SLOVENSKI STANDARD
SIST EN 15713:2023

01-december-2023

Varno uničevanje zaupnega in občutljivega gradiva - Pravila ravnanja

Secure destruction of confidential and sensitive material - Code of practice

Sichere Vernichtung von vertraulichen Unterlagen - Verfahrensregeln

Destruction sécurisée de documents confidentiels - Code d'usages

Ta slovenski standard je istoveten z: **EN 15713:2023**

ICS:

13.310	Varstvo pred kriminalom	Protection against crime

SIST EN 15713:2023 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 15713

September 2023

ICS 13.310

Supersedes EN 15713:2009

English Version

Secure destruction of confidential and sensitive material - Code of practice

Destruction sécurisée de documents confidentiels - Code d'usages

Sichere Vernichtung von vertraulichen Unterlagen - Verfahrensregeln

This European Standard was approved by CEN on 24 April 2023.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. EN 15713:2023 E

Contents

Page

European foreword

This document (EN 15713:2023) has been prepared by Technical Committee CEN/TC 263 “Secure storage of cash, valuables and data media”, the secretariat of which is held by BSI.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by March 2024, and conflicting national standards shall be withdrawn at the latest by March 2024.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN 15713:2009.

In comparison with the previous edition EN 15713:2009, the following technical modifications have been made:

This document has been technically revised to provide a benchmark for the appropriate processes and procedures available for any person or organization that seeks to safely destroy confidential or sensitive material when it is no longer required.

In addition, this document is also intended to be applicable to objects requiring destruction to ensure product or brand integrity.

In this context, securely destroyed means that any object or data carrier containing confidential or sensitive data is destroyed in such a way that reproduction of the information on them is either impossible or is only possible with considerable expenditure (in terms of personnel, resources and time). Destruction outcome tables are contained in Annex A (Tables A.1 to A.7).

The process criteria are specified in Table B.1 in Annex B.

Any feedback and questions on this document should be directed to the users’ national standards body. A complete listing of these bodies can be found on the CEN website.

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

1 Scope

This document provides recommendations and requirements for the procedures, processes and performance monitoring to be implemented for the management and control of the physical destruction of confidential and sensitive material to ensure that such material is disposed of securely and safely.

This document can be referenced by anyone who processes such material on behalf of others and covers the following scenarios:

— on site - using mobile equipment at the location of use (destruction equipment is brought to the confidential or sensitive material);

— off site - transport followed by destruction using equipment at a destruction facility (the confidential or sensitive material is brought to the destruction equipment, such as used at a dedicated external facility operated by a service provider);

— use of equipment at the Data Controller's location (confidential or sensitive material and destruction equipment co-located, such as a shredder in a building occupied by a client or clients).

Destruction by erasure (e.g. crypto erasure, data overwriting, degaussing or other forms of magnetic/electronic erasure) is not covered in this document.

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.

EN 50131-1[1], *Alarm systems — Intrusion and hold-up systems — Part 1: System requirements*

EN 62676-4, *Video surveillance systems for use in security applications — Part 4: Application guidelines*

ISO/IEC 21964-2:2018, *Information technology — Destruction of data carriers — Part 2: Requirements for equipment for destruction of data carriers*

EN 1627, *Pedestrian doorsets, windows, curtain walling, grilles and shutters — Burglar resistance — Requirements and classification*

EN 1628, *Pedestrian doorsets, windows, curtain walling, grilles and shutters — Burglar resistance — Test method for the determination of resistance under static loading*

EN 1629, *Pedestrian doorsets, windows, curtain walling, grilles and shutters — Burglar resistance — Test method for the determination of resistance under dynamic loading*

EN 1630, *Pedestrian doorsets, windows, curtain walling, grilles and shutters — Burglar resistance — Test method for the determination of resistance to manual burglary attempts*

[1] As impacted by EN 50131-1:2006/A1:2009, EN 50131-1:2006/A2:2017 and EN 50131-1:2006/A3:2020.

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— IEC Electropedia: available at https://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1.1
access to documents or materials
ability to obtain or retrieve confidential or sensitive materials

3.1.2
access to secure area
ability to physically enter a secure area

3.1.3
authorized person
individual granted unaccompanied access to confidential or sensitive material in accordance with the needs of their job who has been security cleared to the prevailing national standard or specified requirement, to the extent applicable

Note 1 to entry: An authorized person must not be given access to confidential or sensitive material of protection class HS.

3.1.4
Certificate of Destruction
confirmation that the confidential and sensitive material recorded on the Certificate of Destruction has been through the destruction process and the material has been destroyed

3.1.5
client
owner of confidential or sensitive material who retains a company to provide destruction services in accordance with an agreed contract

3.1.6
company
entity employed by the client designated as a service provider offering one or more capabilities, typically on a commercial basis, to whom the client has delegated one or more tasks relating to the destruction process

3.1.7
competent person
individual with necessary knowledge and skill gained through relevant experience, training and qualification

3.1.8
confidential information
examples of confidential information include stored facts or knowledge such as medical records, financial records, software source code or metadata contained on data carriers, the confidentiality of which the client wishes to protect

3.1.9
contract
documented agreement covering all transactions between the client and the company

3.1.10
critical supplier
contractors with personnel or suppliers who provide equipment that will be used in any area, including vehicles, where confidential or sensitive material are stored or destroyed

3.1.11
data controller
natural or legal person, public authority, agency or other body who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal data are, or are to be, processed, e.g. owners of personal data will be data controllers

3.1.12
data processor
natural or legal person, public authority, agency or other body who processes the data on behalf of the data controller, e.g. destruction company and service providers destroying personal data will be data processors

3.1.13
deforming of data carrier
process of making a data carrier unreadable

Note 1 to entry: Deforming Category H material to the extent that the disk or media cannot be passed over a reader as a means of data destruction, can be specified up to and including level 3.

3.1.14
destruction
physical process after which confidential or sensitive material becomes non-confidential or non-sensitive material

Note 1 to entry: Examples of physical processes include disintegration, shredding, dissolution or any other process which renders material or data unusable or unreadable. Example of a non-physical process might include encryption, which is outside the scope of this document.

3.1.15
destruction engine
actual destruction mechanism itself

3.1.16
destruction equipment
combination of equipment which can include container lifting/transfer mechanisms, infeed conveyors and hoppers, destruction engine/mechanism such as shredders, granulators, cutting units or knives, together with discharge conveyors

3.1.17
destruction facility
service provider premises where destruction equipment is set up and operated

3.1.18
destruction outcome
reduction in size or reduction in composition dependant on the security level chosen and the level of effort required to recover information or reconstitute the materials

3.1.19
destruction output
material that has been through the destruction process, as specified in this document

3.1.20
dissolved
process by which any information or trace of information held on data bearing materials is dispersed so as to be completely erased and destroyed

3.1.21
holding site
geographically separate non-destruction site of the service provider for the secure retention of confidential and sensitive material designated for destruction prior to the ultimate transport to the destruction facility

3.1.22
locked
physically secured to prevent unauthorized access

Note 1 to entry: This includes access to secure areas and confidential or sensitive materials. Unlocking requires a protected input to open such as a key, token, RFID lock, passphrase or PIN.

3.1.23
material type
differentiation of confidential and sensitive material dependent on the information density and the scale of information combined with the construction of the object

3.1.24
protection class
classification of the protection requirement of confidential and sensitive material

3.1.25
record
document describing an event or completion of a process

3.1.26
sealed
physically secured by means of an attached tamper-evident seal restricting access to and withdrawal of confidential and sensitive documents or materials

3.1.27
secure area
building, room, reception area or shredding/destruction compartment of a mobile destruction vehicle or an area containing confidential and sensitive material which is controlled and protected from unauthorized access

3.1.28
security bag
sealable opaque bag designed to securely contain confidential or sensitive material whilst in storage or transit prior to destruction

3.1.29
security clearance
status granted to individuals, via thorough background checks in jurisdictions where it is legally possible to do so and / or to a data controller's specific requirements, allowing them access to confidential and sensitive materials and secure areas

Note 1 to entry: Security clearance does not grant individuals access to confidential information of protection class HS.

3.1.30
security container
lockable container, e.g. a console or bin capable of providing secure protection of confidential or sensitive material including data carriers

3.1.31
security level
classification of the effort needed to recover data and/or information or reconstitute objects to their original form

3.1.32
sensitive material
all objects containing confidential information or sensitive data (paper, film, optical, electronic) and other objects containing sensitive material (validation seals, mechanical/electronic lock keys, defective products, obsolete branded merchandise)

3.1.33
service provider
organization or individual, including subcontractors, offering one or more capabilities relating to the destruction process, typically on a commercial basis, to whom the client has delegated one or more tasks

3.1.34
shredded ash
residue of incinerated data bearing materials whereby any information or trace of information held on them is completely erased and destroyed

3.1.35
subcontractor
service provider not directly employed by the Client, contracted to carry out work on behalf of the Company

3.2 Abbreviations

GPS Global Positioning System

HS Highly Sensitive

OS Official Sensitive

RC Routine Confidential

RFID Radio Frequency Tracking Device

VSS Video Surveillance Systems (CCTV)

4 Protection class

4.1 General

This document recognizes that clients and data controllers will determine the security and protection requirements with regard to processes to be followed after confidential or sensitive material is allocated for destruction through to the point at which material has been destroyed.

The degree of the material sensitivity or its data and information content will inform and determine the need to protect it from violation of the basic principles of confidentiality and integrity, taking into account the harm which would result from such a violation.

There are three classifications of protection:

— routine confidential - requiring normal protective measures;

— official sensitive - requiring heightened protective measure;

— highly sensitive - requiring very high protective measures.

NOTE See criterion in Annex B, at B.1.1.

4.2 Determination of the protection class

In order for the destruction of data carriers to comply with the principles of economy and proportionality, the data contained on them shall be assigned a protection class. The security level which is chosen for the destruction of the data carriers is determined by the protection level of the data.

Protection class RC (Routine Confidential), normal protection level for internal data:

— the most common classification of information, intended for large groups of people;

— unauthorized disclosure or transfer would have limited negative effects on the organization;

— protection of personal data shall be ensured. Otherwise, there is a risk that persons affected may suffer damage to their reputation and economic circumstances.

Protection class OS (Official Sensitive), higher protection level for confidential data:

— the information is restricted to a small group of people;

— unauthorized disclosure would have serious effects on the organization and may lead to violation of laws or contractual obligations;

— the protection of personal data shall meet stringent requirements. Otherwise, there is a risk that persons affected may suffer serious damage to their social standing or economic circumstances.

Protection class HS (Highly Sensitive), very high protection level for strictly confidential and secret data:

— the information is restricted to a very small group of named persons, who are authorized to access the documents or materials;

— unauthorized disclosure would have serious (existence-threatening) effects on the organization and/or would lead to violation of professional secrets, contracts and laws;

— the protection of personal data shall be strictly ensured. Otherwise, the life and safety of persons affected may be at risk, or their personal freedom may be jeopardized.

5 Determination of security level

A level of destruction is to be determined by selection of an outcome, taking into account:

— the state of the art;

— the costs of implementation;

— the nature, scope, context and purposes of processing;

— the risk of varying likelihood and severity of a security breach.

The client as controller and the company/service provider as processor shall implement and approve technical and organizational measures and the method of destruction to ensure a level of security appropriate to the risk, including the ability to ensure the ongoing confidentiality, integrity, and resilience of processing systems and services until the material is destroyed to the required destruction outcomes specified in the Annex A, Tables A.1 to A.7, to ensure that it is unreadable, illegible, unusable and unable to be reconstructed.

A security level from 1 to 7 together with the method of destruction shall be chosen that is applicable to the protection class and that will provide the destruction outcome approved by the client. See Table 1 below.

Table 1 — Assignment of security levels and protection classes

Protection class	Security levels						
	1	2	3	4	5	6	7
RC	x [a]	x [a]	x				
OS			x	x	x		
HS				x	x	x	x

[a] This combination cannot be used for personal data.

NOTE See criteria in Annex B, at B.1.1 and B.2.1.

6 Increasing the security level

For destruction output within Category P, or separately, Category F only, material which has been destroyed to security level 1, 2 or 3, mixing and compacting may increase security to the next higher level once only, up to a maximum of security level 4 provided the following criteria are met:

— mixing comprises a minimum of 100 kg of any single Category P and Category F Material Type to be presented as the aggregate mass of particles or fragments within the destroyed output which shall be destroyed in a single, uninterrupted cycle of the machine or equipment;

— the company/service provider obtains explicit confirmation from the Client that the methods of increasing the security level may be applied for this specific work order.

Mixing and compacting material destroyed at security levels 1 and 2 shall not be used as a means of increasing the security level for the destruction of personal data classified as Material Category P.

It is recommended that the client or data controller of the material gives consideration to the storage of the destruction output. A paper document is easier to reconstitute if all of its particles are kept in one place. It is recognized that mixing and compacting destruction output in larger volumes and from multiple sources dissipates the waste and may make reconstitution less likely. This does not affect the possible information content of individual particles of material.

When selecting a security level, the density and/or size of the represented information on the data carrier shall be taken into consideration. If the colour or other characteristics of the data carrier make it easier to reconstruct, a higher security level may have to be selected.

7 Destruction equipment

7.1 General

The following requirements apply to all physical destruction equipment and related procedures. These apply at any location: client site, mobile vehicle, or at a destruction facility.

7.2 Use of destruction equipment

Destruction equipment shall be operated by authorized personnel that are trained and in line with Clause 9 and 13.3, Controlled access to that equipment.

For category P documents or materials that are protection class HS operating staff shall not have physical access to documents or materials with presentation in original size. The machine, used for the destruction of the data carrier, is fed either by dumping the content out of the security containers directly into the machine or hopper or by a secured feed device. This requirement shall be understood in such a way that ANY access to documents or materials, be it in the normal process of destruction or by design features of the plant in question, is physically prohibited. Therefore, the transfer of data carriers (e.g. from large volume security containers) into a collection hopper or bunker as well as the option of manual sorting, is not sufficient to meet the requirements of protection class HS. This is due to fundamental design principles which may result in data carriers remaining in the open area as part of the regular process, requiring manual removal. Any deviation is only permissible in case of technical faults of the destruction engine itself or of the container lifting/transfer mechanism (e.g. in case of fire).

NOTE 1 See criterion in Annex B, at B.7.1.

With the exception of category P documents or materials at protection class HS, the handling of loose confidential data carriers (such as reloading or emptying) is permitted only within a secure area.

NOTE 2 See criterion in Annex B, at B.5.9.

In the event that material of different protection class or security level become mixed then all material shall be destroyed at the highest security level required.

NOTE 3 See criterion in Annex B, at B.10.

Any and all changes of sieve basket and / or cutting unit shall be documented, including details of the destruction unit, the sieve hole diameter and/or the cutting width of the sieve basket, both installed and uninstalled, as well as the time of completion of the change. All measurements are to be listed in millimetres.

NOTE 4 See criterion in Annex B, at B.7.3.

7.3 Operating instructions

Instructions to enable the operator to achieve the destruction outcome shall be available at the destruction service provider premises.