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*

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 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.

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;

— 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.

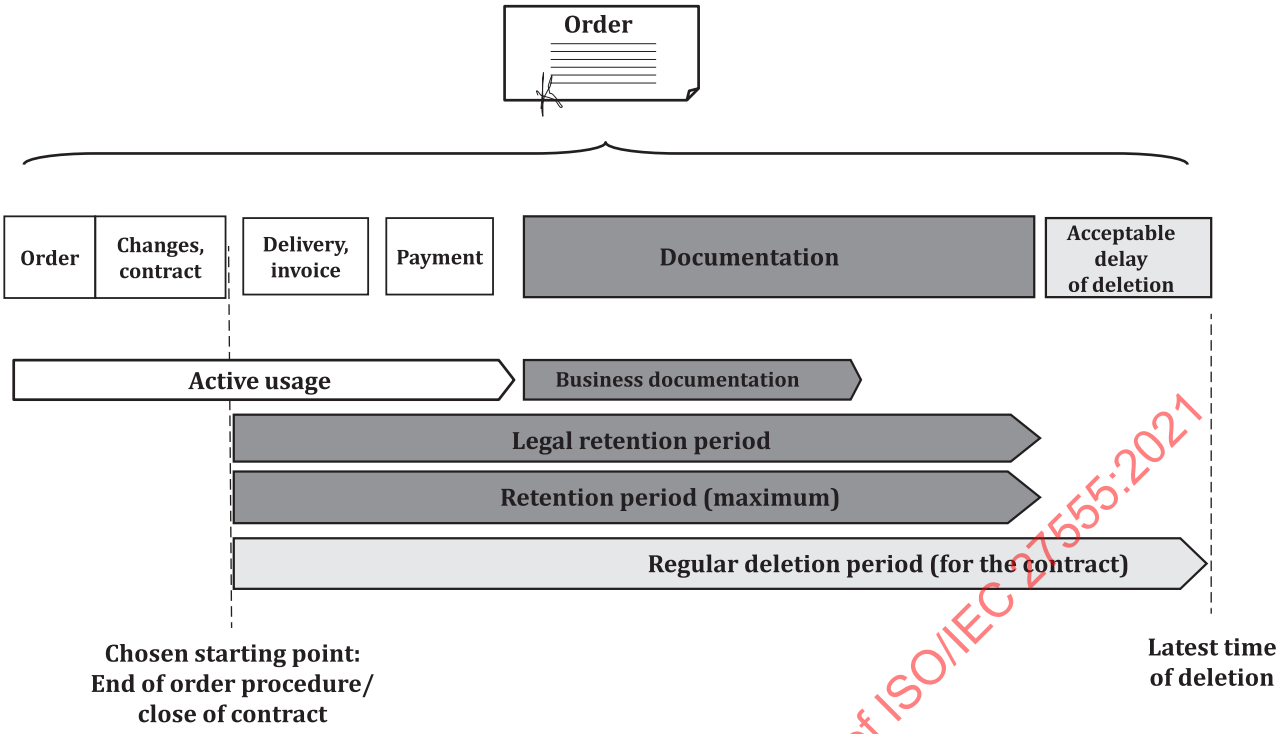


Figure 1 — Example of regular deletion period for an order

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.

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.

It is often impractical (or even impossible) 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 copies is a means of conforming with the deletion provisions.

For the deletion of backup copies, individual time periods should be specified in the backup strategy (see 9.3). These 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 which has exceeded the regular deletion period can be restored. Therefore, restore processes should consider this possibility and describe how to delete such restored 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 define and 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 is the “end of procedure”.

The combination of a standard deletion period and an abstract starting point forms 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.

5.7 Special situations

In some situations, deleting PII in accordance with the general deletion rules can be unfeasible for an organization. These situations include:

— deletion of PII which was collected without proper legal permission;

— deletion of PII after a legally founded request for deletion by the PII principal;

— deletion of PII which is likely necessary for a claim or an anticipated or ongoing legal case.

NOTE 1 In some jurisdictions, compliance requirements grant the PII principal a right to have PII deleted if certain prerequisites are met. For a specific cluster of PII, not all such requests need to be implemented, for example because of overriding compliance retention requirements.

For these and similar special situations, deletion measures should also be determined. These can be specified in the context of the processes and responsibilities for deletion of PII (see 9.7 and Clause 10).

Individual PII can only be deleted if the technical systems have a suitable function for deletion. Therefore, the PII controller should ensure that such a function is required in system procurement or system development processes if PII principals can require the deletion on a case-by-case basis. On the other hand, there is nothing to prevent the use of available standard functions for rare individual cases of such deletions, e.g. SQL instructions in databases.

NOTE 2 Under certain conditions, the PII controller has the option not to delete PII but to restrict the processing of that PII.

5.8 Documentation of policies and procedures

Policies and procedures for PII deletion should be documented. These documents should include advice from different entities within the organization, such as the person in charge in privacy matters, functional users, developers and administrators.

Policies and procedures can be integrated into existing documentation. To prevent inconsistencies and inefficiencies, duplication of policies and procedures should be avoided.

The deletion rules should be described without reference to the technology used for storage, control and deletion.

EXAMPLE 1 Bookkeeping data include invoices, receipts and bank transactions. To be independent from technical aspects, it is irrelevant on which media such data objects are stored (e.g. paper, hard disk, USB stick or microfiche), in which location they are stored (e.g. locally on a laptop, in a central IT system database, using a storage area network or paper file folders in an archive room) or which format is used (e.g. PDF, database record, text file). The same applies to a set of videos or audio tracks: it is irrelevant whether they are stored digitally or on "old media" such as celluloid, cassette, vinyl record or compact disk.

Technology-related requirements for implementation should be specified separately (see Clause 9 for further information). Deletion rules should also be applied to manual processes such as data handled by individuals, e.g. using paper-based documents or files in IT systems.

EXAMPLE 2 A job application is received on paper and stored in a file until the application process is performed. The application is to be deleted following the appropriate deletion rule after a decision is taken through a manual process. In other cases, PII in files is stored manually in the file system, e.g. invoices for special verification or handling. Handling of such data can be regulated by documented work instructions, including the need to delete the data manually.

6 Clusters of PII

6.1 General

Sets of PII should be categorized according to their functional purposes as clusters of PII. Different purposes and, thus, different clusters of PII can result, in particular, if:

— the legal basis for the PII collection differs;

— the relevant legal requirements contain different provisions for the use of PII;

— PII relates to different PII principals;

— PII is only used for purposes pursued by different functional entities;

— PII is of different sensitivity.

The PII controller should define and document clusters of PII for the organization.

Additional clusters of PII can be identified:

— when specifying deletion classes and deletion rules for the clusters of PII already identified;

— when specifying or implementing requirements for implementation for specific sets of PII in specific IT systems or other processes.

NOTE 1 In some cases, it is an option to subdivide individual clusters of PII.

NOTE 2 PII are structured differently (e.g. records in databases, files, paper documents) or are stored at different locations (e.g. tables of a database as well as in the files from which the PII was imported).

EXAMPLE 1 Examples of clusters of PII include accounting data, contract documents or system logs. The cluster of PII "Accounting data" can include, for instance, the data object "Accounting record" (including the details regarding creditor/debtor, payment date and due amount) as well as invoices and payment transactions with banks.

Sometimes, the same information may be contained in different clusters of PII and different data objects.

EXAMPLE 2 The cluster of PII "Logs" includes all records which are created for events in an IT system for monitoring purposes. A uniform deletion period of 42 days starting from the day of recording is adequate for logs because they are evaluated monthly. However, the PII controller wishes to be able to comprehend the status of the IT system at the same time and uses data objects of the cluster of PII "System status documentation" in order to ensure that. A small set of selected log records is also transferred into the system status documentation because it shows statuses and irregularities in system components, defects and successful repairs. An individual deletion rule is defined for the log records of the cluster of PII "System status documentation" (e.g. 4 years after recording), which also comprises the log records contained therein.

EXAMPLE 3 Attributes like the name and the address of a PII principal are usually part of several data objects, for example records of customer master data, invoices, communication letters or service request tickets. These data objects are assigned to different clusters of PII. Each of the data objects is deleted applying the specific deletion rule. In each case, the address attributes are handled together with the whole data object.

The allocation of data objects to clusters of PII should be specific to the organization.

EXAMPLE 4 For customer relations management, PII and the data objects that are needed only during the active customer relationship and shortly afterwards are separated from those for which retention obligations of several years apply. This distinction is often applicable to master data: the "supplementary master data" is used as a cluster of PII for contact data of the active customer relationship. PII and the data objects required to create the customer account (which is required for technical reasons in order to conform with the retention obligations) are allocated to the cluster of PII "Core master data". In a bank, a customer's account number is assigned to the cluster of PII "Core master data". On the other hand, a mail order company needs the account number of a customer only as a bank connection, for instance for credit notes, and would therefore allocate them to the cluster of PII "Supplementary master data". For such a mail order company, the core master data includes the customer's number, name and address.

6.2 Identification

The definition of clusters of PII is typically evident from their functional contexts. Each cluster of PII should have only one deletion rule.

The key steps for the definition of clusters of PII are:

— group data objects into individual clusters of PII to which the same legal basis applies related to the collection, use and retention;

— divide a cluster of PII into several clusters of PII if retention provisions only apply to a subset of them and if the regular deletion period would thereby be considerably extended.

— distinguish PII according to categories of PII principal;

EXAMPLE 1 Contact data such as contact names, telephone numbers and e-mail addresses are stored, for instance, for customers, employees of suppliers and service engineers of service providers. It is then generally useful to distinguish between the clusters of PII 'Supplementary master data of customers', 'Supplementary master data of suppliers' and 'Supplementary master data of service engineers'. These three clusters of PII would be allocated, for instance, to the deletion class '2 years after the end of the relationship with the PII principal'. Other master data are stored for longer periods of time due to the obligation to produce supporting documents. These are distinguished according to core master data of customers, core master data of suppliers and master data of service partners. These three clusters of PII then fall into another deletion class, for instance, '10 years after the end of the relationship with the PII principal'.

— distinguish PII according to functional purpose;

NOTE 1 The purpose for which the PII is processed is useful in selecting a name for the cluster of PII.

EXAMPLE 2 The cluster 'supplementary master data' of a customer contains a customer's master data record as data object. If a customer requires changes, then change requests are created and supplementary master data updated. This data object (the specific change requests) is also assigned to the cluster 'supplementary master data' and deleted one year after the end of the customer relationship as per the deletion rule of 'supplementary master data' cluster. In some cases, the organization finds it useful for functional purposes to maintain other change requests (e.g. IT changes, requests on user access rights) as another cluster 'IT change requests' and applies another deletion rule (e.g. 3 years after the date when change requests were processed).

— distinguish PII according to sensitivity of PII allocating PII of different sensitivity levels to different clusters. The higher the sensitivity of the data, the shorter the acceptable delay for deletion should be (see Figure 1).

NOTE 2 Examples of sensitive PII are given in ISO 29100:2011, 2.26 and 4.4.7. The European Union's General Data Protection Regulation (GDPR), Article 9, defines such PII as 'special categories of data'.[3]

Deletion rules should also be defined for unstructured data containing PII, e.g. remaining e-mails or remaining files in various locations.

6.3 Documentation

Each cluster of PII and its deletion rule should be documented without reference to the technology used for its control (see 5.8). This allows its reuse without requiring modifications for different data storage technologies as well as in the event of a change to a technical system. The reasons for the allocation of clusters of PII and their respective period definitions should be documented. This can be especially helpful in the long term in case of audits or change requests. The whole set of clusters of PII with their deletion rules defined by an organization can be called the deletion rules catalogue of this organization.

7 Specification of deletion periods

7.1 Standard and regular deletion periods

The PII controller should define standard deletion periods for the organization. The number of standard deletion periods should be as small as possible in order to facilitate the understanding of the policies on deletion and save resources for all the parties involved.

Regular deletion periods should always be derived from the standard deletion periods. However, the PII controller should choose the "next in line" standard deletion period.

NOTE 1 Legal requirements can limit the margin for the delay of deletion resulting from selecting the next higher standard deletion period.

Where the retention period of a cluster of PII does not correspond to a standard deletion period, it should wherever possible be reassigned to the next in line standard deletion period. The PII controller should select the standard deletion period where the difference from the legal retention period is adequate and acceptable. If that is not the case, then an additional standard deletion period should be introduced or a specific regular deletion period not identical to a standard deletion period should be defined.

NOTE 2 For the specification of its standard deletion periods, the PII controller can reuse definitions of clusters of PII and deletion rules from other organizations if such are available and suitable.

NOTE 3 Experience shows that a useful number of standard deletion periods lies in the range between 5 and 10 with a suitable distribution (see Figure 2).

NOTE 4 Limiting the standard deletion periods to as few as possible permits the simple derivation of deletion rules and results into a clear, understandable set of deletion rules.

If the retention period of a specific cluster of PII does not match one of the standard deletion periods, then the PII controller should check whether or not:

— the retention period can be shortened by adjustments to the functional process in order to delete after the next-shorter standard deletion period;

— to make full use of the next-shorter standard deletion period by carrying out the technical process of the deletion at the end of that period (and not within a larger interval);

— to move the end of the retention period closer to the regular deletion period by choosing another starting point for the deletion rule;

— to use an individual regular deletion period not included in the list of the standard deletion periods. However, such special cases should, if possible, be avoided.

7.2 Regular deletion period specifications

The PII controller should define regular deletion periods which take the following into account:

— Specific legal provisions which include a deletion period and can be directly adopted.

— Specific legal provisions which provide criteria for the specification of deletion periods without defining a specific deletion period. In such cases, the deletion period can be set taking into account the sensitivity of PII, functional process analysis and the legal provisions interpretation.

— Specific legal provisions which provide for a retention period. In such cases, the relevant legal provisions can offer margins whereby the regular deletion period can be set longer than the retention period. A "period for the deletion process" (see Figure 1) between the end of the retention period and the end of the regular deletion period is acceptable.

— The lack of specific legal provisions on deletion. In such cases, the deletion period can be set taking into account the general concepts of data minimization and data protection legislation.

7.3 Standard deletion period identification

Standard deletion periods should be derived from regular deletion periods, which are frequently identified from PII used in core processes of the PII controller.

Where several clusters of PII have similar deletion periods, it is generally sufficient to allocate an appropriate standard deletion period to those clusters of PII, as recommended in 7.1.

NOTE 1 For each standard deletion period there is at least one cluster of PII allocated.

To this end, clusters of PII are identified in an iterative process, which are potential representatives for deletion classes (see Clause 8). The regular deletion periods of these representatives should be used for the definition of the deletion classes.

If all other clusters of PII can be allocated to the deletion classes thus obtained, then the process is completed. If clusters of PII cannot be suitably allocated, then one or more additional representative clusters should be selected to derive additional standard deletion periods and, consequently, deletion classes are created.

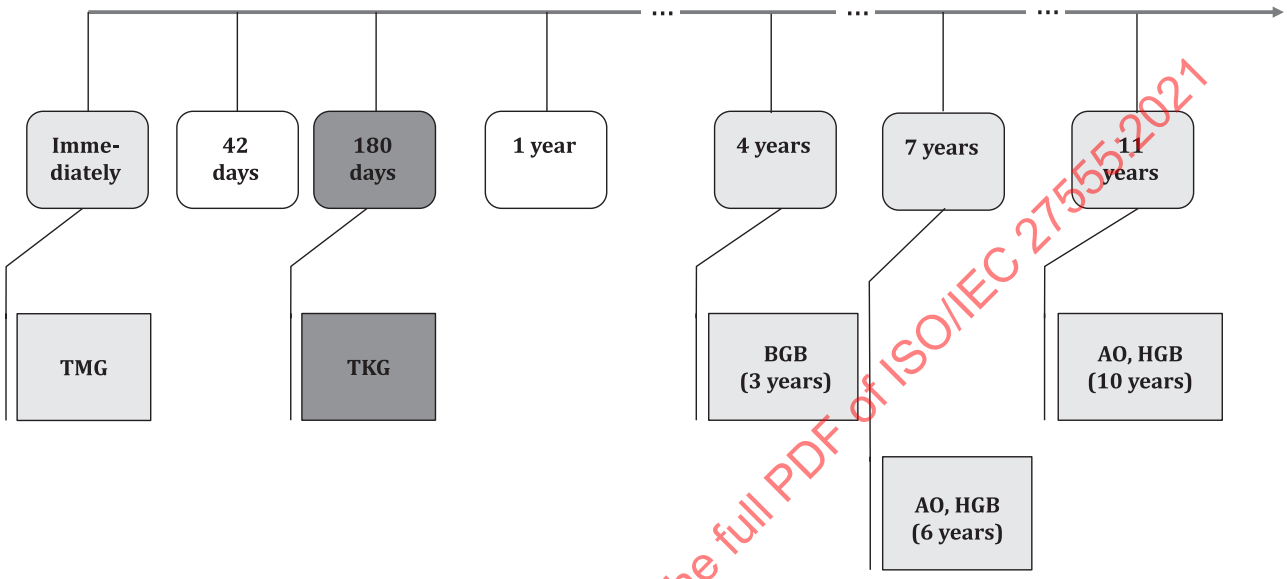
EXAMPLE A telecommunications provider uses, for instance, the period for the deletion of connection data for accounting purposes as a standard deletion period, while a motorway toll company uses the deletion period for trip data as a standard deletion period.

In some cases, it can be necessary to add additional standard deletion periods, particularly where a deletion period required is not defined, for example by legal and/or regulatory requirements. This is particularly true where the use of PII is only regulated by general legal provisions which provide, for example, only criteria for retention. Such criteria should be used to identify standard deletion periods,

and, where appropriate, the identification of additional standard deletion periods to fill gaps in standard deletion periods (see Figure 2).

Figure 2 shows an example of standard deletion periods from German legal regulations; one period is specific for a telecommunication company.

NOTE 2 The specification of very long deletion periods for all clusters of PII is not a good practice. This is also true for using long-term storage for undefined purposes (see 5.2). The freely selected standard deletion periods are appropriately used in the policies for deletion to respect the principle of necessity for the assigned cluster of PII in an acceptable manner.



Key

	time period derived from general laws
	time period derived from the Telecommunications Act
Blank cells	time period freely selected
AO	Fiscal Code
BGB	Civil Code
HGB	Commercial Code
TKG	Telecommunications Act
TMG	Telemedia Act

Figure 2 — Example of standard deletion periods derived from German legal regulations

7.4 Deletion period specifications for special situations

7.4.1 General

In operational practice, special situations can sometimes occur that cannot be handled by strictly applying the deletion rule of a previously assigned cluster of PII. These situations need to be documented and can consist of one or more situations discussed in 7.4.2 to 7.4.5.

7.4.2 Modification of data objects

In the context of processing, data objects of a cluster of PII can be modified and assigned to another cluster of PII (e.g. by statistical aggregation, pseudonymization). If the modified data objects are used

for another or a new purpose, then the new cluster of PII may be assigned to a different deletion period or starting point.

7.4.3 Need to extend period of active use

PII can be required for longer periods of time than is specified by the assigned regular deletion period, for example, because of a complaint case or a pending lawsuit. In such special cases, the PII controller should allocate the PII concerned to another cluster of PII with an appropriately longer deletion period if they determine that it is permitted.

NOTE 1 Technically, there are several options for allocating PII to another cluster of PII with a longer deletion period, e.g. by marking the data objects concerned or storing them in a different location or system.

EXAMPLE A cluster of PII which is needed for processing a complaint is called 'Complaint data'. The deletion rule for that PII is read as follows: 'One year after the end of the case handling'. The cluster of PII required for a lawsuit is allocated to the cluster of PII 'Dispute data'. The deletion rule also specifies a period of one year and refers to the date of the judgement becoming final as the starting point.

Even if the purpose of processing of PII is changed, the deletion rule can, if required, be adapted by allocating the cluster of PII to another cluster of PII.

NOTE 2 Legal constraints can restrict the changing of the purpose of processing of PII.

7.4.4 Suspension of the deletion

The regular deletion can be suspended for only a limited period. The applicability of these special situations (in particular, the identification of suitable cases and the management of repetitive cases) should be documented.

NOTE 1 Legal constraints can limit suspension of deletion rules.

NOTE 2 These situations include, for instance, program errors or erroneous cluster of PII, legal hold, investigation by government or enforcement agency.

EXAMPLE Requirements for error-handling processes are interpreted as 'Since a release cycle for the adjustment of IT systems generally has a duration of 6 months, the deletion period for erroneous sets of PII can generally be extended by 12 months. This provides for a margin sufficient to analyse the error and take measures for its elimination'.

The clusters of PII concerned should be kept as small as possible. The presence of special categories of PII and the measures for usage limitation during the exception should be used as criteria for the duration and permissibility of the suspension. The return to the regular mode of operation is completed when all PII subjected to the exceptional rule has been deleted. The measures by which the exception is ended should be monitored, documented and checked.

7.4.5 Backup copies

Backup copies regularly contain data objects of different clusters of PII whose regular deletion period is about to be reached and which would therefore need to be deleted. To ensure backup copies can be used for restore, they usually need to contain the complete image of data of a system. Deletion within a backup copy often destroys the copy.

However, for the purposes of recovery after a potential disruptive incident, the backup copies are stored for a certain period of time which usually exceeds the regular deletion period for some data objects for a limited time period. Therefore, the deletion period of the backup copies should be aligned according to the shortest deletion period and the sensitivity of the PII contained.

NOTE 1 Legal constraints can limit the margin for data contained in backup copies exceeding the regular deletion period.

NOTE 2 Legal constraints can set out a deletion period for a cluster of PII including backup copies. In such cases, the organizations can define a shorter regular deletion period for that cluster and use the remaining time as storage period for backup copies which are overwritten immediately after that period.

NOTE 3 The complexity of policies and procedures on deletion substantially increases if the deletion policy requires the deletion of backup copies within the regular deletion periods of the clusters of PII.

In exceptional cases, for instance to carry out documented checks after a complicated disruptive incident, longer retention periods of backup copies may be permitted.

Backup copies containing clusters of PII with a short regular deletion period should be overwritten after a short time, e.g. a couple of weeks. Backup copies containing only clusters of PII with a long regular deletion period may be stored for longer, e.g. for 3 months. In order to limit the complexity, only a few specific deletion rules for the backup copies should be specified.

If necessary, the PII controller should review the backup and recovery strategies according to the acceptable deletion periods for the backup copies. This should include separating sets of PII of different deletion periods into different backup copies.

Every backup copy typically contains data objects related to different clusters of PII. Therefore, the deletion rules for backup copies may not fit into the catalogue with clusters of PII and their deletion rules. Thus, it is recommended that deletion rules are defined in a backup policy (see 9.3).

8 Deletion classes

8.1 Abstract starting points — abstract deletion rules

A deletion rule consists of a deletion period and a specific point at which the deletion period starts.

The starting point refers to a condition which occurs in the life cycle of PII. The specific conditions can be determined by reference to the point in time at which the PII was collected or to a specific condition during the life cycle of PII. Thus, an abstract starting point can be:

— the collection of the PII, where the deletion period starts at the time of collection of the PII;

— the end of a procedure, where the deletion period starts on completion of a procedure in the life cycle of the PII;

— the end of the relationship with the PII principal, where the deletion period starts at the end of the relationship with the PII principal.

NOTE 1 The ‘end of the relationship with the PII principal’ is, strictly speaking, a special case of the second type. However, since the deletion period of several clusters of PII starts with the end of the relationship with the PII principal, this event is defined as a separate abstract starting point.

NOTE 2 PII controllers frequently use the PII of different categories of PII principals, e.g. employees, customers and contact persons of the contracting organizations. For every category, the ‘end of the relationship with the PII principal’ refers to a different condition.

EXAMPLE For a repair order, the starting point is ‘Handing-over of the repaired device to the customer’. For accounting records and the accompanying accounting documents, the starting point is the ‘Completion of the balance sheets’ in which the entries were taken into account. For the master data of a social network member, the starting point is ‘The link sent in the confirmation e-mail after deregistration has been requested’.

A deletion rule which refers only to a deletion period and an abstract starting point is referred to as an abstract deletion rule and builds a deletion class. To define a deletion rule for a cluster of PII in the catalogue, a specific event is identified as the starting point.

8.2 Matrix of deletion classes

Any of the possible combinations of standard deletion periods and abstract starting points defines a so-called deletion class.

Referring to the three abstract starting points described in 8.1, this results in three deletion classes per standard deletion period.

It is convenient to represent the deletion classes in a matrix. Figure 3 shows an example of a matrix of deletion classes according to the standard deletion periods from Figure 2 and the three abstract starting points. This matrix can be used to assist the establishment of policies and procedures for deletion. It has three functions:

— it gives a clear structure which helps to define a deletion rules catalogue with relatively low complexity, done by 'sorting' clusters of PII into the classes;

— it allows for the comparison of the rules by giving an overview, thus identifying inconsistencies at a high level of abstraction;

— it provides a graphical overview of the deletion rules.

Entering specific clusters of PII into the matrix can demonstrate that not all deletion classes are required, as some combinations of standard deletion periods and abstract starting points can be unpopulated (see also Figure 3). This enables a reduction in the complexity of the policies and procedures for deletion.

NOTE 1 Some of the standard deletion periods shown in Figure 3 are derived from German legal regulations as in Figure 2.

NOTE 2 The clusters of PII shown in Figure 3 are each representative for all clusters of PII which are sorted into the respective deletion class and contain all respective data objects, e.g. the cluster of PII 'contracts' keeps all contracts and the cluster 'Business letters' contains all business letters.

Abstract starting points	Standard deletion periods						
	Immediately	42 days	180 days	1 year	4 years	7 years	12 years
From collection			Connection data	Connection data requiring special analysis			
From end of procedure	Transient web-logs	Short-time documentation; operational logs	Itemised bill data	Documentation on informal communication	Complaint and receivables data	Business letters	Accounting data
From the end of the relationship				Supplementary master data		Contracts	Core master data

Key

	time period derived from general laws (see Figure 2)
	time period derived from German Telecommunications Act
Blank cells	time period freely selected

Figure 3 — Example matrix of deletion classes for a telecommunications service provider

8.3 Allocation of deletion classes and definition of deletion rules

Where possible, every cluster of PII should be allocated to a deletion class. If the retention period of a cluster of PII does not correspond to a standard deletion period, it is allocated to a deletion class having the next higher standard deletion period (see 7.1). If this is impractical, it should be checked whether another standard deletion period is needed or whether to specify an additional, specific deletion period (see 7.2).

NOTE 1 Legal requirements can limit the margin for the delay of deletion resulting from selecting the next higher standard deletion period.

To define and document a deletion rule, a specific starting point according to the deletion class needs to be identified. This starting point needs to be selected so as not to unnecessarily delay the deletion. If the starting point cannot be identified by automatic processes, a deletion process can also be enabled and triggered by functional or IT operational processes (see also 9.2).

NOTE 2 Legal requirements can limit the margin for the delay of deletion resulting from selecting the starting point. In some cases in the life cycle of the data objects, alternative starting points can be identified. Different combinations of starting points and standard deletion periods can result in different delays of deletion.

9 Requirements for implementation

9.1 General

Deletion rules should be documented without reference to the technology used (see 5.8). Specific measures should be defined in order to apply these deletion rules in information systems and in manual processes. Any document which contains such specific measures is considered to be 'requirements for implementation'. The description of specific measures may be integrated in existing documentation, e.g. system administrator handbooks or work instructions for manual processes.

To make the documentation specific for target groups and to reduce its complexity, separate documentation should be produced for information systems, for manual processes and other aspects of implementation (see Figure 4).

The PII controller should specify its policies for deletion, including where and how requirements for implementation are to be stated. These policies should include at least:

— requirements for implementation of deletion of PII, which should be used uniformly in the organization independently of the cluster of PII contained (e.g. backups, logs);

— specific requirements for implementation for individual IT systems;

— specific requirements for implementation for manual processes;

— requirements for implementation (instructions) for PII processors.

An example of a documentation structure is shown in Figure 4.

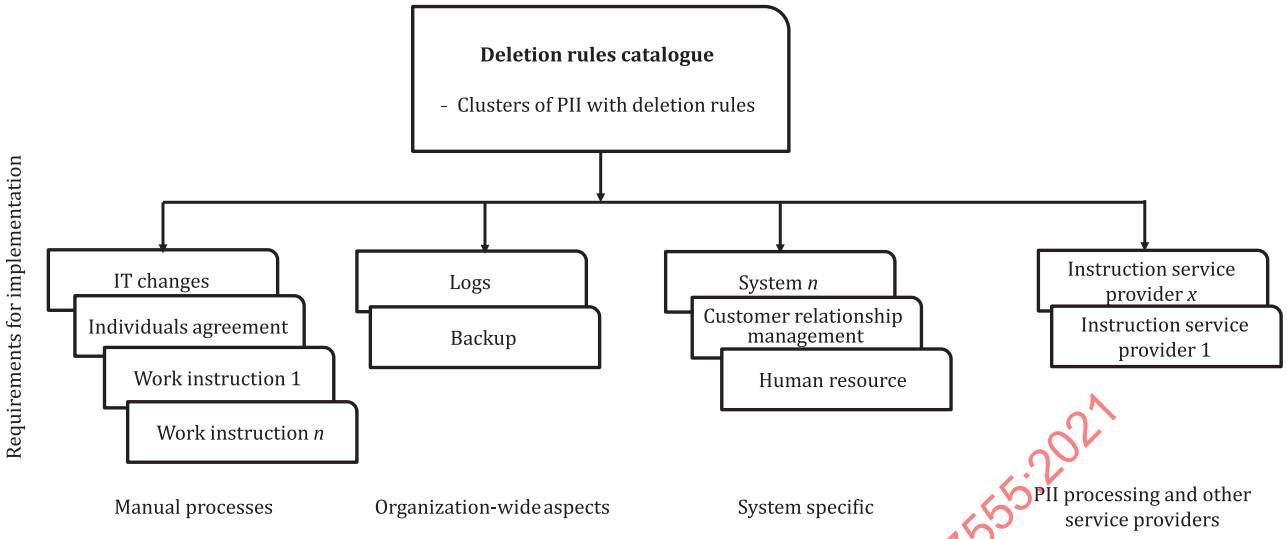


Figure 4 — Example of documentation structure

It should be taken into account that:

— there can be interactions and dependencies between the clusters of PII in different systems, for instance between customer master data in a customer relationship management (CRM) system, downstream order handling and an accounting system that is operated largely independently;

— due to replication, sets of PII can be stored in multiple systems, e.g. e-mails on the e-mail server, in local e-mail archives or on mobile devices.

The requirements for implementation of such sets of PII should ensure that the PII is deleted consistently.

Sometimes data objects of a cluster of PII are stored as multiple copies on multiple systems. However, for such data objects, it can be sufficient to store them after active use until the end of the retention period on only one system. Therefore, a shorter deletion period can, where applicable, be defined in the requirements for implementation for each system. This helps to satisfy the principle of data minimization. For decisions on these shorter periods, functional requirements and requirements of system operation should be taken into account.

NOTE 1 Backup copies are not understood as data 'stored on systems' (see 9.3).

Requirements for implementation documentation should include in which system the retention obligations will be fulfilled.

The deletion rules apply to different data objects. It is usually easier to delete a data object in its entirety. Every requirement for implementation should show clearly which deletion mechanisms are to be applied to which data objects.

Requirements for implementation should also include measures to deal with unstructured clusters of PII, e.g. e-mails.

Requirements for implementation serve several functions during their life cycle. They can define requirements for system development or procurement projects. For IT systems, they can document the implemented deletion mechanisms. For their operation, the required configuration parameters and values as well as, if necessary, additional boundary conditions and guidance for monitoring the deletion mechanisms should be described. The organization, third parties or both should also be able to determine whether or not deletion has been carried out. This generally requires proof. The type of proof available should be specified in the requirements for implementation, e.g. by defining deletion run log entries. The duration for which such proof should be retained should be defined in a deletion rule. Requirements for implementation can also support audits as they provide reference information for the audit conditions.

The 'requirements for implementation' should document the following:

— the specific information systems, sets of PII or both that apply;

— the clusters of PII that are within its scope;

— the deletion rules that are used for which clusters of PII;

— the conditions which initiate the start period as stated in the deletion rule;

— the mechanisms that are used for the deletion processes (if required, the mechanisms need to be such that the appropriate security processes are implemented);

— where the deletion mechanisms are configurable, the parameters that are used with specific clusters of PII in order to determine which PII is to be deleted;

— responsibilities for starting and monitoring the mechanisms;

— the recording of the execution of the deletion operations, e.g. in log entries;

— in the case of data recovery, the specific measures that are required to delete PII that has already exceeded its deletion period.

NOTE 2 During recovery processes, it can be necessary to implement deletion mechanisms, for example, to identify and delete the PII that has exceeded its deletion period.

The deletion mechanisms specified in the requirements for implementation should take into account the security requirements of the respective cluster of PII. Deletion mechanisms should be selected which can demonstrate compliance with legal requirements. To this end, the PII controller should reference an available security classification system.

9.2 Conditions for starting points outside IT systems

Organizations prefer to delete PII automatically. Automated deletion mechanisms should only be implemented where they ensure that the conditions for deletion are met. However, for some clusters of PII, not all information required for implementing deletion is available within the systems. Under these circumstances, manual checks should be carried out prior to deletion mechanisms being initiated.

EXAMPLE 1 For instance, the legal retention period for taxation documentation might not expire when the related assessment period has not yet expired. Thus, the respective deletion is only executed when approved by a person in charge in the responsible department and not automated within the system.

EXAMPLE 2 Where a contract with an undefined end date is in operation, the deletion function will need to take into account the date at which the end date is reached. Thus, manual intervention will be needed to initiate deletion.

Requirements for implementation should document whether deletion runs are controlled by external conditions and how these conditions are triggered.

9.3 Requirements for implementation for organization-wide aspects

9.3.1 General

Some implementation tasks of deletion do not depend on specific systems or clusters of PII. Result of such tasks are called requirements for implementation for organization-wide aspects.

9.3.2 Backup

As backup copies contain mixed data and are generated for system recovery, deletion rules cannot be applied within backup copies. Backup copies are not archives (see 5.4). Backup copies might need to be retained for longer than the regular deletion period of some contained data objects (see 7.4).

The retention of backup copies should be linked to the retention of the clusters of PII contained within the backup copies. The retention of backup copies should be documented, for example in backup policy.

NOTE Legal requirements can limit the margin for the delay of deletion resulting from keeping data in backup copies exceeding the regular deletion period. An option to reduce such delays is to subdivide the clusters of PII to backups with different retention periods related to the clusters of PII contained.

In exceptional cases, backup copies containing PII can be generated for environments different from the production one, for instance, for test or development environments. The requirements for implementation should also apply to these environments. Such situations should be managed, for example, by change management processes.

9.3.3 Logs

If logs contain PII, they should be allocated to the respective clusters of PII. Where specific PII is logged by different systems, deletion should be implemented while taking into account organization-wide requirements. Individual clusters of PII can be specified for different types of logs or log entries.

In some cases, logs contain attributes related to a specific cluster of PII. In such cases, the logs, the entries in the log or at least the attributes should be deleted no later than those of the original cluster of PII.

9.3.4 Transmission systems

Some systems are used for transmission purposes only, for instance communication servers or middleware components in service-oriented architectures. After successful transmission, clusters of PII or metadata related to the cluster of PII that has been transmitted may be retained within the transmission systems for a short period of time for validation or to handle errors, and then deleted. This short period of time should be such that regular deletion periods are not compromised.

To demonstrate that transmission systems are included in the deletion framework, the PII controller should maintain a list of transmission systems. This list should link to the shortest deletion rule of a cluster of PII retained within those transmission systems.

9.3.5 Repair, dismantling and disposal of systems and components

Data storage media can still contain PII if they are reused for new purposes or scrapped. The relevant legal requirements can require the PII to be protected from misuse. Thus, secure deletion of the PII is a suitable measure before the data storage media can be reused. Alternatively, the data storage media can be disposed of if it is ensured that the PII will be inaccessible during and after this process, and that it is destroyed with the security level required. This applies to all kinds of data storage media, such as hard drives, USB flash drives, mobile devices, SD cards, CDs and DVDs. It also applies to all instances of virtual systems.

In order to minimize the risk of misuse, the sets of PII contained in the data storage media should be deleted as soon as possible after the dismantling of the system. The deletion mechanisms should be consistent for all systems within the organization. These mechanisms can already exist for other reasons, for instance in order for a confidentiality classification to be implemented. In this case, the aspects of the policies and procedures for deletion can be integrated.

It can be necessary to prove which data storage media were deleted and which were destroyed. Supplementary to the requirements for implementation related to the ‘dismantling of systems’, it is thus appropriate to keep an ‘inventory of the data storage media’ and to provide documentation of the deletion or destruction processes.

9.3.6 Everyday business life

For the general office operation, deletion rules should be specified, for instance, for the handling of documents from completed projects or for e-mails. These requirements for implementation should