



**SLOVENSKI STANDARD**  
**oSIST prEN ISO/IEC 27555:2026**  
**01-julij-2026**

---

**Informacijska varnost, kibernetika varnost in varstvo zasebnosti - Smernice o izbrisu identifikacijskih podatkov (ISO/IEC DIS 27555:2026)**

Information security, cybersecurity and privacy protection - Guidelines on personally identifiable information deletion (ISO/IEC DIS 27555:2026)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Leitlinien für die Löschung personenbezogener Daten (ISO/IEC DIS 27555:2026)

Sécurité de l'information, cybersécurité et protection de la vie privée - Lignes directrices relatives à la suppression des données à caractère personnel (ISO/IEC DIS 27555:2026)

Ta slovenski standard je istoveten z: **prEN ISO/IEC 27555**

---

**ICS:**

35.030            Informacijska varnost            IT Security

**oSIST prEN ISO/IEC 27555:2026**            **en,fr,de**

# Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)



# DRAFT International Standard

## ISO/IEC DIS 27555

### 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 données  
à caractère personnel*

ICS: 35.030

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:  
**2026-05-29**

Voting terminates on:  
**2026-08-21**

This document is circulated as received from the committee secretariat.

**ISO/CEN PARALLEL PROCESSING**

Reference number  
ISO/IEC DIS 27555:2026(en)

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS 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.

© ISO/IEC 2026

# Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)



## **COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2026

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

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

© ISO/IEC 2026 – All rights reserved

## ISO/IEC DIS 27555:2026(en)

## Contents

	Page
<b>Foreword</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Symbols and abbreviated terms</b> .....	<b>3</b>
<b>5 Framework for deletion</b> .....	<b>3</b>
5.1 General.....	3
5.2 Constraints.....	4
5.3 Clusters of PII.....	4
5.4 Retention period and regular deletion period.....	5
5.4.1 Retention period.....	5
5.4.2 Regular deletion period.....	5
5.4.3 Allocation of clusters of PII.....	6
5.5 Archives and backup copies.....	6
5.6 Standard deletion periods, starting points, deletion rules and deletion classes.....	7
5.7 Special situations.....	7
5.8 Documentation of policies and procedures.....	8
<b>6 Clusters of PII</b> .....	<b>8</b>
6.1 General.....	8
6.2 Identification.....	10
6.3 Documentation.....	10
<b>7 Specification of deletion periods</b> .....	<b>11</b>
7.1 Standard and regular deletion periods.....	11
7.2 Regular deletion period specifications.....	12
7.3 Standard deletion period identification.....	12
7.4 Deletion period specifications for special situations.....	13
7.4.1 General.....	13
7.4.2 Modification of data objects.....	13
7.4.3 Delayed deletion by allocation to another cluster of PII.....	14
7.4.4 Suspension of the deletion.....	14
7.4.5 Backup copies.....	14
<b>8 Deletion classes</b> .....	<b>15</b>
8.1 Abstract starting points — abstract deletion rules.....	15
8.2 Matrix of deletion classes.....	16
8.3 Allocation of deletion classes and definition of deletion rules.....	17
<b>9 Requirements for implementation</b> .....	<b>17</b>
9.1 General.....	17
9.2 Conditions for starting points outside IT systems.....	20
9.3 Requirements for implementation for organization-wide aspects.....	20
9.3.1 General.....	20
9.3.2 Backup.....	20
9.3.3 Logs.....	21
9.3.4 Transmission systems.....	21
9.3.5 Repair, dismantling and disposal of systems and components.....	21
9.3.6 Everyday business life.....	22
9.4 Requirements for implementation for individual IT systems.....	22
9.5 Deletion in regular manual processes.....	23
9.6 Requirements for implementation for PII processor.....	23
9.7 Control deletion in special cases.....	23
9.7.1 Exception management.....	23

**ISO/IEC DIS 27555:2026(en)**

9.7.2	Further sets of PII.....	24
9.8	Handle individual requests for deletion or suspension of deletion.....	25
<b>10</b>	<b>Responsibilities.....</b>	<b>25</b>
10.1	General.....	25
10.2	Documentation.....	26
10.3	Implementation.....	26
	<b>Bibliography.....</b>	<b>27</b>

# Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)

## ISO/IEC DIS 27555:2026(en)

### 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](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://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](http://www.iso.org/patents)) or the IEC list of patent declarations received (see [patents.iec.ch](http://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](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://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](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

**ISO/IEC DIS 27555:2026(en)****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. Processes 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 including deletion or suspension of deletion on individual requests.

# Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)

# 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 processes and 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 <https://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.