SLOVENSKI STANDARD
oSIST prEN 15713:2022

01-junij-2022

Varno uničevanje zaupnega gradiva - Pravila ravnanja

Secure destruction of confidential material - Code of practice

Sichere Vernichtung von vertraulichen Unterlagen - Verfahrensregeln

Destruction sécurisée de documents confidentiels - Code d'usages

Ta slovenski standard je istoveten z: **prEN 15713**

ICS:

13.310 Varstvo pred kriminalom Protection against crime

oSIST prEN 15713:2022 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 15713

March 2022

ICS 13.310

Will supersede EN 15713:2009

English Version

Secure destruction of confidential material - Code of practice

Destruction sécurisée de documents confidentiels - Code d'usages

Sichere Vernichtung von vertraulichen Unterlagen - Verfahrensregeln

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/TC 263.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CEN 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, Turkey and United Kingdom.

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.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

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

Contents

Page

European foreword

This document (prEN 15713:2022) 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 document is currently submitted to the CEN Enquiry.

This document will supersede EN 15713:2009.

In comparison with the previous edition, 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.

This document is intended to be applicable for objects requiring destruction to ensure product or brand integrity.

In this context, safely destroyed means that any object or data carrier containing confidential or sensitive data must be 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).

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 mechanical 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 for themselves or 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);

— using static equipment at the location of use (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 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 50131-1:2006,[1] *Alarm systems – Intrusion and hold-up systems – 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 1627:2021, *Pedestrian doorsets, windows, curtain walling, grilles and shutters — Burglar resistance — Requirements and classification*

EN 1628:2021, *Pedestrian doorsets, windows, curtain walling, grilles and shutters — Burglar resistance — Test method for the determination of resistance under static loading*

EN 1629:2021, *Pedestrian doorsets, windows, curtain walling, grilles and shutters — Burglar resistance — Test method for the determination of resistance under dynamic loading*

EN 1630:2021, *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

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

ISO and IEC maintain terminological 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

— COD = Certificate of Destruction

— GDPR = Regulation (EU) 2016/679 (General Data Protection Regulation)

— VSS = Video Surveillance Systems (CCTV)

— RC = Routine Confidential

— OS = Official Sensitive

— HS = Highly Sensitive

— ANPR = Automatic number-plate recognition

3.1
authorized person
trusted individual granted unaccompanied access to confidential or sensitive material in accordance with the needs of their job who has been security cleared to the appropriate national standard

3.2
Certificate of Destruction (COD)
confirmation that the confidential and sensitive material recorded on the COD has been through the destruction process

3.3
client
owner of confidential or sensitive material who retains a company to provide destruction services in accordance with an agreed contract

3.4
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

3.5
competent person
individual with necessary knowledge or skill gained through relevant experience, training or qualification

3.6
confidential information
stored facts or knowledge such as medical records, financial records or software source code contained on data carriers, the confidentiality of which the client wishes to protect

3.7

contract
written document covering all transactions between the client and the company

3.8
critical supplier
contractors that supply personnel or suppliers who provide equipment that will be used in any area, including vehicles, where confidential or sensitive material may be stored or destroyed

3.9
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. Owners of personal data will be data controllers

3.10
data processor
natural or legal person, public authority, agency or other body who processes the data on behalf of the data controller. Destruction company and service providers destroying personal data will be data processors

3.11
deforming of data carrier
process of making a data carrier unreadable

Note 1 to entry: Deforming Category E 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.

3.12
destruction
process through which confidential or sensitive material becomes waste

3.13
destruction outcome
reduction in size or reduction in composition such that the material becomes, unreadable, illegible, unusable and unable to be reconstructed

3.14
destruction output
material that has been through the destruction process and is converted to waste, as defined in this document

3.15
documented procedure
recorded description of a process to be followed to meet an objective

3.16
destruction facility
premises or mobile destruction vehicle where destruction equipment is set up and operated

3.17
holding site
non-destruction site of the service provider for the secure retention of confidential and sensitive material designated for destruction prior to the transportation to the destruction facility

3.18
locked
physically secured to prevent unauthorised access and requiring a protected input to open such as a key, token or passphrase

3.19
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

3.20
protection class
classification of the protection requirement of confidential and sensitive material

3.21
record
paper or electronic document describing an event or completion of a process

3.22
sealed
physically secured by means of an attached plastic pull tight seal, adhesive seal tape or other tamper-evident seal preventing access and withdrawal of confidential and sensitive material

3.23
secure area
building, room, reception area or shredding compartment of a mobile destruction vehicle or an area containing confidential and sensitive material which is controlled and protected from unauthorised access

3.24
shredding bag
sealable opaque bag designed to securely contain confidential or sensitive material whilst in storage or transit prior to shredding

3.25
security container
lockable container, e.g. a console or bin capable of providing secure protection of confidential or sensitive material including data carriers

3.26
security level
classification of the effort needed to recover data and/or information or reconstitute objects to their original form

3.27
sensitive material
any object or data carrier which, if compromised, would have an adverse impact on the client; or any individual, organisation connected to the object. Sensitive material includes 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)

3.28
service provider
organisation 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

3.29
subcontractor
service provider or a transport service provider not directly employed by the Client, contracted to carry out work on behalf of the Company

3.30
transport service provider
entity offering a capability to convey confidential or sensitive material to a destruction facility

3.31
VSS
Video Surveillance Systems – formerly called CCTV

3.32
waste
output from the destruction process that is no longer sensitive or confidential where the material meets the destruction output as specified by the client

3.33
written notification
paper or electronic communication whereby the delivery of the message to the recipient is confirmed; for example a letter sent by recorded post or electronic mail where a read-receipt is received

4 Protection class

4.1 General

This document recognizes that clients and data controllers will determine different security and protection requirements with regard to processes to be followed after confidential or sensitive material is allocated for destruction through to the point that material is 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, integrity and availability, taking into account the harm which would arise 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.

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 persons, known by name, who are authorized to access it;

— 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

5.1 General

A level of destruction is to be determined by selection of an outcome that produces waste that is no longer confidential or sensitive.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as 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 appropriate technical and organisational 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 outcome (GDPR Article 32. One (b)) 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 appropriate to the Protection Class that will provide the destruction outcome approved by the client as appropriate for the confidential and sensitive material on completion of destruction. See Table 2 below.

Table 2 — 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.

6 Increasing the security level

6.1 General

For destruction output within Category P and 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 is met:

— mixing comprises a minimum of 100 kg of any single Category P 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 once it has been converted to waste. 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 the appropriate 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 mechanical 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 appropriately trained or the operation is observed by authorized personnel in line with Clause 9, Controlled access.

Operating staff shall not have access to un-shredded data carriers 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