Data Protection Authority

Recommendation on data sanitisation and data medium destruction techniques

WARNING: This document is intended to provide additional explanation to the rules in force and does not exempt the controller from its obligations and responsibilities under the GDPR and other applicable texts. Considering its requirements and the risk analysis that it carries out or plans, it shall use one or the other tool and method, given in particular the evolution of knowledge and technologies. The different tools and brands cited in this document are cited for the sole purpose of providing examples. The Authority makes no representation as to their compliance with the GDPR and other regulations or as to their quality and performance.

TABLE OF CONTENTS

Summary

The Data Protection Authority (DPA) fulfils many tasks, including informing citizens, businesses and public players on certain issues related to data protection. Among these issues, those related to the 'secure' disposal of data or data media are certainly recurrent.

Regardless of their motivations, controllers wish to carry out this operation but sometimes lack a clear vision of what constitutes a satisfactory result (in particular in terms of the protection of personal data) and how to achieve such a result.

The scarcity, at the international level, of reference documents on the subject, or even their absence at the European and national levels, combined with the desire of the DPA to provide interested parties with a useful guide in the form of clear, up-to-date and comprehensive guidelines, are the basis of this recommendation.

This document presents the various existing "sanitisation" techniques (overwriting, cryptographic erasure, degaussing, etc.) for different types of media (HD, SSD, paper, etc.) which either make access to the data impossible on a preserved medium (erasure without the option of recompilation and encryption), or result in the destruction of the medium (without the option of reconstruction).

The recommendation also addresses this processing (sanitisation and destruction) more broadly by detailing its various aspects, both legal (in particular related to the GDPR) and technical or organisational and examines the processing from before the purchase of the medium to the verification and recording of results.

Finally, a summary table shows the reader, according to the type of medium, the recommended sanitisation and destruction techniques to achieve the desired level of confidentiality.

While the principles and concepts discussed in this document are by nature relatively perennial, there are certain tools, methods or examples presented which, in view of the evolution of knowledge and technologies in the field, may need to be updated more rapidly. The paragraphs or parts of the text potentially concerned are preceded by '\\' (double backslashes).

1. Introduction

01. As part of their activities, the controller[1] encounters many situations in which they wish to ensure that the transfer of information media to another environment does not lead to an unauthorised disclosure of the data contained on these media.

These situations in which the controller will have to take a decision on the "sanitisation[2]" of data are often linked to the end of their life cycle or that of their medium, or to their reuse in a different security[3] context.

02. For example:

- Scrapping of decommissioned IT equipment (in the broad sense[4]);
- Sending of a photocopier for repair;
- Disposal of paper archives;
- Sorting of HR department files;
- Transfer of computers to a charity;
- Return of PCs in the context of a lease;
- The end of the rental agreement for a multifunction printer;
- Or the sale, after amortisation, of the company's desktops and laptops to staff members.

03. The controller may have diverse motives, such as the need to protect data of particular value to it or classified as 'confidential', the desire to stand out from the competition, the fear of a penalty[5] and/or the desire to comply with the laws in force.

---

[1] Article 4.7 of the GDPR defines a "controller" as the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

[2] The expression "data sanitisation" covers the notion of deep sanitisation (disinfection, cleaning) leaving no trace of the data. The US National Institute of Standards and Technology (NIST) defines "media sanitisation" as a broad term for actions taken to render data written on media unrecoverable by ordinary and extraordinary means.

[3] Will this media be given or sold to a third party? Is it to be discarded or to be reused internally? If the medium is reused as is, the controller must ensure that the medium will be used in a security context at least equivalent to the context in which the medium was used previously (e.g.: information access policy comparable to that which prevailed in the initial environment of the medium, or even stricter).

[4] Such as PCs, servers, printers containing hard disks, removable media (USB key, DVD, external hard drive, etc.) or mobile devices (laptops, tablets, mobile phones, etc.).

[5] It should be noted that the GDPR provides for a violation of the provisions relating to the obligations of the controller/processor, including in particular Art.32 (security), administrative fines of up to EUR 10

In this respect, it should be noted that the controller is required, under penalty of sanctions[6], to comply with Article 5.1.e of the GDPR, which provides that "personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed". When this period is exceeded, the controller must anonymise these data or permanently destroy them [7](see exceptions in the same article).

04. Note that, if the protection of data leaving their initial environment is a growing concern for organisations of all types, it is partly because their protection within them is increasing. Thus, a stricter data access control policy reduces the probability that an unauthorised person can directly access these data. As a result, this person will be tempted to turn to other information access channels, requiring less effort such as data recovery on media that leave the organisation's controlled environment or are placed in a lower privacy/security level environment.

05. With regard to the laws in force, we will retain more specifically, in the context of this document, the European General Data Protection Regulation (GDPR[8]) and in particular its Article 32 (see Appendix B) on the security of processing and Articles 33 and 34 (see Appendix B) relating to personal data breaches. Also note Article 5.1.f enshrining the obligation to protect personal data against, in particular, their unauthorised processing and loss, using appropriate technical or organisational measures.

06. It should be noted that Article 4.12 of the GDPR defines personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

07. The controllers and processors[9], required to comply with their legal obligations must, therefore, have to take the appropriate technical and organisational measures

---

million or, in the case of a company, up to 2% of the total annual worldwide turnover of the previous financial year, whichever is the higher (Art.83.4.a of the GDPR).

The highest administrative fines to date (11/2020) imposed for security under the GDPR already amount to millions of euros. Thus, the British data protection authority (ICO), in agreement with the other European data protection authorities (in application of the cooperation mechanism provided for in the GDPR, known as the one-stop shop) has imposed fines of nearly 21 million euros on the Marriott hotel group and nearly 22 million euros on British Airways for security breaches (violation of Art.5.1.f and 32 - see Appendix B).

[6] Refer, for example, to the penalty of EUR 160,000 imposed by the Danish authority on a taxi company that kept the telephone details of a reservation for more than two years and the penalty (EUR 200,000) imposed by the same authority on a furniture store for failing to erase customer data when renewing computer equipment.

[7] A temporary organisation needs to collect the data of a certain number of members to be able to file a petition, who must be authenticated as actual persons. After authentication, this organisation, which has no other purpose, must not keep any personal data and must therefore delete all of them as well as the petitions containing them since only the number of validated signatories is important (deletion following the achievement of the purpose).

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/CE. The GDPR has been in effect since 25 May 2018.

[9] Article 4.8 of the GDPR defines a "processor" as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

in order to guarantee the confidentiality of the personal data[10] present on the information media that they wish to sanitise.

08. The Data Protection Authority (DPA), responsible for ensuring compliance with the fundamental principles of personal data protection, of which the principles of security and confidentiality[11] are essential elements, aims through this document to assist controllers and processors in complying with these principles.

09. To do this, this document presents various "sanitisation" techniques which either make access to data impossible on a preserved medium (erasure without the option of recompilation and encryption), or lead to the destruction of the medium (without the option of reconstruction).

10. The controller will choose from this range of techniques, taking into account in particular the type of medium, its subsequent allocation and the level of confidentiality of the data.

Limitations

11. Only techniques leading to "sanitisation" of the entire medium or to its destruction are discussed in this document. The specific erasure of files, directories or partitions is therefore not processed.

12. The following is not covered in this document:

- Cases where access to media/data for erasure or destruction is not possible, such as cloud storage or hardware from a PCaaS[12] contract. It is up to the controller, before choosing their cloud provider or other remote storage provider, to examine what service they offer to delete data securely;

- The erasure of data contained in the vehicles (navigation data, data from the synchronisation of contacts with the mobile phone, etc.) during a repair at the garage or at the end of a leasing contract, for example;

- The erasure of data on mobile devices via specific software or centralised management (e.g.: Active Directory). Apple is putting online a procedure for the

[10] Article 4.1 of the GDPR defines "personal data" as any information relating to an identified or identifiable natural person (hereinafter 'data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[11] The controller and the processor must ensure the security and confidentiality of the information that they process. In particular, they must ensure that only authorised persons have access to this information.

[12] "Personal Computer as a Service", also known as "Device as a Service": a device lifecycle management model in which an organisation pays a monthly subscription to a vendor, to lease equipment and associated management services.

E.g.: Description of Dell's PCaaS offer https://www.delltechnologies.com/en-us/services/pc-as-a-service.htm and their optional PCaaS Data Sanitization service https://www.dell.com/learn/us/en/uscorp1/legal~service-descriptions~en/documents~pcaas-data-sanitization-sd-en.pdf

erasure of personal data for the iPhone and iPad[13], and Google for Android devices[14];

- Restoring factory settings. The controller will, however, ensure that the non-volatile memory no longer contains personal data[15];

- The use of images, created by an operating system imaging and deployment software[16], to re-install devices.

Target audience

13. This document is intended for controllers and processors[17] (whether in the public or private sector), their information security advisers and data protection officers (DPOs) or any other person or organisation that needs or wishes to make access to personal data impossible.

Objectives

14. This document aims to:

- Help the target audience to formalise and integrate the different steps to make an informed choice of an appropriate "sanitisation" technique;

- Provide information on the different methods and techniques available, their levels of confidentiality and the results that can be expected depending on the type of medium concerned.

- Help the target audience to comply with certain GDPR requirements, including those relating to accountability (principle of accountability defined in Article 5.2 of the GDPR) and those intended to prevent unauthorised disclosure of data.

---

[13] https://support.apple.com/en-gb/HT201351

[14] https://support.google.com/android/answer/6088915?hl=en

[15] This function returns the device to the condition it was in when it left the factory (generally equivalent to the condition it was in when the device was purchased). It mainly concerns the non-volatile memory (does not erase in the absence of power) integrated on the cards and peripherals. For example, remote management integrated into a motherboard can contain IP addresses, user names, passwords or certificates. Therefore, for erasure it may be necessary to interact with multiple interfaces to completely reset the device status. This can include the BIOS/UEFI[38] interface as well as the remote management interface.

[16] Image deployment software captures an image of the operating system installed on a device and deploys it to similar devices (PCs, servers, mobiles, etc.).

[17] Pursuant to Article 32 of the GDPR, both the controller and the processor implement the appropriate technical and organisational measures to ensure the constant confidentiality of the processing systems and services. This document may be of interest to a processor wishing to offer its services to a controller.

2. Preliminary principles and concepts

15. The 'sanitisation' or destruction of a data[18] medium will be:

- Authorised (according to an internal procedure and/or applicable law);
- Appropriate (irreversible, in accordance with the risk analysis and the resulting security/confidentiality requirements);
- Supervised by the controller (in the event of subcontracting, see section 3.1.3. for additional measures to be taken);
- Documented (proof of destruction, see 6th part);
- And executed at the right time (consider legal deadlines, problems related to standby storage).

2.1. Information classification and inventory

16. In order to be able to determine which method should be used to best mitigate the risks of unauthorised disclosure of data, the controller must know a number of elements.

2.1.1. The type and categories of data on the medium

17. At the very least, the controller must know whether or not personal data are present and if so, it may also usefully want to:

- Identify, in these data, which data is "sensitive" (belonging to a particular category[19]) or relates to criminal convictions or offences (Article 10 of the GDPR);
- Distinguish between data that are encrypted[20] , and/or pseudonymised[21];
- Classify the data according to the risk that the unauthorised disclosure of all or part of the personal data contained on the medium would represent for the data subject. It is preferable when estimating the risk, to consider an overall disclosure of all the data contained on a medium or in a device, which often corresponds to

[18] Note that we use the terms "information" or "data" indiscriminately, not knowing whether the medium contains the former or the latter or both. Data refers to raw data, used to obtain information after analysis. The information is interpreted and gives meaning to the data. Thus the data '21122021' becomes information if we know that it is a date (21 December 2021).

[19] Article 9.1 of the GDPR lists these special categories of personal data. These are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

[20] Encrypted data is data that has been made unintelligible to people without the correct decryption key.

[21] Article 4.5 of the GDPR defines pseudonymisation as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

the reality on the ground. For example, when a database server is hacked, it is usually all the databases that are accessed simultaneously.

18. In fact, the procedure put in place by the controller, in order to determine the appropriate "sanitisation" method, may be based in whole or in part on the information provided in par. 17.

19. We would like to reiterate here that anonymised data[22] no longer meet the definition of personal data insofar as they can no longer be linked to an identified or identifiable natural person.

20. The nature and categories of data must be associated, according to a policy validated by the controller, with a technique making it possible to achieve the required level of confidentiality (clear, purge or destroy – see section 3.1.2.).

21. It is therefore necessary to have an inventory and a classification of information[23].

2.1.2. The nature and characteristics of the medium

22. There are many types (hard disks, SSDs, magnetic tapes, floppy disks, iPhones, SD cards, microfilms, etc.) and classes (optical, electronic, magnetic, write once, paper, etc.) of media.

23. It is logical that the highly different technical and physical characteristics of these information media have an effect on the choice of the method of 'sanitisation'. Moreover, not all techniques are available for all types and classes of media. Consider, for example, degaussing for a paper medium or overwriting for a write once medium.

24. The classification of the data and the nature of the medium are the main criteria used to determine the processing of the media and the method that will be used. To make this choice, the classification will serve as the first filter, insofar as it provides information on the level of sensitivity/confidentiality of the data and on the risk for data subjects in the event of unauthorised disclosure. Considerations based on the type and class of the medium will be used in a second step.

25. Other additional factors can be taken into account such as cost, environmental impact, subsequent allocation [3] or duration of the process.

---

[22] Extract from recital 26 of the GDPR : [...] The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. [...]

[23] Inventory of assets and classification of information is an integral part of an information management system. Thus, measure 8.2.1 (Asset management) of ISO 27002 classifies information in terms of value, sensitivity to disclosure or modification, legal requirements or their critical nature. NB: measure 6.5.2.1 of ISO 27701 (additional implementation guidance for 8.2.1 of ISO 27002), although dedicated to personal data, does not provide much information on a specific classification.

2.2. Processing steps

26. Concisely, the main steps of the 'sanitisation' and destruction operations could be as follows:

A. Policy (security and confidentiality)

27. The first step is to draw up, in a document, a policy line validated by the management and covering the entire data sanitization issue and including all the existing data media in the organisation. This document must in particular describe the context, the goals to be achieved, the 'sanitisation' or destruction authorisation procedure (including for back-ups) and the various stages of processing. It will also describe in detail the responsibilities of stakeholders (and the management) for the execution as well as the control of the different stages of processing (chain of responsibility). It is important that each step, without exception, be placed under the responsibility of a duly appointed person (see example in par.240).

28. The responsibility of the stakeholders extends beyond the actual sanitisation/destruction procedure. It may be useful to determine who would be responsible for damage to reputation, and possible penalties if, at a later stage, it turns out that certain data media have not been processed according to the validated procedure.

29. The authors of the document will ensure complete top-down support of the hierarchy. In binding areas, such as security and confidentiality, the support of management is indispensable, otherwise these policies will remain on paper, the content of which is not enforced. Care should be taken to ensure that the responsibility for 'sanitisation' of media is assigned to a member of the organisation with an appropriate level of authority.

30. The implementer(s) will also ensure that the policy is known to all stakeholders who have a role[24] in it, that it is properly executed in practice and updated if necessary[25]. It is important that this execution of the instructions and their results are also checked.

31. A report[26] from Blancco shows that the discrepancies between the creation, communication and execution of the media sanitisation policy put sensitive data at risk. The study identifies the following risks:

- Not taking direct responsibility for the erasure of IT assets;

---

[24] https://www.realwire.com/releases/More-than-half-of-enterprises-fail-to-communicate-data-sanitization-policies: Although 96% of the heads of organisations consulted have a data disinfection policy, 31% have yet to communicate it to the whole company. 20% of respondents also do not think their organisation's policies are complete. Overall, 56% do not have a data cleaning policy in place that is regularly communicated effectively across the organisation, which increases the risk of potential data breaches.

[25] Like all other policies, this must be part of a cycle that includes an update stage. There are many reasons why an update would be necessary. Consider a change in the context of security/confidentiality within the organisation or a technological upgrade (for example, coercive force of a degausser to be adapted according to the evolution of the media, see par. 120).

[26] Data Sanitization: Policy vs. Reality, produced in partnership with Coleman Parkes (06/02/2020) https://www.blancco.com/resources/rs-data-sanitization-policy-vs-reality/

- Leaving the hardware abandoned in the storage areas without having secured it;
- Off-site erasure without complete visibility of the chain of control;
- Unclear designation of owners of data cleaning policies.

B. Inventory

32. Take a full inventory of all the equipment you have marked as needing 'sanitisation' or destruction. Determine the type(s) of media involved. If this has not already been done, take an inventory of the data contained on the information media to be processed in order to sort them according to a relevant classification, namely;

- depending on the type of personal data found therein,
- and whether their disclosure would represent a high risk for the rights and freedoms of the data subjects (as is a priori the case for data of special categories listed in Article 9 of the GDPR).

33. If the controller does not know the content of the information medium (damaged medium or obsolete technology, lack of time or personnel, etc.), it will treat this medium as if it contained personal data, the disclosure of which would represent a high risk for the rights and freedoms of the data subjects.

34. We would also reiterate that the GDPR requires controllers to keep a record of processing activities (for personal data) which includes in particular a description of the categories of personal data processed (Article 30.1.c).

35. If the controller wishes to make this document a compliance tool that is broader than a simple record, it can usefully include information such as the nature of the medium used for the processing, the destruction or sanitisation technique and its trigger (replacement or obsolescence of the hardware, exit of a co-worker, purpose fulfilled, legal deadlines reached, etc.).

C. Risk analysis

36. This mainly involves determining the risk incurred if an unauthorised person accesses personal data contained in the information medium, which constitutes a data breach and an infringement of Articles 5.1.f and 32.2. of the GDPR (see Appendix B). Also take into consideration any possible security loopholes associated with each technique[27].

[27] Search the Internet for vulnerabilities associated with the selected technique or tool. For example, you can refer to the CVE (Common Vulnerabilities and Exposures) list, which includes the largest number of publicly known cybersecurity vulnerabilities. Other sources of interest: Exploit Database, U.S. National Vulnerability Database (NVD) of the NIST, packet storm.

37. It is important to note that the concern of the GDPR (and the DPA) is about the impact of the disclosure

- of "personal" data (and not of all the data of the organisation),
- of data concerning the data subject (i.e. the person to whom the data relates) and not concerning the organisation.

38. While the risk analysis is an essential step, the controller, assisted by its possible Data Protection Officer, could also usefully carry out a "data protection impact assessment" (DPIA, Article 35 of the GDPR[28]), whether or not it is mandatory.

- The DPIA will help the controller to ask the right questions;
- It will contain information useful for filling in the processing record (Article 30 of the GDPR);
- It will help to fulfil the obligation of data protection by design (Article 25 of the GDPR). Since the DPIA serves, also before processing, to identify the measures to be taken to deal with the risks to the rights and freedoms of the data subjects, it can provide valuable assistance in this regard.

39. If the DPIA were to indicate that the processing still presented a high risk, after the controller has taken measures to mitigate the identified risks, the controller must consult the Data Protection Authority prior to the implementation of processing (Article 36 of the GDPR).

D. Security measures

40. The next step is to put in place the technical and organisational measures to reduce any identified risks to an acceptable level (for the organisation and for the data subjects).

41. This step also includes identifying actions that could be taken, quickly and efficiently, to respond to a possible data breach. If personal data were to be compromised during media 'sanitisation' or even after you leave your organisation, you could still be held liable for the breach (you remain the controller until the end of the data lifecycle).

E. Assessment

42. It is then necessary to assess to what extent the actions undertaken have achieved the set objective (preventing loss of confidentiality). If necessary, choose another technique.

---

[28] See also the own-initiative recommendation on data protection impact assessment and prior consultation (CO-AR-2018-001) of the former Commission for the protection of privacy. (https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2018.pdf)

F. Documentation

43. The different stages must be documented in detail. The principle of accountability of the GDPR (defined in Article 5.2) in fact implies that the controller is able to demonstrate its compliance with the data protection rules. In particular, the following will be documented: the justification[29] of the method chosen, the description of the measures taken (steps of the method, verification included) and the proof of their proper execution (for example, by issuing a document containing all the information related to 'sanitisation' or destruction of the medium and, after a verification step, the result, failure or success).

44. In order to strengthen its transparency vis-à-vis the data subjects, we recommend that the controller communicate certain information, in addition to the information that must be communicated under Articles 13, 14 and 15 of the GDPR. Thus, in addition to the data retention period (Articles 13.2.a, 14.2.a and 15.1.d), it may, without effort, using the documentation already at its disposal, inform them more concretely of what will happen to their data once this period has elapsed.

45. Likewise, we will recommend that the controller adopt the same transparent attitude, in the context of their communication with the data subject relating to Article 17 of the GDPR (right to erasure).

G. Example

46. Here is a more concrete example illustrating the main steps of a data cleansing and/or media destruction project:

1. You plan to replace some computers in your organisation and sell them to a company that will refurbish them before reselling them.

2. You determined during the inventory phase that the media contained in the PCs were ATA hard disks with a capacity of 500GB and contained HR personnel files and that these files included special categories of personal data (sensitive data such as trade union membership or data related to absences due to illness).

3. According to your security/confidentiality policy, personal data must remain under your control at all times, so no data can leave the physical and/or logical perimeter of your company.

4. In the risk analysis, you compare the different methods meeting this objective (erasure, storage, destruction).

5. In view of the nature of the data, the time needed to erase the hard disks, the possibility that some data may remain accessible, the low resale value of the PCs, the risk to the organisation (e.g. reputation, financial, legal proceedings, etc.) and

[29] The justification may be based on a balancing of the interests of the controller with the rights and interests of the data subject and/or an assessment of the risk inherent in the processing, considering the state of knowledge and the costs of implementation in relation to the risks and the nature of the personal data to be protected.

the risk to the rights and freedoms of the data subjects (e.g. identity theft, scamming, phishing, blackmail, discrimination, etc.), you consider that the risk is not worth taking.

6. Consequently, in order to reduce the risk to an acceptable level, you opt for the physical destruction of the media and take the following measures:

A. Whether the destruction is done within the organisation or by an external partner, you appoint the managers involved in the project: the operational manager will be a member of the IT department while the overall supervision will be provided by the DPO who will give a positive (or negative) opinion at the end of the procedure, knowing that a final decision, whether it concerns the choice of the sanitisation method, the level of confidentiality achieved, or the agreement to release/transfer the media always rests with the controller (the management of your organisation). This or these decisions could usefully be referenced in the record of processing activities;

B. You decide that the destruction must be carried out within the confines of the organisation, in the presence of the project manager;

C. You choose[30] a specialised external partner, offering guarantees of quality and respect for confidentiality, who can, using mobile equipment, implement the technique you have selected. You check with the service provider that the technical characteristics of the equipment used (e.g. maximum size of destruction residues) meet the requirements of your security/confidentiality policy.

7. You ensure that the destruction took place according to the established procedure and that the data are no longer usable. You collect and keep the evidence of the actual destruction of the media (for the whole or specific to each medium) as well as all the information useful for demonstrating your compliance with legal obligations.

2.3. In the best of all worlds

47. In a perfect world, you will have already thought about the 'secure sanitisation' of your media, even before their acquisition and asked the vendor of these media on this subject. For organisations having to draw up specifications, it may include specifications relating to the erasure commands integrated into the equipment (if applicable - see Articles 3.2.1.2. And 3.2.4.1.) and require the assistance of the vendor and the provision of certain related information (e.g.: execution time, description of supported commands and their options or excluded areas). This should facilitate the informed choice of a storage medium or of a device comprising a storage medium, on the basis of the secure erasure options offered by the product.

[30] Let us reiterate here that the controller has a responsibility and obligations in the choice of the processor (Article 28 of the GDPR). The reputation of the vendor is not sufficient assurance. The written contract, binding between the controller and the processor, will help ensure that an appropriate level of security is in place and will mention as precisely as possible the method chosen, its characteristics and the means to be implemented.

48. Likewise, collecting all the technical information needed at the time of acquisition will not only facilitate the 'inventory' stage of the processing but also the 'risk analysis' stage where you will have to compare the different erasure techniques available depending on the characteristics of the medium.

49. For example, knowing the coercivity[31] of a magnetic medium, we can include or exclude degaussing (see section 3.2.3.) from the list of available techniques. Alternatively, having noted that two different types of disks (hard/magnetic and SSD/electronic) are present in the organisation's computers, the operational manager will know that they must be distinguished when choosing the 'cleaning' method. \\ It should be noted that both types of disks can be present simultaneously in the devices (SSD disks are much faster but more expensive, and are often used to boot the computer and coupled with a slower magnetic hard disk, but which takes care of storing most of the data).

3. The different methods and techniques

3.1. Introduction

3.1.1. Important details

50. From the outset, let us make an important point, by specifying that simply deleting (by pressing the delete key on your keyboard, for example) files or directories via the interface of your device erases only pointers to these files and not the data itself. By erasing the pointers, the device makes the area where the files were located available again for writing other data. As an analogy, it is like for deleting the chapter of a book, you delete any reference to the said chapter in the table of contents. By going through the book, you can therefore find the content of the chapter.

51. This is why this action, which does not result in any actual erasure, is not commented on in this document.

52. Note also that formatting does not erase data either, whether it is quick or full[32].

3.1.2. Three levels of confidentiality

53. In the specialised literature, the different techniques are often classified according to the level of confidentiality (security) desired or, in other words, the probability of recovery of the initial data. There are three levels of confidentiality associated with three classes of techniques: clear, purge and destroy.

- Clear level techniques aim to prevent data recovery carried out using software. They offer moderate confidentiality (some data can be recovered if the necessary time, knowledge and competence are available). These are purely logical[33] techniques.

[31] In this context, coercivity refers, in non-academic terms, to the force that is required for a magnetic field to modify data stored on a magnetic medium. The higher it is, the more difficult it will be to modify ('erase') the data using a degaussing technique.

[32] The difference between the two is mainly due to the fact that a full format will check all the bad sectors, which explains the long duration of the operation compared to a quick format.

[33] The term 'logical' refers to a technique in which the mechanisms are implemented using software.

Examples: (partial) overwriting using standard commands (read and write) and resetting the device or media ('factory' reset - often recommended for mobile devices and routers/switches).

■ Purge level techniques are designed to prevent data recovery performed using advanced laboratory techniques. They offer a higher level of confidentiality and are appropriate when the medium is intended to be reused in a security/confidentiality context different from the initial context. These are logical and physical techniques.

Examples: overwriting using dedicated commands, degaussing and cryptographic erasure (see section 3.2.4.).

■ Destroy techniques offer the highest level of confidentiality/security. Data recovery is indeed impossible, even using advanced laboratory techniques. They are based on physical destruction and are therefore incompatible with reuse of the medium. Note that a technique rendering the medium unusable will not reach the destroy level if some data nevertheless remains recoverable.

Examples : incineration, shredding and crushing.

54. The different techniques presented in this document all fall into one of these three classes. The reader will find in Appendix A, a table showing the most common types of information media[34], associated with the different techniques which can be applied to them according to the level of confidentiality/security required (clear, purge and destroy).

55. The level of confidentiality to be achieved, followed by the choice of a technique allowing this level to be reached, depending on the type of medium, is based on a preliminary risk analysis.

Techniques available depending on the desired level of confidentiality		
Clear	Purge	Destroy
• Overwrite (standard commands) • Reset (restore factory settings see par. 12)	• Overwrite (dedicated/integrated commands) • Degaussing • Cryptographic erasure	• Incineration • Shredding • Crushing • Disintegration • Degaussing

56. We will split the methods used into two groups, depending on whether or not they lead to physical destruction of the information medium.

[34] For a more complete list of media, the reader may refer to Appendix A of the "Guidelines for Media Sanitization" of the "NIST Special Publication 800-88".
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

3.1.3. Processing not supervised by the controller

57. When the destruction or 'sanitisation' of the medium is subcontracted or partially subcontracted and is therefore not carried out under the end-to-end control of the controller, the latter must obtain assurances as to the proper conduct of the various stages of processing. To achieve this, we will recommend the following measures:

- The use of eye witnesses (validated by the service provider and/or the controller);
- The transport of the media in secure and locked vehicles. Although the protection provided by the security seals is not absolute[35] (it could possibly be overcome by trained and equipped attackers), vehicles may be usefully provided with them;
- Taking photographs or using other documentation techniques at each stage of processing;
- The establishment of a continuous, non-stop process involving temporary storage;
- Procedures for monitoring and selecting personnel involved in the processing;
- The issuance of a certificate of destruction by the processor (see 6th part).

58. It is advisable to include these measures in the contract between the controller and the processor and to describe therein, where applicable, the elements constituting the proof of destruction (in particular the method used and the result obtained). In this regard, the reader may refer to the clauses in a document[36] of the government services of New Brunswick (Canada).

3.2. The data medium is retained

59. As a preamble to the various techniques presented in this chapter, it is important to note that apart from a destruction method that leaves no part of the medium intact (regardless of the nature of the medium – paper, magnetic or other), it is difficult to guarantee that no more data will be usable on the entire surface of the medium, including by specialised laboratories.

60. If the risk of data remaining on the medium or that it can be reconstructed is not acceptable to the controller (taking into account the risk to data subjects), a method resulting in the destruction of the medium will be preferred (see chapter 3.3.).

3.2.1. Erasure - overwriting

61. The "erasure" (also called overwriting or rewriting) consists of writing, in the same place as that where the data already present on an information medium are found, one

[35] https://web.archive.org/web/20081007232536/http://www.ne.anl.gov/capabilities/vat/defeat.html

[36] Secure destruction of documents: Directives - Appendix C, p.15 - Standard contractual clauses on the secure destruction of documents

or more series of information elements – determined, random or both (depending on the protocol chosen) – in order to reduce the possibility of being able to recover the data thus overwritten (or rewritten).

62. It would therefore be more appropriate to speak of an "overwrite" method than of an erasure[37] method because the initial information or parts of this information are still potentially present on the medium, depending on the efficiency of this overwriting.

63. Overwriting is obviously not applicable to media which are natively 'write once' or which no longer support writing following damage (breakdown, partial destruction, wear).

64. This method can lead to two levels of confidentiality, namely 'clear' and 'purge'. The level achieved will depend on the combination of the type of medium containing the data, the software used (linked to the hardware or independent) and the associated commands (standard or dedicated). The choice and the correct use of the software and the commands will themselves depend on the level of computer knowledge of the person in charge of the procedure.

65. The discs, whether magnetic (see point 3.2.1.1.a) or electronic (see point 3.2.1.1.b) have different areas. Some of these areas are a priori inaccessible to software independent of the hardware, to the operating system or to the BIOS/UEFI[38], which makes it impossible to clean the entire storage areas of the medium.

66. \\ Among these areas that are apparently inaccessible, we find:

- Bad/unmapped/corrupted sectors
- Over-provisioned space
- Trimmed cells
- Device Configuration Overlay (DCO)
- Host Protected Area (HPA)
- Garbage Collection (GC)

[37] Note that the term "erasure" is regularly used in the literature on the subject or in the description of software used for the secure deletion of digital information.

[38] BIOS (Basic Input Output System) is firmware stored on a memory chip and used to perform hardware initialisation during the boot process and to provide runtime services for operating systems and programs. It is non-volatile, which means that its settings are saved and recoverable even after the device is turned off. As for UEFI, it is essentially an improved version of the BIOS.

3.2.1.1. Clear level - Third party software

A. Magnetic hard drives

67. \\ The clear level can be achieved for hard disks (internal and external) and floppy disks using third-party software[39], independent of the hardware, such as BitRaser, Blancco Drive Erasure, PartedMagic, Active@KillDisk or the open source project DBAN. These software often offer a wide range of different protocols (up to several dozen) from which the uninformed user will find it difficult to choose.

68. What differentiates these different protocols is, on the one hand, the number of overwrites, i.e. the number of successive overwrite passes that the surface of the disk will undergo and, on the other hand, the last stage of the protocol, i.e. the control of the effect of the overwrite passes.

69. For example, the DoD 5220.22-M protocol, very often used and present in all flagship software on the market, recommends writing on all addressable spaces of the medium, a binary character (in this case 0), then its complement (1) and finally a random binary character (0/1). The verification of the result is the last step[40] of the protocol.

70. The version of this "erase" protocol, still perceived as a true standard and which is delivered in most third-party software, corresponds to an obsolete version of a standard of the United States Department of Defense (DoD) [41]. The triple overwriting of the disk required by this old version of the protocol is more than sufficient to prevent the recovery of data by commercially available software (clear level). While the effectiveness of the erasure protocols seems logically and a priori linked to the number of overwrite passes that all the areas of the disk will have undergone, this logic is exceeded.

71. In fact, in recent years, a consensus has emerged (NIST, HMG British Standard, BSI-GS, CMRR[42]) to assert that, following the technological evolution of media (in particular linked to the increase in their density and therefore their capacity), the number of overwrite passes can be reduced to 1, without, however, increasing the possibility of recovering the data on the disk from logical solutions. However, a verification pass must be performed.

72. If a write pass and a verification pass are sufficient (except for old hardware dating from before 2000 or of unknown age), we can then conclude that a protocol offering

---

[39] Search your usual search engine (the DPA currently uses startpage.com) for the terms "data erasing" or "data sanitization" to find information on paid software or freeware offering this type of function.

[40] In the literature, it is mostly referred to as a pass. Thus, DoD 5220.22-M is a 4-pass protocol, 3 dedicated to writing (erase/overwrite) and one to verification.

[41] To be precise, the current version of this protocol no longer specifies these steps and thus these software refer to an older version of the protocol. For more information: https://www.blancco.com/blog-dod-5220-22-m-wiping-standard-method/

[42] Extract from the "Tutorial on Disk Drive Data Sanitization" (p.8) of the Center for Magnetic Resonance Research (CMRR): "The U.S. National Security Agency published an Information Assurance Approval of single pass overwrite, after technical testing at CMRR showed that multiple on-track overwrite passes gave no additional erasure."

3 overwrite passes and a final verification, or a verification after each write pass (such as the older version of the popular DoD 5220.22-M), is also sufficient.

73. \\ On the other hand, although they are not strictly discouraged, the protocols proposing a number of passes higher than a write pass and a verification pass can be qualified, in the current state of our knowledge and techniques used, as not being useful[43].

74. When it comes to choosing software, give preference to software that has been analysed by an independent laboratory and/or that meets the requirements of specialised government agencies.

75. \\ Here are some examples of links to players evaluating products or services in the field of data destruction:

- ADISA Research Centre (UK),
- BSI - Bundesamt für Sicherheit in der Informationstechnik (DE),
- National Association for Information Destruction - NAID (USA),
- ANSSI - Agence nationale de la sécurité des systèmes d'information (FR),
- NCSC - National Cyber Security Centre (UK),
- NBV - Nationaal Bureau voor Verbindingsbeveiliging (NL),
- NCI - NATO Communications and Information Agency (USA),
- NSA | CSS - National Security Agency Central Security Service (USA).

B. Flash memory media

76. Unlike discs and floppy disks (see previous point 3.2.1.1.a), which are magnetic media, flash memory is electronic media. This non-volatile memory (it is not erased in the absence of power, unlike the RAM for example) can be erased and reprogrammed electrically.

77. Thanks in particular to falling prices, excellent performance and the absence of mechanical breakdowns, flash memory has emerged over time as an information storage technology that is increasingly present in electronic devices and information media. It can therefore be found in mobile phones, computers, digital cameras, USB keys, memory cards, SSDs (see below), calculators, medical devices, hi-tech toys, etc.

---

[43] The Gutmann (1996) protocol, reminiscent of a bygone past where the techniques used for writing to hard disks theoretically allowed specialised laboratories to find overwritten data, corresponds to no less than 35 overwrite passes plus a verification pass. Current hard disks have made this protocol, which is also very resource-intensive, completely obsolete*. However, it still appears in the list of protocols offered by the main software on the market.

*For specialists: this protocol has become obsolete at the same time as the appearance of high-density disks (large capacity) and the technology of hard disks has moved from MFM/RLL coding technique to PRML techniques in the late 90s.

78. \\ More specifically, as regards information media, we can distinguish two large families of devices[44] containing flash memory:

- memory cards of which there are many types (e.g.: Secure Digital SD, SDHC, SDXC, micro and mini SD, xD card, CompactFlash or MemoryStick). They are intended for small equipment such as digital cameras or mobile phones;

- SSDs or solid-state drives, which can be referred to as static disks, semiconductor disks or simply electronic disks. They are available in a large number of formats and interfaces (PCIe, SATA, USB, etc.). By extension of language, any type of medium that does not contain 'moving' parts (unlike rotating magnetic hard disks, for example) is sometimes called SSD (RAM, ROM, Smart Cards, Flash).

  NB: For several years now, SSDs have all been based on flash memory (hence the confusion between the two terms) but this has not always been the case (RAM) and this may change again in the future.

ATA or SCSI Solid-State Drives (SSD)

79. We have seen that certain areas of 'traditional' hard disks (see point 3.2.1.1.a) are inaccessible to third-party software. It should be noted that for flash memory, a technological peculiarity (see par. 81 and 82) linked to this type of medium accentuates this access problem.

80. This is why, even if the use of independent software for the 'electronic' disks could make it possible to achieve the 'clear' level of confidentiality via an overwrite pass (especially via several), the use of these third-party software alone will be considered insufficient to achieve the desired objective.

81. For information, the technological peculiarity mentioned in par. 79 is due to the fact that any writing on this type of medium causes wear. Its components are therefore only guaranteed by the manufacturer for a finite number of program / erase cycles or p/e cycles. \\ In order to extend the life of flash memories and avoid any premature wear of the cells of certain blocks[45] compared to others[46], manufacturers have developed strategies such as wear-levelling[47], dedicated file systems or the

---

[44] https://fr.wikipedia.org/wiki/M%C3%A9moire_flash#Grandes_familles

[45] Flash memories are divided into blocks which are made up of pages, themselves made up of memory cells. Writing and reading are done at the page level. However, before being able to overwrite in the same place, it is necessary to reset (erase) the memory cells, which is only done by whole block (generally made up of several hundred pages). You will therefore have to copy the entire block to another location, delete the original block, then write the contents of the old block with the new pages.

[46] In this case, avoid premature wear of the blocks which are often erased compared to those which store data which are not or only slightly modified.

[47] The principle is to copy data that are never or rarely modified on already worn cells, in order to distribute more uniformly the number of erasures/writes per cell (and therefore the wear).

exclusive allocation of storage spaces to the SSD controller (overprovisioning)[48].

82. The use of these techniques therefore results in the copying of the same data in multiple locations, including areas to which independent software do not have access (examples: bad blocks or wear-levelling blocks).

USB keys

83. Known by many other names[49] and whose flash memory is of lower quality than that of SSDs, they have, just like memory cards[50] intended for small equipment (e.g.: digital cameras and mobiles phones), the same limitations at the clear level as SSD disks.

C. Important points

84. Remember that in the context of the overwriting of media by third party software (clear level):

- The level of confidentiality reached does not exceed the clear level;
- These software does not have, a priori, access to all the writing areas of the medium;
- For flash memory media, creating copies of data blocks increases the possibilities for recovery after erasure.

85. This is why, depending on the risk (mainly incurred by the data subjects), it may be necessary to combine the erasure with another technique such as encryption (see par. 126) or physical destruction (see chapter 3.2).

3.2.1.2. Purge level - Integrated commands

86. Storage media have different interfaces depending on the model (ATA, SCSI, NVMe). These interfaces, used to communicate between host systems and storage devices, have different types of commands for cleaning the medium.

[48] The use of these techniques and the absence of mechanical parts nevertheless allow current SSDs to obtain guarantees equivalent to hard drives.

[49] Thumb drive, pen drive, gig stick, flash stick, jump drive, disk key, disk on key, flash-drive, memory stick, USB stick, USB memory or USB flash drive.

[50] List of card types: https://en.wikipedia.org/wiki/Comparison_of_memory_cards#Common_information

A. IDE/ATA magnetic hard drives

87. Most modern IDE/ATA[51] (PATA[52][53], eSATA, etc. included) hard disks[53] are delivered with "Secure Erase" commands (generalised since 2001 for disks over 15GB). Secure Erase is the name given to a set of commands stored in and available from the firmware[54] on the disk.

88. These built-in commands[55] erase (overwrite) all the data on a disk (including sectors marked bad or inaccessible) and achieve a purge level of confidentiality.

89. \\ Third-party software differs from those discussed in section 3.2.1.1.: HDDerase. Developed by the CMRR[42], this utility indeed incorporates the ATA Secure Erase command and can therefore reach certain storage areas inaccessible to traditional third-party software.

90. \\ Also note under Linux, the command line program 'hdparm' (NB: the programs GParted and Parted Magic both include hdparm).

ATA commands - details

91. So far we have discussed the Secure Erase "command". It is the term most frequently used in the literature but also one that is regularly used in an imprecise manner.

92. The correct name of the command is 'Security Erase Unit' (one of the ATA standard commands) and is available in two modes, the standard 'Secure Erase' or 'Normal Erase' mode and the 'Enhanced Secure Erase' or 'Enhanced Erase' mode.

93. The 'enhanced' mode, which targets sectors that are no longer in use due to reallocation, is not supported by all ATA media.

94. Although their names are similar, there are differences between these two modes. When the normal erase mode is selected, the 'Security Erase Unit' command writes zeros (in binary) in all areas where data has been written by the user.

95. When the enhanced erase mode is selected, the 'Security Erase Unit' command writes data according to predefined patterns and also overwrites the disk sectors that are no longer in use or marked as inaccessible to the user. The use of this mode is

---

[51] To be distinguished from ATA SSD (solid-state drives).

[52] IDE is a standard interface, also known by the acronym ATA, used to connect storage devices (hard disks, CD/DVD drives, etc.) to the motherboard of a PC. Although the name IDE is often used interchangeably with ATA, IDE actually refers only to the electrical specifications of the signals on the 40/80 pin drive cable. ATA is the correct name for the entire specification.

[53] When SATA (Serial AT Attachment), the new ATA standard for data transmission emerged, the old, well-known forms of ATA were retroactively renamed PATA (Parallel ATA).

[54] Firmware is software embedded in hardware, which provides the instructions necessary for the operation of the same hardware.

[55] These commands (firmware commands) cannot be run on a hard disk like, for example, commands in Windows are run from command prompt. To run the Secure Erase commands, you will need to use a program which gives direct access (I/O) to the ATA interface of the hard disk and which allows sending ATA commands to this same drive. Even so, the user will often not run the command manually.

optional and is not supported by all manufacturers. However, if it is available, it will be preferred to the standard mode.

96. From the point of view of the ATA specification, these are two different commands and it is sometimes difficult to know which one is used by the manufacturers. Likewise, if a medium says it implements both uses, it is possible that it combines both with a single action/version.

97. More recently, another ATA command, 'Sanitize Device', has emerged. Also optional, it is not used on all the media. Just like the equivalent command for SCSI and NVMe[56] interfaces ('sanitize', see par. 103), it consists of the three modes – crypto scramble, block erase and overwrite – the latter attempting to clean up all areas of user data, including bad, spare, and unallocated blocks.

- Overwrite[57] allows the user to specify the overwrite pass(es) they want to apply (e.g.: 3 passes, the 2nd using the 'invert'[57] option and 3rd being identical to the 1st)

- Crypto scramble initiates cryptographic erasure which modifies/removes the encryption keys from the medium (see section 3.2.4.):

- Block erase is used to erase flash memory media.

98. The command line software 'hdparm', already mentioned, integrates since 2016 (v.9.49) the 'Sanitize Device' feature set. It offers an alternative for suspicious users who would rather not rely on manufacturer utilities (and their varying implementation of quality) to 'sanitise' their media.

99. In order of preference, when they are supported by the data medium, it will be preferable to use the 'sanitize device' command, then the 'Enhanced Secure Erase' mode and finally the 'Secure Erase' mode (both modes of the Security Erase Unit command).

Secure Erase - confusion

100. Some devices for destroying information media (see chapter 3.3) as well as some 'sanitisation' software include the words 'secure erase' in their name or indicate that they are securely erasing data from a hard disk.

101. However, unless these devices and software specifically state that they use the 'Secure Erase' mode of the ATA 'Security Erase Unit' command, this is likely not the case. In other words, although many data erasure techniques can be considered 'secure' compared to a simple delete, not all of them include the 'ATA Secure Erase Unit' command, which is the only way to reach the purge level of confidentiality and therefore lead to an effectively secure erasure.

---

[56] The 'Sanitize' command for the NVMe interface also has the three modes – block erase, crypto erase and overwrite.

[57] The 'overwrite ext' mode fills the user data area with a four-byte pattern. The settings for this mode include a number of multiple overwrites and the ability to invert the four-byte pattern between consecutive overwrite passes ('Invert' setting).

102. If necessary, when choosing software, the reader will pay attention to this point. \\ Examples include Secure Eraser and the online command SDelete[58] (Secure Delete), which may appear to support Secure Erase, but do nothing. Remember that programs like HDDErase (see par.89) or hdparm (see par. 90) are examples of free programs that use Secure Erase.

B. Magnetic SCSI hard drives

103. Most SCSI[59] hard disks[60] (Parallel SCSI, Serial Attached SCSI, Fiber Channel, USB Attached Storage and SCSI Express included[61]) support (are supplied with) the 'sanitize'[62] command.

104. Like the equivalent command for ATA and NVMe interfaces, the sanitize command, with the overwrite option, performs one or more overwrite passes on all addressable[63] areas of the disk and allows the purge level of confidentiality. The other two options ('block erase' and 'cryptographic erase') are also similar to those of the ATA and NVMe interfaces.

C. Common notes for ATA and SCSI hard drives

105. The result of these dedicated commands, issued from the disk manager[64] itself, is especially more reliable[65] than the use of third-party software (see Article 3.2.1.1.) because the manufacturer knows its hardware well and these commands take into account all the writable areas[66] of the medium which are invisible to the operating system and the BIOS/UEFI. This technique is also faster than third-party software. In

---

[58] SDelete is part of the suite of tools for administration and troubleshooting of 'sysinternals' for Windows.
Extract from the documentation of the 'sysinternals' tools: "Secure delete applications overwrite a deleted file's on-disk data using techniques that are shown to make disk data unrecoverable, even using recovery technology that can read patterns in magnetic media that reveal weakly deleted files. SDelete (Secure Delete) is such an application. You can use SDelete both to securely delete existing files, as well as to securely erase any file data that exists in the unallocated portions of a disk (including files that you have already deleted or encrypted)."

[59] To be distinguished from SCSI SSD (solid-state drives).

[60] SCSI (Small Computer System Interface) is a set of standards describing the physical connection and transfer of data between computers and devices. SCSI standards define commands, protocols, electrical, optical and logical interfaces.

[61] Some interfaces do not comply with all of the SCSI standards but nevertheless use the SCSI command protocol.

[62] For a full description of SCSI commands: https://www.t10.org - SCSI Block Commands (T10/BSR INCITS 506 - Rev.22 15/09/2020)

[63] Zone receiving a unique address (identifying its location on the medium) in order to be accessible in read/write (sector).

[64] Tool for performing the usual disk administration tasks such as formatting, managing partitions (creation, deletion, sizing, etc.), changing the letter of a drive, etc.

[65] It seems that in some cases (for which it is difficult to assess the frequency) and at least for ATA interfaces, these commands are not or have not always been correctly implemented by some manufacturers. http://www.hddoracle.com/viewtopic.php?f=56&t=1412 .

[66] Most hard drives support the creation of hidden storage spaces that are not known to the operating system or BIOS. There are 2 examples: the Host Protected Area (HPA) and the Device Configuration Overlay (DCO). https://site.aleratec.com/blog/2011/03/31/remember-hpa-dco-sanitizing-hard-drives/

addition, the integrated commands are also less susceptible to malware attacks than third-party software.

106. Knowing that some problematic implementations of the sanitize command have been reported [65], whether the erasure is done using third-party software or through an integrated command, it will always be necessary to verify the proper execution of the instructions[67], i.e., whether the command has resulted in the expected erasure.

D. Solid State Drives (SSD)

107. As with magnetic hard disks, most manufacturers generally provide software for use with their SSD media (ATA, SCSI and NVM Express interfaces) including a firmware update tool [54], the secure erase[68] commands and optionally a media cloning tool.

108. \\ For example, the reader will find below the links to SSD tools of some well-known vendors:

- Samsung Magician (secure erase is available in the Data Management section)
- Western Digital SSD Dashboard (secure erase and sanitize are available in the Drive Management section)
- Seagate: SeaTools SSD GUI (with graphical user interface/GUI - secure erase is available in Operations - Maintenance - Erase) and SeaTools SSD CLI (without GUI - the sanitize command provides block-erase and overwrite options)
- Lenovo ThinkPad Drive Erase Utility: This utility resets the cryptographic key of the supported hard disks (HDD) (Full Disk Encryption - FDE, see Article 3.2.4.2.) and erases the solid state drive (SSD).

109. The manufacturer's website is the first place to look for a suitable secure erase tool. However, these tools do not always allow the execution of the integrated commands or if they do, the quality of the result of their execution is uncertain.

110. Therefore, in view of the characteristics of SSDs and the above, in order to achieve a sufficient level of security/confidentiality, it will be recommended to perform an additional 'sanitisation' using a different technique[69].

---

[67] Third-party software generally allow you to include a verification pass, the safest option being the use of specialised software, such as data recovery tool or disk editor.

[68] In practice, when the secure erase command is executed, the SSD controller simultaneously applies an electrical voltage to all the storage cells and resets them (release of the stored electrons). The command therefore does not write anything to the medium.

[69] In this case for ATA, we will follow a block erase by an overwrite and cryptographic erase by a secure erase. For SCSI, we will execute a sanitize-block erase after a cryptographic erase and finally for NVM Express, we will launch the user data erase command after a cryptographic erase.

3.2.2. Anonymisation

111. \\ Anonymisation, which makes it impossible to re-identify data subjects, is less and less possible to ensure as access to increasingly large and online databases intensifies.

112. \\ Therefore, this technique will not be considered as having a sufficient level of confidentiality/security. And this is regardless of the resources (time and human) needed for its execution, which further reduce its benefit compared to other techniques.

113. If anonymisation has already been carried out, before any transfer of an information medium, the validity of the method used must have been examined and a re-identification test carried out, preferably by personnel independent of the person who carried out the anonymisation (which will be all the more justified if the quantities of data on the medium are large).

114. Finally, let us not forget that modifying the data contained on a medium (values in a database for example) does not necessarily delete them from the medium (no overwriting of the data).

3.2.3. Degaussing

115. Degaussing involves applying a magnetic force of sufficient strength to erase all data from a particular magnetic medium. The effectiveness of this technique is linked to the relative strength of the magnetic force offered by the degaussing device and to the magnetic properties of the data medium.

116. Although it is an important technique for cleaning magnetic media, the reader will be able to infer from the above that degaussing is not effective, given their nature, on most flash memory devices, including SSDs. This is because they use integrated circuits to store data instead of storing it magnetically. Nor will it be used on mixed information media consisting of at least one non-volatile, non-magnetic medium.

117. This underlines the need for a correct inventory of the media, indicating their type and the associated sanitisation method, because if care is not taken to distinguish SSDs from hard drives during degaussing, the data stored on SSDs will be left intact.

118. Let us not forget that some devices can integrate both types of media (electronic and magnetic). If degaussing is considered for these hybrid devices, care will also be taken to apply a sanitisation technique suitable for the electronic storage medium.

119. The ideal inventory (see chapter 2.3.) should mention the degaussing force necessary for the 'sanitisation' of the medium, i.e. its coercivity[31]. In fact, the coercivity can be difficult to determine based only on the information on the product label. Therefore, it may be helpful to consult the device manufacturer beforehand for this information.

120. It is important to always ensure that adequate power is applied to the media (too strong, the medium risks being rendered unusable, and too weak, the data may not be properly 'sanitised'), and especially ensure that the required power evolves with the technology. In fact, the coercivity of the media increases along with their

density/capacity[70]. Newer and larger capacity media therefore require more powerful degaussers.

121. Depending on the intensity of the degaussing, the medium may be rendered unusable. In this case, degaussing also becomes a destruction technique (see section 3.3.5.). In the same vein, degaussing could also be considered in the case of a damaged medium which can no longer be 'sanitised' by a method requiring the operation of the medium.

122. As not all degaussers work in the same manner, it will be necessary to ensure that the operators who use them know their specific operating modes. For example, some devices require only a single pass while others require multiple passes, and some models require the information media to be disassembled while others do not.

123. For your information, the NSA publishes an updated list of degaussers to safely 'sanitise' magnetic tapes and hard drives. The devices listed in this document[71] are listed against the coercivity of the storage device that they can safely erase.

3.2.4. Cryptographic erase (crypto-erase - CE)

124. It is the last of the "sanitisation" techniques preserving the medium which is presented because, although it is a technique in its own right, it is often used as a complement to others.

125. The aim of the methods presented in this document is, ultimately, to make the data contained on a medium permanently inaccessible. Data encryption[72] can, at first glance, also achieve this objective by making these data unintelligible to anyone who does not have access to the decryption key. It is this additional step, i.e. the final destruction of the key allowing the decryption, which constitutes the difference between encryption and cryptographic erasure and allows this technique to be a "sanitisation" technique.

126. Encryption is of course very useful in many other data protection cases. It is indeed a significant measure to counter a loss of confidentiality, in the event of theft, unauthorised access or loss of the medium. Encryption is also mentioned in the GDPR[73], as a potential means of mitigating the risks for data subjects, and in certain

---

[70] In order to increase the magnetic storage density, the area allocated to each bit must be reduced. For this, it is necessary to use magnetic materials with increased coercivity to prevent the information from being erased due to interactions with nearby bits. This makes bit recording more difficult because it requires a higher magnetic field. This also explains why with the increase in capacities, it becomes more difficult to degauss (the power required increases) the media concerned.

[71] https://www.nsa.gov/Portals/70/documents/resources/everyone/media-destruction/NSAEPLMagneticDegaussersMarch2020.pdf?ver=2020-03-17-094749-040

[72] Encrypting an information medium is usually based on an authentication key and a data encryption key. The encryption key is the key with which data is actually encrypted and decrypted. The authentication key relies on the user's password or passphrase and is used to decrypt the data encryption key (which in turn decrypts the data). With this two-level approach, the user can thus change their password without having to encrypt all their data again, because the encryption key remains unchanged (it will have to be re-encrypted using the user's new password).

[73] Encryption is mentioned in Articles 6§4.e (lawfulness), Article 32§1.a (security) and Article 34§3.a (communication to the data subject) of the GDPR.

cases exempting from the communication of a data breach to data subjects (Art.34.3.a of the GDPR)[74]. But this is outside the scope of the analysis covered by this document.

3.2.4.1. Integrated commands

127. Both the ATA/IDE (crypto scramble option) and SCSI (cryptographic erase option) command groups discussed in Article 3.2.1.2., include specific commands that enable cryptographic erasure of data located on the medium. However, they are not implemented on all media from all manufacturers.

128. If this technique is used, the NIST (guidelines SP.880-88r1) recommends overwriting the medium subsequently, either through the other integrated commands or using third-party software (see Article 3.2.1.1.). This is to reduce the potential risk generated by a decryption key still present and accessible on the medium following an ineffective or absent destruction.

129. NB: we have seen (par.92) that two distinct ATA commands, bearing a similar name, existed and presented differences for overwrite operations (Secure Erase and Enhanced Secure Erase). When used for media encryption, whether one or the other is used, they will produce the same result.

3.2.4.2. SEDs

130. Many information media contain integrated "self-encryption" mechanisms. This is generally referred to as hardware-based full disk encryption (FDE) and more particularly self-encrypting devices (SEDs[75]), when it comes to hard disks or solid state drives (SSD). Self-encryption means that all the data written to the medium is encrypted by the medium before it is written and decrypted by the medium when it is read[76]. The encryption key is known only to the medium, but it can nevertheless be changed by an authorised user. If the key is modified, any data previously written with the initial key becomes unreadable. The key can therefore be changed to 'destroy' the data by making them irrecoverable (unreadable).

131. The cryptographic erasure technique is therefore easy and above all quick to perform on the SEDs since the encryption phase has already been performed.

---

[74] Article 34.3.a of the GDPR: The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;"

[75] For example, here is the link to the detailed technical guide (EN) on the security implementation and full encryption of Seagate SED models:

https://www.seagate.com/files/staticfiles/support/docs/manual/Interface%20manuals/100515636c.pdf.

[76] In practice, for FDE media, data are always encrypted (via the data encryption key) when stored on the medium, even if there is no defined password (in the case, for example, of a new disk or of a user who does not wish to set a password).

132. The SEDs which comply with the OPAL[77] standard of the Trusted Computing Group[78] use the AES[79] (Advanced Encryption Standard) encryption algorithm with 128- or 256-bit keys. For these media, cryptographic erasure is called "PSID Revert" because it requires, before launching the command itself and erasing the keys, a unique ID specific to each medium to be entered: the PSID[80] or Physical Security ID.

3.2.4.3. Security vulnerabilities of SEDs

133. \\ Another important point lies in the publication of a study highlighting a security flaw in the integrated "self-encryption" mechanism of SSDs and allowing this encryption to be bypassed if one has physical access to the information medium.

134. Depending on the risk analysis, a software encryption solution, such as open source software VeraCrypt (for Windows, Mac OSX and Linux) and LUKS (Linux Unified Key Setup), may be preferred to the hardware-based solution.

135. It should be noted that some manufacturers take these potential violations of SSD disks into account and issue warnings (e.g.: Samsung).

3.2.4.4. Important points

136. This technique (encryption followed by cryptographic erasure) can be used on other media (which are not SEDs or do not support integrated commands), by using third-party encryption software and by permanently deleting the keys, once the encryption is complete. The prior encryption of the medium can, however, be a very time-consuming process (several hours, depending on the capacity of the medium, its write/read speed and the computing power allocated to the operation).

137. In contrast, the on-the-fly encryption of SEDs makes the cryptographic erasure technique very fast and almost immediately prevents access to the data contained on the medium.

138. In the case of cryptographic erasure, it is also necessary to be sure that no personal data has been written before the on-the-fly encryption because these will not be protected by the cryptographic erasure.

139. In the risk analysis prior to choosing this technique, the manager will have to take into account future technological developments which may make current encryption methods less secure.

---

[77] A set of specifications for self-encrypting drives developed by the TCG to protect the confidentiality of stored data.

[78] The TCG is a group of companies created to develop and promote trusted computing standards and technologies which must allow hardware manufacturers to have control over what can run on their systems and refuse non-validated (unsigned) software to be run. Its members include Western Digital, Samsung, Seagate, HP, Toshiba, Lenovo, Dell or Microsoft.

[79] The AES encrypts the plaintext, in blocks of 128 bits at a time, using symmetric keys of 128, 192, or 256 bits. A symmetric key is a key which is used both to encrypt a text and to decrypt this same text.

[80] The PSID is a unique identifier consisting of 32 alphanumeric characters that is most often printed on the medium label.

140. The encryption operation, performed to prevent access to the data contained on the medium, must be carried out according to a procedure validated by the controller.

3.2.4.5. Risks

141. Once encrypted, the data, although saved in another form, is still present on the medium. The use of this technique therefore implies that the encryption algorithm is sufficiently robust to resist decryption without knowledge of the key and, on the other hand, that the initial key (i.e. before its modification/destruction) is not, in any way, recoverable, both on the medium itself and elsewhere (also consider any backups). These requirements are common to techniques using encryption.

142. This procedure will provide that:

- The encryption algorithm used is recognised and secure[81,82] (do not use an obsolete algorithm such as DES or 3DES for example);
- The encryption keys used are of sufficient length [83,82];
- The encryption keys used are managed correctly (they are not on the medium and in any case, not in plain text);
- Encryption is either applied to the entire media or to a logical subdivision of it (as opposed to encryption of individual directories or files).

Note that most modern encryption techniques meet these requirements.

143. Along with the risks associated with technological developments, cryptographic erasure, or more precisely encryption, also presents intrinsic risks linked to a possible weakness of the password protecting the authentication key (if applicable), the presence of keys in memory, the existence of unencrypted data in temporary files or even the weakness of the encryption protocol used. In addition, the certainty that the encryption keys are indeed made permanently inaccessible, can be difficult to establish[84].

144. Finally, note that, with regard to inaccessible areas of the medium, hardware-independent encryption software is subject to the same limitations as third-party 'sanitisation' software (see Article 3.2.1.1.).

145. Therefore, like the NIST, we recommend carrying out, following a cryptographic erase, an erasure/overwriting of the medium (with verification). This is particularly to

---

[81] \\ For example, Appendix B1 of the general security reference system published by ANSSI recommends the AES symmetric encryption mechanism (links in Appendix C).

[82] ENISA (European Union Agency for Cybersecurity) also publishes documents relating to recommended algorithms, key lengths, encryption protocols and parameters on its website.

[83] \\ For example, Appendix B1 of the general security reference system published by ANSSI recommends a minimum symmetric key size of 128 bits (links in Appendix C).

[84] On this subject, see section 4.7.3 (Verification of Sanitization Results) of the guidelines SP.880-88r1 of the NIST, where the specific case of cryptographic erase is discussed on p.21.

reduce the potential risk generated by a decryption key still present and accessible on the medium following an ineffective or absent destruction.

Ideal situation

146. In the best of all worlds, the manufacturers of SEDs or media offering 'secure erase' commands should provide, in detail, all the necessary information on the commands implemented and above all guarantee the result of the erasure, preferably contractually. Moreover, nothing prevents the controller from requesting written assurances on this subject when purchasing these media.

3.3. The data medium is destroyed

147. It should be noted from the outset that there are a number of cases where the physical destruction of the information medium should be preferred to its 'sanitisation':

- If the media is defective;
- If the drive is defective;
- If the equipment required to access the data is no longer available;
- If the media type makes 'sanitisation' impossible, such as WORM media (write once, read many - example: write once CD-ROM);
- If the verification step that closes the purge or clear methods does not give safe results or it fails (for known or unknown reasons).

148. Regardless of environmental concerns, it may be more economical to destroy media than to 'sanitise' them for reuse.

149. Finally, it should be noted that chemical destruction will not be considered in this document. Even if certain chemical agents are capable of attacking data media and destroying them, this rarely used technique is also dangerous for health and harmful for the environment.

3.3.1. Segmentation of techniques

150. A) Certain destruction techniques only partially damage the medium.

- As a result, the data stored on intact parts can remain accessible. This is the case with the deformation techniques discussed in the following section 3.3.2.

151. B) Other techniques, such as shredding, crushing or disintegration break the medium into pieces (see section 3.3.3.).

- It is important to realise that in this case too, the data are still present on the targeted medium. They are simply divided into smaller parts. Given that a hard disk can contain several terabytes of data, a fragment of a hard disk tray, barely one cm^2 in size, can still contain several gigabytes of data.

- The level of security/confidentiality provided by a fragmentation of the medium will be linked to the size of the fragments obtained. The smaller the fragments, the more resources and time it will take to reconstruct the data. This link (size of fragments - security/confidentiality) is at the core of the DIN 66399 standard, discussed in section 3.3.6.

152. C) Finally, a 3rd group of techniques allows the complete destruction of the medium and especially of the data it contains.

- The result is achieved by changing the state of the support, i.e. by changing it from the solid state to the gaseous state (sublimation) or to the liquid state (melting).

3.3.2. Physical deformation

153. A large number of different techniques are covered by the term 'physical deformation[85] techniques'. They can be implemented, both by large industrial devices, and by common tools such as a hammer, a compressed air nailer, a drill or even a press.

154. These techniques include in particular:

- Folding / bending;
- Cutting;
- And drilling / puncturing / punching / piercing.

155. Benders use a metal wedge to bend a medium (mostly hard drives) along its length at a 90 degree angle. The metal wedge, pressed with great force, damages the platters, read heads, electric motor and electronics of the hard disk such that it is no longer accessible through its interface.

156. With regard to puncturing, while you immediately think of a technician using his drill to make holes in a hard disk, this is not the method recommended by the ITAD sector (IT Asset Disposition). There are machines for implementing this method. A hole punch uses a hardened steel pin to pierce through the media. When drilling a hard drive, the platters, read heads, electric motor and electronics are damaged such that it is no longer accessible through its interface.

157. Some devices offer an optional module that can also destroy SSD (Solid State Drive) by puncturing. Depending on the model, the SSD is pierced in several places with metal pins or cracked in a wave shape.

158. The common factor in these techniques is that they only partially damage the medium and leave the data stored on the parts not affected by the deformation accessible.

---

[85] n/a

159. As a result, these techniques do not achieve the destroy level of confidentiality, even though they may make the data impossible to retrieve through the media interface and the media cannot be used for subsequent storage. The medium is in fact not considered 'destroyed' as long as data recovery is possible, even if this requires state-of-the-art laboratory techniques.

160. As confirmation, in its reference document[86] on the subject, the NSA (National Security Agency of the United States) cites deformation techniques only as complementary but nevertheless highly recommended measures[87], to degaussing of magnetic hard drives. Deformation alone is therefore not validated by the NSA as a 'sanitisation' method.

3.3.3. Shredding, crushing and disintegration[88]

161. While these techniques are different, all three result in the breaking down of the medium, transforming it into smaller components. The size of the debris will depend on the technique, the materials making up the medium and technical characteristics of the device used for this.

162. Shredders, for example, come in a wide range of sizes and depending on the model, can shred just about anything from tyres to hard drives or SSDs, to paper or even a sofa. The average size of the debris will depend on the model while their individual size will depend on the materials used in their composition. Thus, for a hard drive, the plastic pieces of the case will especially be larger than the pieces of the platters.

163. The choice of one technique rather than another is secondary to the size of the debris obtained. This is why we will not dwell, beyond a simple description, on the techniques themselves.

164. As specified by the ISO/IEC 21964 standard, "in this context (destruction of the medium), securely destroying means destroying the data media containing the personal data, such that the recovery of information concerning them is impossible or is only possible with considerable expenditure (in terms of personnel, material resources and time)".

3.3.3.1. Shredding

165. Shredders consist of juxtaposed cylinders carrying hardened steel knives, which rotate in opposite directions to cut, tear and extrude materials. For the materials that we are specifically interested in, there are shredders that accept only thin media, such as optical media (CD, DVD, Blu-Ray), memory media (USB keys, memory cards), magnetic tapes (audio, video, data), magnetic or chip cards of all types, while others also accept smartphones, tablets, hard drives and possibly SSDs and finally other devices dedicated to paper destruction.

---

[86] NSA/CSS Storage Device Sanitization Manual

[87] However, the NSA is evaluating the ability of some devices to deform the platters of a hard drive (magnetic) in 30 seconds or less, by bending, punching or waffling. Devices meeting these criteria are covered in the document 'NSA/CSS Evaluated Products List for Hard Disk Drive Destruction Devices'

[88] n/a

166. A paper shredder is a mechanical device used to cut paper into strips or particles. Note that it can also be used to destroy flexible media such as floppy disks, once the media are physically removed from their outer containers. The size of the shreds should be small enough that there is reasonable assurance, commensurate with the confidentiality of the data, that the data cannot be reconstructed. To be approved by the NSA, paper shredders must be able to reduce paper documents into fragments measuring no more than one millimetre by five millimetres[89]. Disintegrators can also destroy paper documents (see par.178)

Solid State Drives - SSDs

167. Once again, note that hard disks (magnetic) and SSDs (electronic) have very different technical characteristics and cannot, therefore, be 'sanitised'/destroyed in the same way.

168. Shredders not specifically suited for these media will produce debris too large to safely destroy data on high density semiconductor chips.

169. The NSA security standards require that hard drives be reduced to a final particle size of two millimetres, i.e., be degaussed and then physically destroyed (shredders or crushers). This second option is not possible for SSDs. However, according to a study conducted by firm Blancco (Dec. 2018), many organisations (33% in the USA and Canada) do not have a different process for handling these 2 types of media.

170. With ever-increasing data storage density, the size of chips on SSDs is reducing. Shredding to sizes larger than these components can therefore leave the information on the media completely intact.

171. To make the reconstruction of the data even more difficult, the shredded material can be mixed with a non-sensitive material of the same type (shredded paper or shredded flexible media), with a larger amount of debris increasing the difficulty of reconstruction accordingly. This is also valid for all techniques and types of destruction residues.

3.3.3.2. Crushing

172. Crushers use compressive force to crush the medium by breaking it into pieces (examples: between two jaws, one of which is fixed - jaw crusher or by percussion - impact crusher).

173. The term crusher is sometimes used for "devices capable of reducing the data-bearing layer of an optical disc to fine dust while leaving the disc itself intact for recycling or disposal. However, this method cannot be used for DVDs since their information medium layer is sandwiched in the centre" (source: BCSS[90]). However, in this case it will be more of an abrasion technique. We will add that Blu-Ray discs have the same problem.

---

[89] https://www.nsa.gov/Portals/70/documents/resources/everyone/media-destruction/NSAEPLPaperShreddersMarch2020.pdf?ver=2020-03-17-094747-943

[90] Document of the BCSS (Belgian Crossroads Bank for Social Security): Information security & privacy guideline - Erasure of electronic information media (March 2017) p.7

174. Still on the subject of optical media, let us note that the NSA also publishes, like for hard disks [87] and other types of media[91], a list of devices validated[92] for destruction by fragmentation. To be included, the devices must provide residues whose side does not exceed:

- For CDs, a length of 5 millimetres;
- For DVDs and Blu-Ray, a length of 2 millimetres.

3.3.3.3. Disintegration

175. The term disintegration/disintegrator is often used when the size of the fragments obtained is less than or equal to two millimetres per side. This size is related to the NSA prescriptions, mentioned in the document NSA/CSS Storage Device Sanitization Manual. If the hardware has been tested by the NSA and meets the requirements of the manual, it will be included in the NSA/CSS Evaluated Products List for Hard Disk Drive Destruction Devices.

176. In parallel, it is recommended to disintegrate media (both HD and SSD) in batches with other storage devices.

177. Disc disintegrators use knife milling technology to cut the media into pieces continuously until the pieces are small enough to pass through a waste sieve of specific size. Disintegration is slower than shredding but the size of the debris is smaller and the level of security/confidentiality achieved is higher.

178. Paper disintegrators (different from paper shredders - see par.166) must, to be approved by the NSA, produce shreds with sides no greater than three millimetres by five millimetres[93].

3.3.3.4. Notes

179. Note that translation tools are not very precise, and can produce several different translations for the same technique in the same sentence. Websites dealing with the physical destruction of information media (including some manufacturers) also quite frequently mix up the names of devices and techniques, or even use names unrelated to the technology used (destroyer, disassembly device, cracker, etc.).

180. We have seen, for example, that for an information medium such as hard disks and SSDs to be considered by the NSA as adequately 'sanitised' using a disintegration technique, two conditions must be met: the residues must be no more than 2mm on one side and the device used must be part of the list of approved devices (there are only American companies). This differs from the DIN 66399 standard.

---

[91] https://www.nsa.gov/resources/everyone/media-destruction/

[92] NSA/CSS Evaluated Products List for Optical Destruction Devices

[93] https://www.nsa.gov/Portals/70/documents/resources/everyone/media-destruction/NSAEPLPaperDisintegratorsMarch2020.pdf?ver=2020-03-17-094733-413

181. This standard specifies, depending on the size of the residue, what level of security is achieved by a destruction method, for six major classes of information media (e.g. paper, optical, electronic or magnetic); we will come back to this in section 3.3.6.

182. The controller will bear in mind that when it chooses to use an external service provider in order to dispose of its media using the techniques discussed in chapter 3.3., once the destruction has been carried out, this service provider will probably recycle them or deposit them in a landfill.

183. This means that the data, if the media has not been securely destroyed, will again potentially be accessible to third parties. The remains of the media could even end up in different parts of the world if they are sold to waste management or recycling companies. Incineration eliminates this risk.

3.3.4. Incineration

184. Incineration, although more rarely used and having a significant environmental impact, is an effective technique because, if carried out in suitable incinerators[94], it alone guarantees the total and irreversible destruction of data and media. These can consist of large waste incinerators, as well as smaller mobile and compact incinerators that specialist companies can bring to the site of the controller who requests them. Some mobile models are dedicated to eliminating paper but others are also able to melt metal.

185. As part of their digital transformation, many organisations digitise documents to store them online or archive them and then end up with the originals for disposal. When quantities of paper to be disposed of are large, incineration can be an alternative to shredding.

186. Other types of media can be destroyed by this technique. In its manual relating to media sanitisation, the NSA cites magnetic tapes, floppy disks, optical media, electronic media and paper as being capable of being destroyed in a secure manner by incineration, provided that the material was reduced to ashes. Regarding hard disks, it specifies that the lining of the internal platters must be reduced to ash and/or the internal platters must be physically deformed by the action of heat.

187. If the incineration takes place outside the control of the controller, the latter will ensure that a processing of the media, offering a complete traceability chain, is set up by the external service provider(s).

3.3.5. Degaussing

188. Degaussing, already presented as a 'sanitisation' technique (with preservation of the medium - see section 3.2.3.), also makes it possible to destroy (render unusable) magnetic media if they are subjected to a sufficient magnetic force[95], regardless of their operating system and interface, even if they are damaged.

---

[94] Unit which allows almost total combustion of the combustible constituents of waste.

[95] Examples of degaussers capable of destroying hard disks and magnetic tapes

189. It must be reiterated that degaussing is not effective on flash memory devices including SSDs. Likewise, this technique is not suitable for paper and optical media.

190. Degaussing subjects magnetic media to a strong magnetic field which can be created either by strong magnets or by electromagnetic discharge.

191. It is recommended that degaussing be followed by another destruction technique. This will help to achieve the highest level of confidentiality/security, compensate for a degausser failure or an oversight on the technician's part, and provide visual verification that the media has been destroyed and is ready for disposal. Under these conditions and with the use of an approved[717196], the NSA validates the technique at the purge level.

3.3.6. The DIN 66399 standard

192. The DIN 66399 standard of Deutsches Institut für Normung, titled "Büro- und Datentechnik - Vernichten von Datenträgern"[97] specifies, depending on the size of the debris resulting from the destruction of the medium, what level of security is reached by devices the intended use of which is to destroy data media.

193. Very popular in Europe, it takes less account of the technique used than of the results thereof, for six major classes of information media.

194. This standard (fee-based[98]) or more exactly this series of standards is made up of three parts[99]:

- Part 1: Principles and definitions (publication 10/12);
- Part 2: Requirements for equipment for destruction of data carriers (publication 10/12);
- Part 3: Process for destruction of data carriers (publication 02/13).

195. Although it has been replaced since 2012 by the DIN 66399 standard, the classification[100] related to the obsolete DIN 32357 standard (1995), which applied exclusively to paper, is still often cited in the description of the devices concerned (mainly paper shredders).

196. The DIN 66399 standard defines protection classes, media categories and security levels.

---

[96] The degausser is a finely tuned magnet that comes into contact with other magnetic media and can destroy the magnetic signature of any stored data.

[97] German Institute for Standardization - "Office machines - Destruction of data carriers"

[98] Each part costs a few tens of euros.

[99] Part 1: Principles and definitions, Part 2: Requirements for equipment for destruction of data carriers and Part 3: Process for destruction of data media.

[100] The DIN 32757 standard defines 5 security levels. The literature also includes an unofficial 6th level 'Level 6 - Highest Security'. These security levels are linked to the fineness of the shredding of the material and therefore express the level of security offered by the shredders.

Three protection classes

197. They determine the extent to which data should be protected, based on an assessment of the type of data present on the medium. The protection/security requirement is divided into normal, high and very high categories:

- Protection class 1 - Normal security requirement for internal data. The loss of data would have a negative impact on the organisation or would present a risk of identity theft for the data subjects;

- Protection class 2 - Higher security requirements for confidential data. The loss of data would have a very negative impact on the organisation or could violate its legal obligations or present a financial or social risk for the data subjects;

- Protection class 3 - Very high protection requirements for very confidential and secret data. The loss of data could have irreparable consequences for the organisation or pose a risk to the health and safety or the individual freedoms of the data subjects.

Six categories of data media

198. The standard divides the different types of data media into 6 categories or classes:

- Class P (paper) – Information in original size (paper, x-ray films);

- Class F (microfilm) – Information in reduced format (microfilm);

- Class O (optical) - Optical data media (CD, DVD, Blu-Ray);

- Class T (tape) - Magnetic data media (tapes, floppy disks, credit cards);

- Class H (hard drive) - Magnetic hard drives;

- Class E (electronic) - Electronic data media (USB key, SSD, memory cards, smart cards, flash memory for smartphones and tablets, memory cards for digital cameras).

Seven levels of security

199. The seven security levels are derived from the three protection classes, each of the classes covering three security levels:

- Protection class 1 - Security levels 1, 2 and 3

- Protection class 2 - Security levels 3, 4 and 5

- Protection class 3 - Security levels 5, 6 and 7

200. These security levels determine the amount of effort and resources that will be required to recover data from destroyed media (the higher the security level, the smaller the debris must be):

- Security level 1 - Data recovery requires a simple effort (concerns general documents to be made illegible).

In other words, level 1 is selected for ordinary data, for which little or no protection is necessary (for example brochures and newspapers) and whose possible reconstitution from the destroyed medium would not present any data protection problem;

- Security level 2 - Data recovery requires special effort and tools (concerns internal documents to be made illegible);

- Security level 3 - Data recovery requires a considerable effort in terms of manpower, time and tools (concerns sensitive/confidential data as well as personal data subject to high protection requirements);

- Security level 4 - Data recovery requires exceptional effort and uncommon tools (concerns highly sensitive/confidential data as well as personal data subject to high protection requirements);

- Security level 5 - Data recovery possible only with uncommon tools (concerns confidential data of fundamental importance for an organisation or the data subjects);

- Security level 6 - Data recovery is unlikely with the current state of technology (concerns confidential data subject to extraordinary protection requirements);

- Security level 7 - Data recovery is impossible with the current state of technology (concerns strictly confidential data subject to the highest protection requirements).

In other words, level 7 is selected for 'top-secret' data (secret services, military documents), when the possibility of reconstructing the data from the destroyed medium must be absolutely ruled out (according to the current state of knowledge).

Tables

201. We can group all of these elements together in a table to find the necessary level of destruction.

	Protection class 1		Protection class 2		Protection class 3		
Category of data media	Security level 1	Security level 2	Security level 3	Security level 4	Security level 5	Security level 6	Security level 7
P	P-1	P-2	P-3	P-4	P-5	P-6	P-7
F	F-1	F-2	F-3	F-4	F-5	F-6	F-7
O	O-1	O-2	O-3	O-4	O-5	O-6	O-7
T	T-1	T-2	T-3	T-4	T-5	T-6	T-7
H	H-1	H-2	H-3	H-4	H-5	H-6	H-7
E	E-1	E-2	E-3	E-4	E-5	E-6	E-7

202. For example, here are the recommended security levels for media categories H and P:

H – Magnetic hard drives		P – Original size (paper)	
Security level	**Status / Max. particles size**	**Security level**	**Status / Max. particle size**
H-1	Out of order	P-1	Strip width of 12 mm ou 2000 mm^2
H-2	Damaged	P-2	Strip width of 6 mm or 800 mm^2
H-3	Deformed	P-3	Strip width of 2 mm or 320 mm^2
H-4	160 mm^2	P-4	160 mm^2
H-5	30 mm^2	P-5	30 mm^2
H-6	10 mm^2	P-6	10 mm^2
H-7	5 mm^2	P-7	5 mm^2

203. Note: at level H1, the disk may be out of service for mechanical or electronic reasons.

Examples of interpretation

204. Many manufacturers and resellers add references such as "E-1 / H-3" or "T-1 / E-2 / H-3" to the description of their media destruction devices. According to the manufacturers, these are the security levels as per the media class of the DIN 66399 standard which the equipment can achieve. Here are some examples of how these security levels are interpreted:

- A hard drive falling under media category "H" (see table above) and containing sensitive or confidential data requiring security level 3 (i.e. level H-3) must be deformed to meet the requirements of the DIN 66399 standard.

- If a destruction device indicates that it has reached level P-5 (see table above), this means that it meets security level 5 for media in the original format (e.g.: paper - "P" category of data media) and that it is therefore capable of shredding the medium into particles of 30 mm^2. Such a device will therefore meet the requirements of the DIN standard for highly confidential data (for example medical documents). Once destroyed by this device, these data can no longer be reconstructed using usual techniques.

- A microfilm belonging to the "F" category of media (table not provided above), which is highly confidential and which requires a security level 5 (i.e. level F-5) must be shredded to a particle size of up to 1 mm^2.

Use of the DIN standard in practice

205. Steps to determine the security level to be reached and the maximum size of the residue after destruction of the medium in order to select the appropriate destruction device:

A. Among the 3 protection classes, choose the one corresponding to the level of confidentiality/security of the data contained on the media to be destroyed (internal document, confidential or highly confidential)

B. The selected protection class then offers you a choice among 3 security levels (the higher the selected security level, the smaller the residue).

C. Then select the type of medium to be destroyed (paper, electronic, magnetic tapes, etc.)

D. Now connect the data medium and the security level. You can then use this information to select an appropriate document shredder.

DIN and ISO

206. In 2018, ISO/IEC JTC101 standardised at the international level the DIN 66399 standard, developed in 2013. Numbered ISO/IEC 21964, this standard is now referenced by organisations around the world for data destruction requirements. The materials referenced in the security levels are identical to those referenced in the DIN 66399 standard.

207. The 3 parts of the DIN standard (see par.194) correspond to the following 3 parts of the ISO standard:

- ISO/IEC 21964-1:2018 - Information technology — Destruction of data carriers — Part 1: Principles and definitions
- ISO/IEC 21964-2:2018 - Information technology — Destruction of data carriers — Part 2: Requirements for equipment for destruction of data carriers
- ISO/IEC 21964-3:2018 - Information technology — Destruction of data carriers — Part 3: Process of destruction of data carriers

DIN - NSA - NIST comparison

208. In general, the DIN 66399 standard is not as demanding as the NIST or NSA guidelines and standards.

209. Thus, contrary to the DIN standard, the NSA recommends that the destruction of hard disks (magnetic and electronic) be preceded by degaussing. In addition, destruction must be done with devices approved by the NSA.

210. Furthermore, degaussing, like any technique that does not result in fragmentation of the medium, is not taken into account by the DIN standard, whereas the NSA on the one hand, integrates it and recommends that it be followed by a deformation or destruction technique and the NIST on the other hand, integrates it at the purge level (and indirectly at the destroy level, given the irreparable damage that the technique can cause).

211. With regard to the security levels themselves, the NIST requires, for example for paper media, shredding that produces residues of no more than 1mm x 5mm per side,

[101] Joint Technical Committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission.

or spraying/disintegration using a device fitted with a 2.4 mm safety screen[102]. Only the latest DIN security level (P-7) meets this requirement (maximum residue size of 5 mm^2).

212. Another peculiarity, associated with each security level of the DIN standard and absent from the NIST and NSA guidelines and standards, also reduces the level of requirement. It is the permissible deviation or discrepancy from the recommended particle size for each security level of the DIN standard.

213. For example, the security level H5 (see table par.202) of the DIN standard, specifies a maximum residue size of 320 mm^2, but the full specifications of this level actually state that only 90% of these particles must be less than or equal to this size and allows 10% of them to reach 800 mm^2. This in itself would tend to disqualify H5 as acceptable for confidential data of fundamental importance to an organisation or the data subject.

214. This permissible deviation is defined at each security level for each type of medium.

215. In summary, the DIN 66399 standard is easy to read and useful to the business world but is arguably less suitable for media containing highly confidential data and requiring a high level of security, than the NIST and NSA guidelines and standards.

[102] The medium is cut continuously until the resulting particles are small enough to pass through a sieve of specific size.

4. Special cases

216. It is not always possible for the controller to erase or destroy the information media.

217. This is the case when the media are not owned by it. For example, IT equipment under rental contract (printers/photocopiers, server infrastructure at the IT service provider's premises, cloud computing or even video surveillance system with recording).

218. The controller must thus ensure that the contract provides for the possibility of erasing the data or destroying the media according to a method that is acceptable to it and whose proper execution and result it will be able to verify. If contractual adaptation or control prove to be difficult, the controller can also negotiate a purchase of the media contained in the devices.

219. We cannot overemphasise the need to address data protection issues before the contract is signed. This often turns out to be difficult afterwards.

220. This is also the case when a device containing an information medium (or the medium itself) must be repaired, replaced or undergo maintenance outside your scope of control. You must then assess the risk associated with access to the data by the service provider. It should be reiterated that the GDPR focuses on the impact of a loss of confidentiality for the data subjects (the people to whom the data relate).

221. If this operation presents a risk to the data subjects, it must remain under the control of the controller (e.g. on-site repair or purchase of a replacement medium in order to keep the defective one[103]).

[103] It should be noted that some suppliers (including HP, Dell and Lenovo) offer the possibility of subscribing to an additional "keep your drive" guarantee allowing the customer to retain defective media which must be replaced.

5. Verification

222. The last step of the procedure prior to the issuance of a document certifying the sanitisation or destruction (see 6th part "Recording"), is to verify the destruction of the data, which helps to ensure that they have been properly sanitised or destroyed. It is essential because there could be multiple causes of failure. Consider human errors (e.g.: unprocessed disk put in the stack of processed disks, lack of training, desire to finish fast), hardware errors (e.g.: damaged shredder knife or failure of one of the components located between the erasure software and the data on the disks) and software errors (lack of update, software quality).

223. When the controller calls on a subcontractor for the sanitisation or destruction operations, this will require discussing the verification procedures with the latter and possibly defining them contractually.

224. The verification is ideally performed by an independent person who has not taken part in the actual destruction or sanitisation of the data media. Following the same logic, when software is used for data sanitisation, the verification part should be performed by software different from that used for sanitisation.

225. This quality control process is documented in the same way as the other steps of the destruction/sanitisation procedure. For example, the number of samples to be tested will be provided for in the documentation.

226. In addition to this documentation, the controller must have an information system that allows, on request, to produce proof of compliance (i.e. confirm the successful erasure of data), medium by medium.

227. We will end this 5th part with some verification information specific to different 'sanitisation' techniques.

Erasure - overwriting

228. Depending on its extent, the result of the verification may be more or less reliable, the best assurance of an effective 'sanitisation' of the data being generally obtained by a complete reading of all the accessible areas of the medium, in order to ensure that they comprise the expected values (binary numbers 0 or 1), i.e. those decided in the configuration of the overwrite pass.

229. This verification reading is obviously possible when the media is not destroyed.

230. Even though the verification is a time-consuming process, the percentage of the medium surface to be verified should, depending on the time available, be as large as possible, and in any case should not be less than 10% (which is also often the percentage offered by default by third-party software).

231. Third-party software and integrated commands provide verification capabilities. However, if you wish to carry out a manual and independent verification of the tool used for sanitisation, a disk editor (often combined with a hex editor) can be used. These software are also most often used for data recovery and digital forensics. \\ For example, we will cite three of these software: Active@ Disk Editor and HxD (freeware) as well as WinHex (well-known commercial software).

232. For the clear and purge levels, either with third-party software or when an integrated overwrite command is used, the verification shall confirm that the expected values (see par.228) are present on the medium. In case several overwrite passes have been applied, the values of the last pass will be considered.

Cryptographic erasure

233. In the case of cryptographic erasure, the most effective verification will be to read random locations before erasure, and again after cryptographic erasure to compare the results.

234. This means that if the cryptographic erasure is followed by another technique (e.g. destruction), the verification must be carried out before the latter. Verification via rapid sampling will also be performed after the additional technique is performed.

Shredding, crushing, disintegration

235. For media that have been reduced to pieces, a verification of the size of the residues will be carried out visually or using a sieve corresponding to the maximum accepted size or another measuring instrument (e.g. high-precision digital caliper).

Degaussing

236. Ensuring proper degaussing depends primarily on selecting an effective degausser, using it properly, and periodically carrying out verification of the results to ensure it is working as intended.

6. Recording

237. Proof of destruction is an essential part of the traceability chain. In accordance with the principle of accountability of the GDPR (Article 5.2), it will allow the controller to demonstrate compliance with the principles applicable to the processing of personal data, including those relating to limitation of storage and integrity and confidentiality (Art.5.1.e and f - see Appendix B).

238. It is therefore important to record and keep information relating to the proper conduct of sanitisation and/or destruction and to the technique (and thus to the level of confidentiality/security selected), whether the procedure is carried out internally or with the help of a subcontractor. Proof of destruction/sanitisation is generally issued by the person in charge of the operation (under the authority of the subcontractor or the controller) and validated by a person designated by the controller.

239. Although this proof is often called 'certificate' of destruction by the various players in the sector, we prefer the terms attestation or declaration, for their less official connotation[104].

Subcontracting

240. When a subcontractor is called upon for the sanitisation and/or destruction of information media, the latter can be collected and retained by the controller in a place to which access is not secure, until the subcontractor collects them. Temporary storage of these media does not exclude the possibility of loss or theft. Therefore, it may be useful to compare the list of media that have been stored and the list of media that are actually supported by the external service provider. We would like to remind you of the need to appoint one or more managers for each stage of processing, including those for collecting media and storing them.

241. The actual sanitisation process can be carried out on the controller's site or off-site (depending on the technical possibilities at the subcontractor's disposal or the request of the controller). In the case of off-site operations, ideally a representative of the controller should be physically present throughout the destruction process, in order to ensure that the media have indeed been destroyed. Without this, the "proof of destruction" submitted by the subcontractor might not correspond to reality and not constitute documentary evidence. The controller may also call on bailiffs to control and record all of the operations.

242. As already mentioned in par.58, the issuance by the subcontractor of a sanitisation/destruction certificate must be part of the contractual agreement concluded with it. If data which were to be processed under the contract are found subsequently, the certificate may constitute proof that the subcontractor has committed a fault.

Certificate

243. Proof of sanitisation/destruction will be in the form of a detailed certificate for each medium that has been processed. Whether in paper or digital format, it is a

[104] The Merriam-Webster defines a certificate as a "a document containing a certified statement especially as to the truth of something".

critical element that must make it possible to validate that the data has been rendered irrecoverable from the medium that has been sanitised.

244. It generally lists each storage device by serial number, describes the level of confidentiality/security targeted (clear, purge, destroy, H-1, P-5, etc.), the sanitisation technique used (degaussing, shredding, cryptographic erasure, etc.), the tools used to achieve this, the verification method used and its result as well as other information, for example related to the date, place and persons involved.

245. Concisely, the destruction certificate will include information relating to:

- The date and place of the procedure;
- The organisation, the person carrying out the destruction (identification);
- The data medium and the equipment incorporating this medium (serial number, type, etc.);
- The technique used (software and hardware tools, level of confidentiality/security, reference standard, method, etc.);
- The verification (method) and its final result;
- The purpose of the medium (reuse, disposal, return to the supplier, etc.);
- The validation of the certificate (contact details of the person verifying the certificate, this person being different from the one who carried out the destruction).

246. The certificate must be retained and be produced on request. Although the Belgian Crossroads Bank for Social Security (BCSS) recommends a retention period of the certificate "of at least 2 years[105]", we consider it prudent to take into account the legal limitation periods[106]. These periods will generally be 5[107] or 10 years[108].

247. In fact, as long as the limitation period has not expired, a person or an organisation having suffered damage as a result of inadequate data sanitisation or insufficient destruction of a data medium, may apply to the courts and tribunals in order to obtain an order that the controller be ordered to pay compensation for the damage or even be subject to other sanctions.

---

[105] https://ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_erase_effacement_supports.pdf

[106] The limitation periods are detailed in Articles 2262bis et seq. of the Civil Code.

[107] Personal actions deriving from an extracontractual event: 5 years (Art. 2262 bis §1, al. 2 and 3 Civil Code)

[108] Personal actions deriving from the execution of a contract: 10 years (Art. 2262 bis §1, al. 1 Civil Code).

Appendix A: Recommended techniques for the main types of media

Magnetic media Floppy Disks	**Clear**	⇨ **Overwrite** (rewriting) the media using software approved by the organisation and then validate (verification). The Clear level must result in at least one write pass with a fixed data value (e.g.: all zeros). Optional: multiple write passes or more complex values can optionally be used.
	Purge	⇨ **Degaussing** of the medium using a degausser approved by the organisation (if necessary, refer to the list of devices approved by the NSA.
	Destroy	⇨ **Incineration** of the medium: the medium must be reduced to ashes. ⇨ **Shredding - Disintegration** (if necessary, refer to the list of devices approved by the NSA. The DIN standard recommends the following debris sizes for these levels: max. 2000 mm^2 for T2, max. 320 mm^2 for T3 , max. 160 mm^2 for T4, max. 30 mm^2 for T5, max. 10 mm^2 for T6 and max. 2.5 mm^2 for T7
Optical discs CD/DVD/BD	**Clear**	Not available.
	Purge	Not available.
	Destroy	⇨ **Grinding** (abrasion). Removal of layers containing information from the media using a commercial optical disc grinder. This technique is not suitable for DVDs and Blu-Ray (see par.173). ⇨ **Incineration** of the medium: the medium must be reduced to ashes. ⇨ **Shredding - Disintegration - Crushing** The NSA cites a maximum debris size of 2mm per side for DVDs and Blu-Ray and 5mm per side for CDs (see par.174) (if necessary, refer to the list of devices approved by the NSA. The DIN standard recommends the following debris sizes for these levels: max. 2000 mm^2,for O1, max. 800 mm^2 for O2, max. 160 mm^2 for O3, max. 30 mm^2 for O4, max. 10 mm^2 for O5, 5 mm^2 for O6 and max. 0.2 mm^2 for O7.

Magnetic media ATA Hard Drives	**Clear**	⇨ **Overwrite** (rewriting) the media using software approved by the organisation and then validate (verification). The Clear level must result in at least one write pass with a fixed data value (e.g.: all zeros). Optional: multiple write passes or more complex values can optionally be used.
	Purge	In order of preference: ⇨ **1. Sanitize Device command**: If supported, use one of the commands of the ATA Sanitize Device features (preferable to the Secure Erase command). One or both of the following options may be available: **1.a) Overwrite** (overwrite ext. command). Apply a write pass with a fixed data value (e.g.: all zeros). A single write pass should suffice to purge the media. Optional: instead of one write pass, use three write passes, using the invert option so that the second write pass is the inverted version of the specified model. **1.b) Cryptographic erase** (crypto scramble ext command). Optional: After cryptographic erasure is successfully applied, use the overwrite command to write a series of zeros or a pseudo-random pattern to the media. If this command is not supported, the Secure Erase or Clear procedure can also be applied after the cryptographic erase. ⇨ **2. Secure Erase command**: If supported, use the Secure Erase Unit command, in enhanced mode. ⇨ **3. Cryptographic erase** through the Opal security subsystem class (see par.132), if integrated commands are not available. Optional: After cryptographic erasure is successfully applied, use the overwrite command to write a series of zeros or a pseudo-random pattern to the media. If this command is not supported, the Secure Erase or Clear procedure can also be applied after the cryptographic erase. ⇨ **4. Degaussing** of the medium using a degausser approved by the organisation (if necessary, refer to the list of devices approved by the NSA. It is recommended to damage the hard drive by bending its internal platters before disposing of it.
	Destroy	⇨ **Incineration** of the medium: the medium must be reduced to ashes. The lining of the internal platters must be reduced to ash and/or the internal platters must be physically deformed by heat. ⇨ **Shredding - Disintegration** The NSA cites the maximum debris size of 2mm per side and recommends destruction in batches with other storage

		devices (if necessary, refer to the list of devices approved by the NSA). The DIN standard recommends a mechanically/electronically inoperable medium for the H1 level, a damaged medium for the H2 level and a deformed medium for the H3 level. It recommends the following debris sizes for these levels: 2000 mm^2 for H4, max. 320 mm^2 for H5, max. 10 mm^2 for H6 and max. 5 mm^2 for H7
Magnetic media SCSI Drives	**Clear**	⇨ **Overwrite** (rewriting) the media using software approved by the organisation and then validate (verification).
	Purge	⇨ **Sanitize command** (see Sanitize Device command for ATA Hard Drives) ⇨ **Degaussing** of the medium using a degausser approved by the organisation (if necessary, refer to the list of devices approved by the NSA. It is recommended to damage the hard drive by bending its internal platters before disposing of it.
	Destroy	⇨ **Incineration** of the medium: the medium must be reduced to ashes. The lining of the internal platters must be reduced to ash and/or the internal platters must be physically deformed by heat. ⇨ **Shredding - Disintegration** The NSA cites the maximum debris size of 2mm per side and recommends destruction in batches with other storage devices (if necessary, refer to the list of devices approved by the NSA). The DIN standard recommends a mechanically/electronically inoperable medium for the H1 level, a damaged medium for the H2 level and a deformed medium for the H3 level. It recommends the following debris sizes for these levels: 2000 mm^2 for H4, max. 320 mm^2 for H5, max. 10 mm^2 for H6 and max. 5 mm^2 for H7

Paper	**Clear**	Not available.
	Purge	Not available.
	Destroy	⇨ **Incineration** of the medium: the medium must be reduced to ashes. ⇨ **Shredding - Disintegration** For debris produced by shredders, the NIST recommends a size of max. 5 mm^2 and the use of a 2.4 mm sieve for the disintegrators (if necessary, refer to the list of disintegrators approved by the NSA and shredders approved by the NSA). The DIN standard recommends for level P1 a bandwidth of max. 12 mm and 6 mm for P2. It recommends the following debris sizes for these levels: max. 320 mm^2 for P3, max. 160 mm^2 for P4, max. 30 mm^2 for P5, max. 10 mm^2 for P6 and max. 5 mm^2 for P7.

Flash media - USB Removable Drives - Memory Cards - Solid State Drives	**Clear**	⇨ **Overwrite** (rewriting) the media using software approved by the organisation and then validate (verification). For ATA & SCSI Solid State Drives, USB Removable Media and Memory Cards: ⇨ **Overwrite** (rewriting) the media using software approved by the organisation and then validate (verification). The Clear level must result in at least one write pass with a fixed data value (e.g.: all zeros). Optional: multiple write passes or more complex values can optionally be used. For ATA Solid State Drives (only): ⇨ **Secure Erase command**: If supported, use the Secure Erase Unit command, in enhanced mode.
	Purge	A) ATA Solid State Drives ⇨ **1. Sanitize Device command**: If supported, use one of the commands of all the ATA Sanitize Device features (preferable to the Secure Erase command), One or both of the following options may be available: **1.a) Block Erase command** Optional: once the command is successfully applied, write binary 1s in the user-addressable area of the media, then perform a second block erase. **1.b) Cryptographic erase** (crypto scramble ext command). Optional: Once cryptographic erasure is successfully applied, use the block erase command. If this command is not supported, the Secure Erase or Clear procedure can also be applied after the cryptographic erase. ⇨ **2. Cryptographic erase** through the Opal security subsystem class (see par.132), if integrated commands are not available. Optional: Once cryptographic erasure is successfully applied, use the block erase command. If this command is not supported, the Secure Erase or Clear procedure can also be applied after the cryptographic erase. B) SCSI Solid State Drives ⇨ **1. Sanitize command**: If supported, use one of the commands of the SCSI Sanitize features. One or both of the following options may be available: **1.a) Block Erase command** **1.b) Cryptographic erase** (cryptographic erase command). Optional: Once cryptographic erasure is successfully applied, use the block erase command. If this command is not supported, the Secure Erase or Clear procedure can also be applied after the cryptographic erase.

		⇨ **2. Cryptographic erase** through the Opal security subsystem class (see par.132), if integrated commands are not available. Optional: Once cryptographic erasure is successfully applied, use the block erase command. If this command is not supported, the Secure Erase or Clear procedure can also be applied after the cryptographic erase. C) Removable USB media and Memory Cards - Not available Most of these media do not support the integrated commands, or if they are supported, the interfaces are not supported in a standardised manner.
	Destroy	⇨ **Incineration** of the medium: the medium must be reduced to ashes. ⇨ **Shredding - Disintegration** The NSA cites the maximum debris size of 2mm per side and recommends destruction in batches with other storage devices (if necessary, refer to the list of devices approved by the NSA). The DIN standard recommends the following debris sizes for these levels: max. 160 mm^2 for E3, max. 30 mm^2 for E4, max. 10 mm^2 for E5, 1 mm^2 for E6 and max. 0.5 mm^2 for P7.

Appendix B: Extracts from the GDPR

Article 5 : **Principles relating to processing of personal data**

1. Personal data shall be:

   a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

   b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

   c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

   d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

   e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

   f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality');

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 32 : **Security of processing**

1. 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 for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

   a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33 : **Notification of a personal data breach to the supervisory authority**

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) describe the likely consequences of the personal data breach;

d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34 : **Communication of a personal data breach to the data subject**

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

   a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

   b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

   c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Appendix C : References

Main references:

- "Guidelines for Media Sanitization" of the National Institute of Standards and Technology – NIST Special Publication 800-88 Revision 1:
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
  - https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization

- Publications of the US National Security Agency (NSA):
  - NSA/CSS Storage Device Sanitization Manual (12/2017)
  - NSA/CSS Evaluated Products List for Hard Disk Drive Destruction Devices (03/2020)
  - NSA/CSS Evaluated Products List for Magnetic Degaussers (03/2020)
  - NSA/CSS Evaluated Products List for Optical Destruction Devices (03/2020)
  - NSA/CSS Evaluated Products List for Paper Disintegrators (03/2020)
  - NSA/CSS Evaluated Products List for Paper Shredders (03/2020)
  - NSA/CSS Evaluated Product List for Punched Tape Disintegrators (03/2020)
  - NSA/CSS Evaluated Product List for Solid State Disintegrators (03/2020)

Other references:

- https://www.blancco.com/blog-many-overwriting-rounds-required-erase-hard-disk/
- https://cmrr.ucsd.edu/_files/data-sanitization-tutorial.pdf
("Tutorial on Disk Drive Data Sanitization" of the "Center for Magnetic Recording Research" (CMRR))
- https://dban.org/
- https://www.enterprisestorageforum.com/storage-hardware/flash-vs-ssd-storage-whats-the-difference.html
- https://eprint.iacr.org/2015/1002.pdf
- https://www.irs.gov/privacy-disclosure/media-sanitization-guidelines
(IRS "Media Sanitization Guidelines")
- https://www.killdisk.com/blog-gutmann-method.htm
- https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_data_data_securite.pdf
- https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_erase_effacement_supports.pdf
("Information security & privacy guideline relating to the deletion of electronic Social Security information media")
- https://www.seagate.com/files/staticfiles/support/docs/manual/Interface%20manuals/100293068j.pdf
- https://www.semshred.com/data-destruction-devices/paper-destruction/
- https://www.ssi.gouv.fr/rgs
- https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_Corps_du_texte.pdf
and its appendices B: https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf
- https://tinyapps.org/docs/wipe_drives_hdparm.html
- https://en.wikipedia.org/wiki/Data_remanence
- https://en.wikipedia.org/wiki/Flash_memory
- https://en.wikipedia.org/wiki/Hardware-based_full_disk_encryption
- https://en.wikipedia.org/wiki/Write_amplification