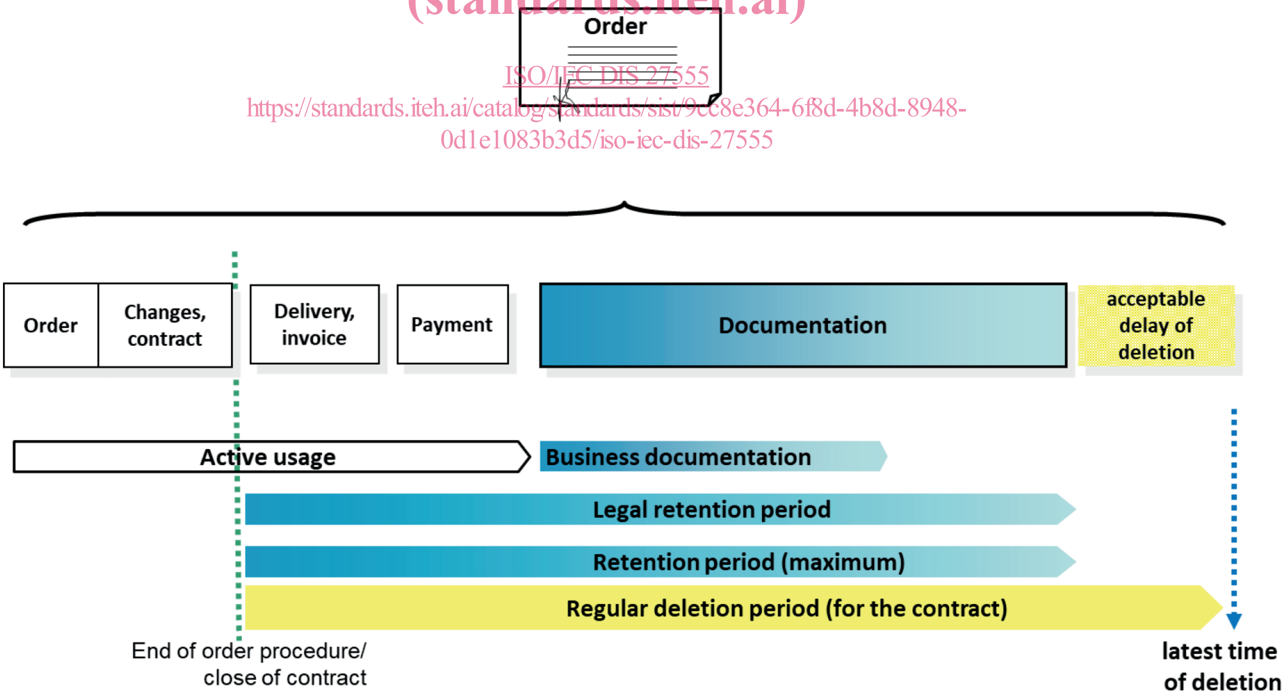

Figure 1 — Example of regular deletion period for an order

NOTE In the example in Figure 1 the retention period for the order is shorter than the regular deletion period. Depending on which cluster of PII is involved and its defined deletion period, the retention period and the regular deletion period sometimes have nearly the same duration. The invoice and the booking of the payment received are categorized as separate clusters of PII and therefore have different deletion rules.

5.4.3 Allocation of clusters of PII

The allocation of clusters of PII to specific standard deletion periods should be based on compliance and/or contractual requirements in alignment with business needs. The standard deletion periods should be kept as few as possible and should be the minimum required in order to ensure compliance and business needs. For further information on standard deletion periods, see 7.1.

If the relevant compliance and/or contractual business requirements specify specific deletion provisions, then the regular deletion periods should be aligned accordingly. These provisions might also include guidelines for the design of the deletion processes.

EXAMPLE For instance, the retention of traffic data required for calculating usage charges is sometimes limited by law.

Further guidance for the allocation of regular deletion periods to clusters of PII can be found in Clause 7 and 8.3.

5.5 Archives and backup copies

Archives serve the purpose of keeping data available for extended periods of time. Data are transferred into archives when they are no longer expected to be actively used but are still required to be retained for permissible reasons. An archive can contain different clusters of PII with different deletion periods. The relevant compliance and/or contractual requirements can require restriction of processing for archived data.

Purpose of backup copies is the recovery of IT systems. Backup copies should not be used as archives.

The organization should clearly distinguish between backup copies and archives. PII contained in archives should be subject to the same deletion rules of the respective clusters of PII and these rules should be implemented in the archives concerned.

Often it is not practical (or even possible) to delete individual data objects within a backup copy, as it would contradict the purpose of a backup. To fulfil their purpose, backup copies are required to be available for only short periods of time. Using short deletion periods for the backup generations is a means of complying with the deletion provisions.

For the deletion of backup copies, individual time periods should be specified in the backup strategy (see 9.3). This time periods should be in acceptable proportion to the regular deletion periods of the various clusters of PII contained in the specific copy (see 7.4.)

During recovery of a system PII exceeded the regular deletion period may be restored. Restore processes therefore should consider this and state how to delete such old PII (see 9.1 and 9.4.)

5.6 Standard deletion periods, starting points, deletion rules and deletion classes

Before deletion rules can be defined for individual clusters of PII, considerable effort can be required for analysis. It is appropriate to involve the person responsible for privacy matters within the organization in the assessment of the standard deletion periods, starting points, deletion rules and deletion classes.

The PII controller should use standard deletion periods.

The starting points for the deletion periods may also be grouped (see 8.1.)

EXAMPLE One such abstract starting point is the “collection of the data”, another one is the “end of procedure.”

The combination of a standard deletion period and an abstract starting point form a deletion class (see Clause 8.) Clusters of PII should be assigned to the appropriate deletion class. For example, all clusters of PII which are subject to the same deletion period and the same starting point should be assigned to the same deletion class.