FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
27555**

ISO/IEC JTC **1**/SC **27**

Secretariat: DIN

Voting begins on:
2021-07-07

Voting terminates on:
2021-09-01

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

Reference number
ISO/IEC FDIS 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 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 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*

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 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 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.

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 disk
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;

— 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 the deletion procedure.

The PII controller should implement deletion mechanisms for each cluster of PII based on the established policies and procedures (see 10.3).

5.2 Constraints

The PII controller should establish policies and procedures for deletion of PII which enable the organization to demonstrate compliance with relevant legal, regulatory and other requirements. 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 should be considered when designing the deletion processes:

a) use, retention and disclosure limitation;

b) data minimization.

EXAMPLE The deletion rule for the cluster of PII named “Accounting data” can 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 such cases, restricting the processing of the clusters of PII concerned can 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 and itemized bill data are possible 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;

NOTE Some attributes, such as 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 usually applied 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. Functional processes can require that 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 wherever 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 can include retention period complying with business requirements as well as 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 organization's 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 their defined retention period, unless specific approvals have been obtained.

Legal obligations can allow for time flexibility to perform deletion after the retention period has been reached. This flexibility can be used to apply a process and mechanisms for deletion which may take into account the availability of technical solutions as well as the general organizational requirements. 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 storage places. This should include the deletion of data objects stored in physical documents. Also included is the deletion of clusters of PII processed by PII processors contracted by the PII controller.

Figure 1 shows an example of how to derive a regular deletion period based on the life cycle 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.

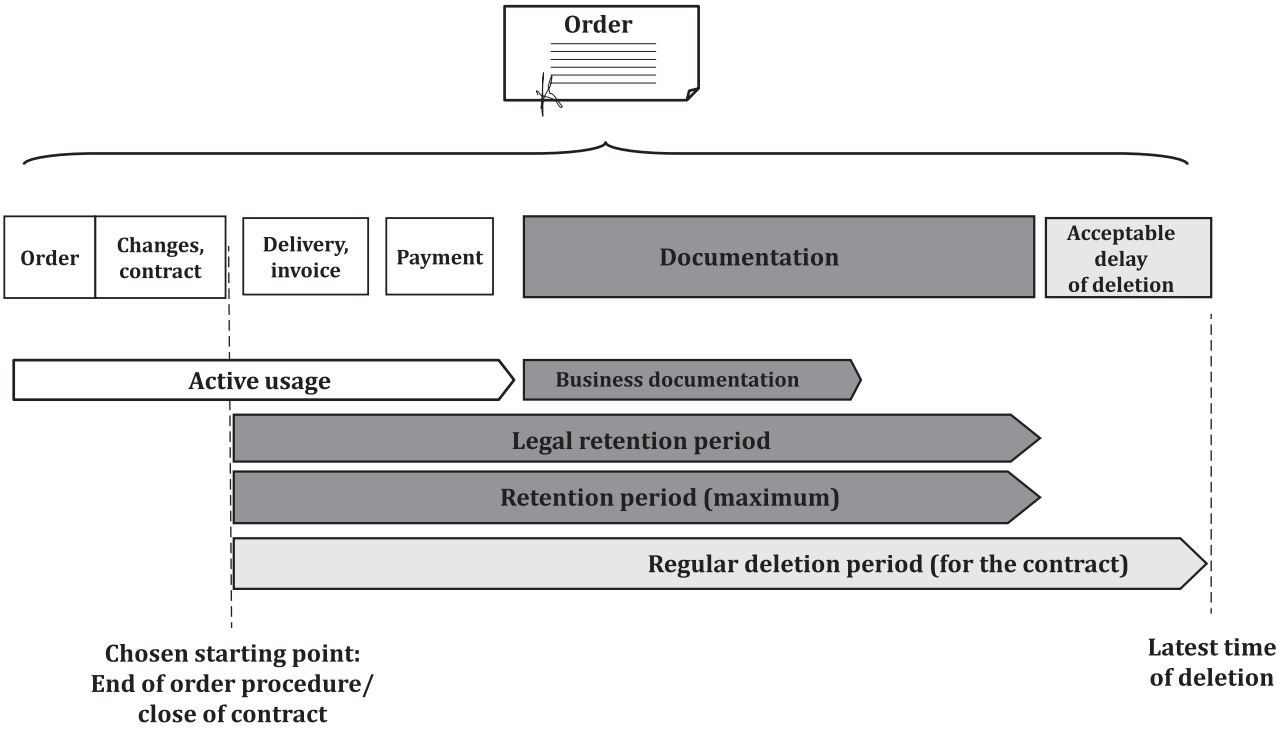

Figure 1 — Example of regular deletion period for an order

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 number of standard deletion periods should be as low as possible and should be the minimum required in order to meet these requirements and business needs. For further information on standard deletion periods, see 7.1.

The PII controller should consider relevant legal, regulatory and/or contractual business requirements giving specific deletion provisions when defining regular deletion periods. These provisions can also include guidelines for the design of the deletion processes.

EXAMPLE In the area of telecommunications, 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.

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

