Autorité de protection des données

Recommandation relative aux techniques de nettoyage de données et de destruction de supports de données

AVERTISSEMENT : Le présent document a pour but de fournir des explications complémentaires aux règles en vigueur et ne soustrait pas le responsable du traitement à ses obligations et responsabilités issues tant du RGPD que d'autres textes applicables. Tenant compte de ses besoins et de l'analyse des risques qu'il effectue ou envisage, il lui appartient de faire le choix de recourir à l'un ou l'autre outil et méthode, en tenant notamment compte de l'évolution des connaissances et des techniques. Les différents outils et marques cités dans ce document le sont aux seules fins de fournir des exemples. L'Autorité ne se prononce en aucune façon quant à leur conformité avec le RGPD et autres règlementations ni quant à leurs qualités et performances.

TABLE DES MATIÈRES

Synthèse

L'Autorité de protection des données (APD) remplit de nombreuses missions, dont celle d'éclairer les citoyens, entreprises et acteurs publics quant à certaines questions en lien avec la protection des données. Parmi ces questions, celles liées à une élimination 'sécurisée' de données ou de supports de données sont assurément récurrentes.

Quelles que soient leurs motivations, les responsables du traitement souhaitent mener à bien cette opération mais manquent parfois d'une vision claire sur ce qui constitue un résultat satisfaisant (notamment sur le plan de la protection des données à caractère personnel) et sur la manière d'atteindre un tel résultat.

La rareté, au niveau international, des documents de référence sur le sujet, voir leur absence au niveau européen et national, conjuguée avec la volonté de l'APD de fournir aux parties intéressées un guide utile sous forme de lignes directrices claires, à jour et complètes, sont à l'origine de la présente recommandation.

Ce document présente les différentes techniques de « nettoyage » existantes (réécriture, effacement cryptographique, démagnétisation,...) pour différents types de supports (HD, SSD, papier,...) qui, soit rendent l'accès aux données impossible sur un support préservé (effacement sans possibilité de reconstitution et chiffrement), soit aboutissent à la destruction du support (sans possibilité de reconstruction).

La recommandation aborde aussi ce traitement (nettoyage et destruction) d'une manière plus large en détaillant ses différents aspects, tant légaux (notamment liés au RGPD) que techniques ou organisationnels et examine le traitement dès avant l'achat des supports jusqu'aux étapes de vérification et d'enregistrement des résultats.

Enfin, un tableau récapitulatif présente au lecteur, en fonction du type de support, les techniques de nettoyage et destruction recommandées permettant d'atteindre le niveau de confidentialité désiré.

Si les principes et concepts évoqués dans ce document sont par nature relativement pérennes, il est certains outils, méthodes ou exemples présentés qui, au vu de l'évolution des connaissances et des techniques dans le domaine, pourraient devoir être actualisés plus rapidement. Les paragraphes ou parties de texte potentiellement concernés sont précédés des caractères '\\' (double barres obliques inversées).

1. Introduction

01. Dans le cadre de ses activités, le responsable du traitement[1] rencontre de nombreuses situations dans lesquelles il souhaite s'assurer que le transfert de supports d'information vers un autre environnement n'entraîne pas une divulgation non autorisée des données contenues sur ces supports.

Ces situations dans lesquelles le responsable du traitement devra prendre une décision relative au « nettoyage[2] » de données sont souvent liées à la fin de leur cycle de vie ou à celle de leur support ou encore à leur réutilisation dans un contexte de sécurité[3] différent.

02. Citons par exemple :

- La mise au rebus de matériel informatique (au sens large[4]) déclassé ;
- L'envoi en réparation d'une photocopieuse ;
- L'évacuation des archives papier ;
- Le tri des dossiers du service RH ;
- La cession d'ordinateurs à une association caritative ;
- La restitution de PC dans le cadre d'un leasing ;
- La fin du contrat de location d'une imprimante multifonctions ;
- Ou encore la vente, après amortissement, des desktops et laptops de l'entreprise aux membres du personnel.

03. Les motivations du responsable du traitement peuvent être diverses, telles le besoin de protéger des données ayant une valeur particulière à ses yeux ou classées

---

[1] L'art.4.7 du RGPD définit le «responsable du traitement» comme la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

[2] L'expression anglaise « data sanitization » correspondant à ce traitement, recouvre la notion de nettoyage en profondeur (désinfection, assainissement) ne laissant pas de trace des données. Nous la traduirons simplement par « nettoyage » des données ou des supports de données. L'U.S. National Institute of Standards and Technology (NIST) définit « media sanitization » comme un terme général désignant les actions entreprises pour rendre irrécupérables les données écrites sur des supports par des moyens ordinaires et extraordinaires.

[3] Ce support va-t-il être donné ou vendu à une partie tierce ? Va-t-on s'en débarrasser ou bien le réutiliser en interne ? Si le support est réutilisé tel quel, le responsable du traitement doit s'assurer que le support sera utilisé dans un contexte de sécurité au moins équivalent au contexte dans lequel le support était utilisé précédemment (ex. : politique d'accès aux informations comparable à celle qui prévalait dans l'environnement initial du support, voir plus stricte).

[4] Tels des PC, serveurs, imprimantes contenant des disques durs, supports amovibles (clé USB, DVD, disque dur externe, etc.) ou des appareils mobiles (laptops, tablettes, Gsm, etc.).

'confidentiel', la volonté de se démarquer de la concurrence, la crainte d'une sanction[5] et/ou la volonté de se conformer à la législation en vigueur.

À cet égard, rappelons que le responsable du traitement est tenu, sous peine de sanction[6], au respect de l'article 5.1.e du RGPD qui prévoit que « les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ». Quand cette durée est dépassée, le responsable du traitement doit donc anonymiser ces données ou les détruire de manière définitive[7] (voir exceptions dans le même article).

04. Notons que, si la protection des données quittant leur environnement initial, est une préoccupation grandissante des organisations de tout type, c'est entre autres parce que leur protection au sein de celles-ci se renforce. Ainsi, une politique plus stricte de contrôle d'accès aux données, réduit la probabilité qu'une personne non autorisée puisse accéder directement à ces données. En conséquence, cette personne sera tenté de se tourner vers d'autres canaux d'accès aux informations, requérant moins d'efforts telle la récupération de données sur des supports qui quittent l'environnement contrôlé de l'organisation ou sont placés dans un environnement de niveau de confidentialité/sécurité inférieur.

05. Pour ce qui est de la législation en vigueur, nous retiendrons plus spécialement, dans le cadre du présent document, le règlement général européen sur la protection des données (RGPD[8]) et en particulier son article 32 (voir Annexe B) sur la sécurité du traitement et ses articles 33 et 34 (voir Annexe B) relatifs à la violation de données à caractère personnel. Notons également son article 5.1.f consacrant l'obligation de protection des données à caractère personnel contre notamment, leur traitement non

---

[5] Rappelons que le RGPD prévoit pour une violation des dispositions relatives aux obligations incombant au responsable du traitement / sous-traitant, dont notamment l'art.32 (sécurité), des amendes administratives pouvant s'élever jusqu'à 10 millions EUR ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu (art.83.4.a du RGPD).

Les amendes administratives les plus élevées à ce jour (11/2020) infligées en matière de sécurité au titre du RGPD se chiffrent déjà en millions d'euros. Ainsi l'Autorité de contrôle britannique (ICO), en accord avec les autres Autorités européennes de protection des données (en application du mécanisme de coopération prévu par le RGPD, appelé « guichet unique » ou « one-stop shop ») a imposé des amendes de près de 21 millions d'euros au groupe hôtelier Marriott et de près de 22 millions d'euros à la British Airways pour manquements à la sécurité (violation des art.5.1.f et 32 - voir Annexe B).

[6] Voir par exemple, la sanction de 160.000 euros imposée par l'autorité danoise à l'encontre d'une société de taxi ayant conservé plus de deux ans les coordonnée téléphoniques ayant effectué une réservation et la sanction (200000 euros) imposée par la même autorité à l'encontre d'un magasin de meubles pour avoir omis d'effacer des données clients lors d'un renouvellement du matériel informatique.

[7] Une organisation temporaire a besoin de récolter les données d'un certain nombre d'adhérents pour pouvoir déposer une pétition, lesquels adhérents doivent être authentifiés comme de vraies personnes. Après authentification, cette organisation, qui ne poursuit aucune autre finalité, ne doit conserver aucune donnée à caractère personnel et doit donc supprimer l'ensemble de celles-ci ainsi que les supports pétitions contenant ces dernières puisque seul le nombre de signataires validés est important (suppression suite à la réalisation des finalités).

[8] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE. Le RGPD est d'application depuis le 25 mai 2018.

autorisé et leur perte, et ce à l'aide de mesures techniques ou organisationnelles appropriées.

06. Rappelons que l'art.4.14 du RGPD définit la violation de données à caractère personnel, comme « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ».

07. Les responsables du traitement et les sous-traitants[9], tenus de se conformer à ses obligations légales devront, en conséquence, prendre les mesures techniques et organisationnelles adéquates, afin de garantir la confidentialité des données à caractère personnel[10] présentes sur les supports d'information qu'ils souhaitent nettoyer.

08. L'Autorité de protection des données (APD), chargée de veiller au respect des principes fondamentaux de la protection des données à caractère personnel, dont les principes de sécurité et de confidentialité[11] sont des éléments essentiels, vise par le biais du présent document à aider responsables de traitement et sous-traitants à respecter ces principes.

09. Pour ce faire, ce document présente différentes techniques de « nettoyage » qui soit, rendent l'accès aux données impossible sur un support préservé (effacement sans possibilité de reconstitution et chiffrement), soit aboutissent à la destruction du support (sans possibilité de reconstruction).

10. Le responsable du traitement fera son choix dans cet éventail de techniques en prenant notamment en compte, le type de support, son affectation ultérieure et le niveau de confidentialité des données.

Limitations

11. Seules les techniques menant à un « nettoyage » de l'intégralité du support ou à sa destruction sont abordées dans ce document. L'effacement spécifique de fichiers, répertoires ou partitions n'est donc pas traité.

---

[9] L'art.4.8 du RGPD définit le «sous-traitant» comme la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

[10] L'art.4.1 du RGPD définit les «données à caractère personnel» comme toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

[11] Le responsable du traitement et le sous-traitant doivent garantir la sécurité et la confidentialité des informations qu'ils traitent. Ils doivent en particulier veiller à ce que seules les personnes autorisées aient accès à ces informations.

12. Ne sont pas abordés dans le présent document :

- Les cas où l'accès aux supports/données, en vue d'un effacement ou d'une destruction, n'est pas possible tels le stockage dans le cloud ou le matériel provenant d'un contrat PCaaS[12]. Il appartient au responsable du traitement, avant de choisir son fournisseur cloud ou autre fournisseur de stockage distant, d'examiner quel service il propose pour supprimer les données en toute sécurité ;

- La suppression de données contenues dans les véhicules (données de navigation, données issues de la synchronisation des contacts avec le gsm, ...) à l'occasion d'une réparation chez le garagiste ou d'une fin de contrat de leasing par exemple ;

- La suppression de données sur mobiles via logiciels spécifiques ou gestion centralisée (ex. : Active Directory). Apple met en ligne une procédure de suppression des données personnelles pour l'iPhone et l'iPad[13], ainsi que Google pour les appareils Android[14] ;

- La restauration des paramètres d'usine. Le responsable du traitement veillera cependant à ce que la mémoire non volatile ne contienne plus de données à caractère personnel[15] ;

- L'emploi d'images, créées par un logiciel[16] de capture d'image et de déploiement d'image du système d'exploitation, pour la réinstallation d'appareils.

Public visé

13. Ce document est destiné aux responsables de traitement et aux sous-traitants[17] (qu'ils appartiennent au secteur public ou au secteur privé), à leurs conseillers en

---

[12] « Personal Computer as a Service », connu aussi sous le nom de « Device as a Service » : modèle de gestion du cycle de vie des appareils dans lequel une organisation paie un abonnement mensuel à un fournisseur, pour louer le matériel et les services de gestion associés.

Ex : Description de l'offre PCaaS de Dell https://www.delltechnologies.com/en-us/services/pc-as-a-service.htm et de leur service optionnel PCaaS Data Sanitization https://www.dell.com/learn/us/en/uscorp1/legal~service-descriptions~en/documents~pcaas-data-sanitization-sd-en.pdf

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

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

[15] Cette fonction ramène l'appareil à l'état dans lequel il était à sa sortie de l'usine (en général, équivalent à l'état au moment de l'achat de l'appareil). Elle concerne surtout la mémoire non volatile (ne s'efface pas en l'absence de courant) intégrée sur les cartes et les périphériques. Ainsi, la gestion à distance intégrée dans une carte mère peut contenir des adresses IP, des noms d'utilisateur, des mots de passe ou des certificats. Par conséquent, pour l'effacement, il peut être nécessaire d'interagir avec plusieurs interfaces pour réinitialiser complètement l'état de l'appareil. Cela peut inclure l'interface BIOS/UEFI[38] ainsi que l'interface de gestion à distance.

[16] Un logiciel de déploiement d'images capture une image du système d'exploitation installé sur un appareil et la déploie sur des appareils semblables (pc, serveurs, mobiles,...).

[17] Aux termes de l'art.32 du RGPD, tant le responsable de traitement que le sous-traitant met en œuvre les mesures techniques et organisationnelles appropriées permettant de garantir la confidentialité constante des systèmes et des services de traitement. Le présent document pourra être intéressant pour un sous-traitant souhaitant offrir ses services à un responsable de traitement.

sécurité de l'information et délégués à la protection des données (data protection officer ou DPO en anglais) ou à toute autre personne et organisation qui doit ou souhaite rendre l'accès à des données à caractère personnel impossible.

Objectifs

14. Le présent document vise à :

- Aider le public visé à formaliser et intégrer les différentes étapes permettant de choisir, en connaissance de cause, une technique appropriée de « nettoyage » ;

- Fournir une information sur les différentes méthodes et techniques disponibles, leurs niveaux de confidentialité et les résultats qui peuvent être attendus en fonction du type de support concerné.

- Aider le public visé à se conformer à certaines exigences du RGPD dont celles relatives à l'accountability (principe de responsabilité défini à l'article 5.2 du RGPD) et celles destinées à empêcher la divulgation non autorisée des données.

2. Principes et concepts préalables

15. Le 'nettoyage' ou la destruction d'un support de données[18] sera :

- Autorisé (selon une procédure interne et/ou la loi applicable) ;
- Approprié (irréversible, conforme à l'analyse des risques et aux exigences de sécurité/confidentialité qui en découlent) ;
- Supervisé par le responsable du traitement (en cas de sous-traitance, voir section 3.1.3. pour les mesures additionnelles à prendre) ;
- Documenté (preuve de destruction, voir 6e partie) ;
- Et exécuté au moment opportun (tenir compte des délais légaux, des problèmes liés au stockage d'attente).

2.1. Inventaire et classification des informations

16. Afin de pouvoir déterminer quelle méthode sera utilisée pour atténuer au mieux les risques d'une divulgation non autorisée des données, le responsable du traitement doit connaître :

2.1.1. La nature et les catégories de données présentes sur le support

17. Il doit, pour le moins, savoir si des données à caractère personnel sont présentes ou non et dans l'affirmative, il pourra aussi utilement vouloir :

- Identifier, parmi ces données, celles qui sont dites « sensibles » (appartenant à une catégorie particulière[19]) ou relatives à des condamnations pénales ou à des infractions (article 10 du RGPD) ;
- Distinguer les données qui sont chiffrées[20], et/ou pseudonymisées[21] ;

---

[18] Notons que nous utilisons de manière indiscriminée les termes « information » ou « donnée », ne sachant pas si le support contient les premières ou les deuxièmes ou les deux. Les données sont des données brutes, utilisées pour obtenir des informations après analyse. L'information est interprétée et donne un sens aux données. Ainsi la donnée '21122021' devient une information si l'on sait que c'est une date (21 décembre 2021).

[19] L'art.9.1 du RGPD fait l'inventaire de ces catégories particulières de données à caractère personnel. Il s'agit des données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, les données génétiques, les données biométriques traitées afin d'identifier une personne physique de manière unique, les données concernant la santé et les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

[20] Des données chiffrées sont des données qui ont été rendues incompréhensibles pour les personnes ne disposant pas de la clé de déchiffrement appropriée.

[21] L'art.4.5 du RGPD définit la pseudonymisation » comme le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et

- Classer les données selon le risque que représenterait, pour la personne concernée, une divulgation non autorisée de tout ou partie des données à caractère personnel contenues sur le support. Il est préférable lors de l'estimation du risque, d'envisager une divulgation d'ensemble de toutes les données contenues sur un support ou dans un appareil, ce qui correspond souvent à la réalité du terrain. Par exemple, quand un serveur de bases de données est piraté, ce sont en général toutes les bases qui sont accédées simultanément.

18. En effet, la procédure mise en place par le responsable du traitement, afin de déterminer la méthode de « nettoyage » appropriée, pourra reposer en tout ou partie, sur les informations développées au par. 17.

19. Nous rappellerons ici que des données anonymisées[22] ne répondent plus à la définition de donnée à caractère personnel dans la mesure où elles ne peuvent plus être reliées à une personne physique identifiée ou identifiable.

20. La nature et les catégories de données doivent être associées, selon une politique validée par le responsable du traitement, à une technique permettant d'atteindre le niveau de confidentialité requis (clear, purge ou destroy – voir section 3.1.2.).

21. Il est donc nécessaire de disposer d'un inventaire et d'une classification des informations[23].

2.1.2. La nature et les caractéristiques du support

22. Il existe de très nombreux types (disques durs, SSD, bandes magnétiques, disquettes, IPhones, cartes SD, microfilms, …) et classes (optique, électronique, magnétique, non-réinscriptible, papier, …) de supports.

23. Il est logique que les caractéristiques techniques et physiques très différentes de ces supports d'information aient une influence sur le choix de la méthode de 'nettoyage'. Toutes les techniques ne sont d'ailleurs pas disponibles pour tous les types et classes de support. Pensons par exemple à la démagnétisation pour un support papier ou la réécriture pour un support non-réinscriptible.

24. La classification des données et la nature du support sont les principaux critères utilisés pour déterminer le traitement des supports et la méthode qui sera employée. Pour effectuer ce choix, la classification servira de premier filtre, dans la mesure où

---

organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable

[22] Extrait du considérant 26 du RGPD : […] Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. […]

[23] L'inventaire des actifs et la classification des informations font partie intégrante d'un système de gestion de l'information. Ainsi la mesure 8.2.1 (Gestion des actifs) de l'ISO 27002 classe les informations en termes de valeur, de sensibilité à une divulgation ou modification, d'exigences légales ou de leur caractère critique. NB : la mesure 6.5.2.1 de l'ISO 27701 (additional implementation guidance for 8.2.1 of ISO 27002), pourtant dédié aux données à caractère personnel, n'apporte quant à elle que peu de précision sur une classification spécifique.

elle fournit des informations sur le niveau de sensibilité/confidentialité des données et sur le risque pour les personnes concernées en cas de divulgation non autorisée. Les considérations basées sur le type et la classe du support seront utilisées dans un deuxième temps.

25. D'autres facteurs additionnels peuvent être pris en compte tels le coût, l'impact environnemental, l'affectation ultérieure[3] ou la durée du processus.

2.2. Étapes du traitement

26. Synthétiquement, les étapes principales des opérations de 'nettoyage' et destruction pourront être les suivantes :

A. Politique (sécurité et confidentialité)

27. La première étape consiste à rédiger un document, validé par la direction, englobant toute la problématique 'data sanitization' et en y incluant tous les supports de données existants dans l'organisation. Ce document devra notamment décrire le contexte, les buts à atteindre, la procédure d'autorisation de 'nettoyage' ou destruction (y compris pour les back-ups) et les différentes étapes du traitement. Il décrira également de manière détaillée les responsabilités des intervenants (et de la direction) quant à l'exécution mais aussi le contrôle des différentes étapes du traitement (chaîne de responsabilité). Il est important que chaque étape, sans exception, soit placée sous la responsabilité d'une personne dûment désignée (voir ex. par.240).

28. La responsabilité des intervenants s'étend au-delà de la procédure proprement dite de nettoyage/destruction. Il peut être utile de déterminer, qui serait responsable des atteintes à la réputation, et les éventuelles sanctions si, à un stade ultérieur, il s'avérait que certains supports de données n'aient pas été traités selon la procédure validée.

29. Les rédacteurs du document s'assureront du support top-down, plein et entier, de la hiérarchie. Dans des domaines contraignants, tels que la sécurité et la confidentialité, le support de la direction est indispensable, sous peine de voir ces politiques n'être que du papier dont le contenu n'est pas appliqué. Il faut s'assurer que la responsabilité du 'nettoyage' des supports soit confiée à un membre de l'organisation doté d'un niveau d'autorité approprié.

30. Le ou les responsables de la mise en œuvre s'assureront également que la politique est connue de tous les acteurs qui y ont un rôle[24], qu'elle est correctement

---

[24] https://www.realwire.com/releases/More-than-half-of-enterprises-fail-to-communicate-data-sanitization-policies: Bien que 96% des dirigeants des organisations consultées disposent d'une politique de désinfection des données, 31% doivent encore la communiquer à l'ensemble de l'entreprise. 20 % des répondants ne pensent pas non plus que les politiques de leur organisation soient terminées. Dans l'ensemble, 56% n'ont pas mis en place de politique de nettoyage des données qui soit régulièrement communiquée efficacement à l'ensemble de l'entreprise, ce qui augmente les risques de violations potentielles des données.

exécutée dans la pratique et mise à jour si nécessaire[25]. Il est important que cette exécution des instructions et leurs résultats soient aussi contrôlés.

31. Un rapport[26] de la société Blancco montre que les écarts entre la création, la communication et l'exécution de la politique de nettoyage des supports mettent en danger les données sensibles. L'étude identifie les risques suivants :

- Ne pas assumer la responsabilité directe de l'effacement des actifs informatiques ;
- Laisser le matériel croupir dans les zones de stockage sans l'avoir sécurisé ;
- Effacement hors site sans visibilité complète de la chaîne de contrôle ;
- Désignation peu claire des propriétaires des politiques de nettoyage des données.

B. Inventaire

32. Rédiger un inventaire complet de tous les équipements que vous avez marqués devoir faire l'objet d'un 'nettoyage' ou d'une destruction. Déterminez le ou les types de supports concernés. Si ce n'est déjà fait, procédez à un inventaire des données contenues sur les supports d'information à traiter afin de les trier selon une classification pertinente, à savoir ;

- en fonction du type de données à caractère personnel qui s'y trouvent,
- et de si leur divulgation représenterait un haut risque pour les droits et libertés des personnes concernées (comme c'est à priori le cas des données de catégories particulières énumérées à l'article 9 du RGPD).

33. Si le responsable du traitement ne connait pas le contenu du support d'information (support endommagé ou de technologie obsolète, manque de temps ou de personnel, etc.), il traitera ce support comme s'il contenait des données personnelles dont la divulgation représenterait un haut risque pour les droits et libertés des personnes concernées.

34. Nous rappellerons par ailleurs que le RGPD impose aux responsables de traitement de tenir un registre des activités de traitement (de données à caractère personnel) qui comporte notamment une description des catégories de données à caractère personnel traitées (article 30.1.c).

---

[25] Comme toutes les autres politiques, celle-ci doit faire partie d'un cycle englobant une étape de mise à jour. Les raisons pour lesquelles une mise à jour serait nécessaire peuvent être nombreuses. Pensons à un changement du contexte de sécurité/confidentialité au sein de l'organisation ou à une évolution technique (par exemple, force de coercivité d'un dégausseur à adapter en fonction de l'évolution des supports, voir 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/

35. Si le responsable du traitement désire faire de ce document un outil de conformité plus large qu'un simple registre, il pourra utilement inclure des informations telles la nature du support utilisé pour le traitement, la technique de destruction ou de nettoyage et son déclencheur (remplacement ou obsolescence du matériel, départ du collègue, finalité remplie, délais légaux atteints ...).

C. Analyse des risques

36. Il s'agit principalement de déterminer quel est le risque encouru si une personne non autorisée accédait à une donnée à caractère personnel contenue sur le support d'information, ce qui constitue une violation de données et une infraction aux art.5.1.f et 32.2 du RGPD (voir Annexe B). Prenez également en considération les éventuelles failles de sécurité associées à chaque technique[27].

37. Il est important de noter que la préoccupation du RGPD (et de l'APD) porte sur l'impact de la divulgation de données

- « à caractère personnel » (et non pas de l'ensemble des données de l'organisation),
- sur la personne concernée (c.-à-d. la personne à qui la donnée est relative) et non pas sur l'organisation.

38. Si l'analyse des risques est une étape indispensable, le responsable du traitement, aidé de son éventuel Délégué à la protection des données, pourra aussi utilement procéder à une « analyse d'impact relative à la protection des données » (AIPD, article 35 du RGPD[28]), qu'elle soit obligatoire ou pas.

- L'AIPD aidera le responsable du traitement à se poser les bonnes questions ;
- Elle contiendra des informations utiles au remplissage du registre des traitements (article 30 du RGPD) ;
- Elle aidera à respecter l'obligation de protection des données dès la conception (article 25 du RGPD - data protection by design). Étant donné que l'AIPD sert, également avant le traitement, à identifier les mesures à prendre pour faire face aux risques pour les droits et libertés des personnes concernées, l'AIPD peut apporter à cet égard une aide précieuse.

39. Si l'AIPD vient à indiquer que le traitement présentait encore un risque élevé, après que le responsable du traitement eût pris des mesures pour atténuer les risques

---

[27] Recherchez sur Internet si des vulnérabilités sont associées à la technique ou l'outil sélectionné. Vous pouvez, à titre d'exemple, consulter la liste CVE (Common Vulnerabilities and Exposures) qui recense le plus grand nombre de vulnérabilités de cybersécurité connues du public. Autres sources d'intérêt : Exploit Database, U.S. National Vulnerability Database (NVD) du NIST, packet storm.

[28] Voir aussi la Recommandation d'initiative concernant l'analyse d'impact relative à la protection des données et la consultation préalable (CO-AR-2018-001) de l'ex-Commission de la protection de la vie privée. (https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2018.pdf)

identifiés, le responsable du traitement doit consulter l'Autorité de protection des données préalablement à la mise en place du traitement (article 36 du RGPD).

D. Mesures de sécurité

40. L'étape suivante consiste à mettre en place les mesures techniques et organisationnelles qui permettent de réduire les éventuels risques identifiés à un niveau acceptable (pour l'organisation et pour les personnes concernées).

41. Cette étape inclut également l'identification des actions qui pourraient être entreprises, rapidement et efficacement, pour répondre à une éventuelle violation de données. Si des données personnelles venaient à être compromises pendant le 'nettoyage' des supports ou même après avoir quitté votre organisation, vous pourriez toujours être tenu responsable de la violation (vous restez responsable du traitement jusqu'à la fin du cycle de vie des données).

E. Évaluation

42. Il convient ensuite d'évaluer dans quelle mesure, les actions entreprises ont atteint l'objectif fixé (prévenir la perte de confidentialité). Le cas échéant, choisir une autre technique.

F. Documentation

43. Les différentes étapes doivent faire l'objet d'une documentation détaillée. Le principe d'accountability du RGPD (principe de responsabilité défini à l'article 5.2) implique en effet que le responsable du traitement soit à même de démonter son respect des règles relatives à la protection des données. Seront notamment documentées : la justification[29] de la méthode choisie, la description des mesures prises (étapes de la méthode, vérification inclue) et la preuve de leur bonne exécution (par exemple via l'émission d'un document reprenant toutes les informations liées au 'nettoyage' ou à la destruction du support et, après une étape de vérification, le résultat, échec ou succès).

44. Afin de renforcer sa transparence vis-à-vis des personnes concernées, nous recommandons au responsable du traitement de communiquer, en sus des informations dont la communication est obligatoire aux termes des articles 13, 14 et 15 du RGPD, certaines informations additionnelles. Ainsi, en complément de la durée de conservation des données (articles 13.2.a, 14.2.a et 15.1.d), il pourra, sans effort, à l'aide de la documentation dont il disposera déjà, les informer plus concrètement de ce qu'il adviendra de leurs données, une fois cette durée dépassée.

[29] La justification pourra reposer sur une mise en balance des intérêts du responsable du traitement avec les droits et intérêts de la personne concernée et/ou une évaluation du risque inhérent au traitement en tenant compte de l'état des connaissances et des coûts de mise en œuvre par rapport aux risques et la nature des données personnelles à protéger.

45. De même, nous recommanderons au responsable du traitement d'adopter la même attitude transparente, dans le cadre de sa communication avec la personne concernée relative à l'article 17 du RGPD (droit à l'effacement).

G. Exemple

46. Voici un exemple plus concret illustrant les principales étapes d'un projet de nettoyage de données et/ou de destruction du support :

1. Vous envisagez de remplacer certains ordinateurs de votre organisation et de vendre ceux-ci à une entreprise qui procédera à leur reconditionnement avant de les revendre.

2. Vous avez déterminé lors de la phase d'inventaire que les supports contenus dans les pc étaient des disques durs de type ATA d'une capacité de 500GB et contenaient les dossiers RH du personnel et que ces dossiers incluaient des catégories particulières de données à caractère personnel (données sensibles telles l'appartenance syndicale ou liées aux absences pour cause de maladie).

3. Selon votre politique de sécurité/confidentialité, les données à caractère personnel doivent rester en permanence sous votre contrôle, aucune donnée ne peut donc quitter le périmètre physique et/ou logique de votre entreprise.

4. Dans l'analyse des risques, vous comparez les différentes méthodes rencontrant cet objectif (effacement, stockage, destruction).

5. Vous estimez au vu de la nature des données, du temps nécessaire à l'effacement des disques durs, de la possibilité que certaines données restent accessibles, de la faible valeur de revente des pc, que le risque pour l'organisation (ex.: réputation, financier, procédure judiciaire,...) et le risque pour les droits et libertés des personnes concernées (ex.: vol d'identité, arnaque, hameçonnage, chantage, discrimination, ...) ne valent pas la peine d'être pris.

6. En conséquence, afin de ramener le risque à un niveau acceptable, vous optez pour la destruction physique des supports et prenez les mesures suivantes :

   A. Que la destruction soit faite au sein de l'organisation ou par un partenaire externe, vous nommez les responsables intervenant dans le projet : le responsable opérationnel sera un membre du service informatique tandis que la supervision globale sera assurée par le DPO qui donnera à la fin de la procédure son avis positif (ou pas), sachant qu'une décision finale, qu'elle concerne le choix de la méthode de nettoyage, le niveau de confidentialité atteint, ou encore l'accord pour libérer/transférer les supports revient toujours au responsable du traitement (la direction de votre organisation). Cette ou ces décisions pourront utilement être référencées dans le registre des activités de traitement ;

   B. Vous décidez que la destruction devra être effectuée dans l'enceinte de l'organisation, en présence du responsable de projet ;

C. Vous choisissez[30] un partenaire externe spécialisé, offrant des garanties de qualité et de respect de la confidentialité, qui peut à l'aide d'un matériel mobile, mettre en œuvre la technique que vous avez sélectionnée. Vous vérifiez avec le prestataire que les caractéristiques techniques du matériel utilisé (ex. taille maximum des résidus de destruction) répondent aux exigences de votre politique de sécurité/confidentialité.

7. Vous vérifiez que la destruction s'est bien déroulée selon la procédure établie et que les données ne sont effectivement plus exploitables. Vous collectez et conservez les preuves de la destruction effective des supports (pour l'ensemble ou propre à chaque support) ainsi que toutes les informations utiles à la démonstration de votre conformité aux obligations légales.

2.3. Dans le meilleur des mondes

47. Dans un monde parfait, vous aurez déjà réfléchi à l'étape 'nettoyage sécurisé' de vos supports, dès avant leur acquisition et interrogé le fournisseur de ces supports à ce sujet. Pour les organisations devant rédiger un cahier des charges, celui-ci pourra inclure des spécifications relatives aux commandes d'effacement intégrées au matériel (si applicables - voir articles 3.2.1.2. et 3.2.4.1.) et imposer l'assistance du fournisseur et la fourniture de certaines informations y liées (ex : temps d'exécution, description des commandes supportées et de leurs options ou encore zones exclues). Ceci devra faciliter le choix informé d'un support de stockage ou d'un appareil comportant un support de stockage, sur base des possibilités d'effacement sécurisé offertes par le produit.

48. De même, récolter toutes les informations techniques nécessaires au moment de l'acquisition, facilitera non seulement l'étape 'inventaire' du traitement mais aussi l'étape 'analyse des risques' où vous aurez à comparer les différentes techniques d'effacement disponibles en fonction des caractéristiques du support.

49. Par exemple, en connaissant la coercivité[31] d'un support magnétique, on pourra inclure ou écarter la démagnétisation (voir section 3.2.3.) de la liste des techniques disponibles. Ou encore, en ayant bien noté que deux types différents de disques (durs/magnétiques et SSD/électroniques) sont présents dans les ordinateurs de l'organisation, le responsable opérationnel saura qu'il faut les distinguer au moment du choix de la méthode de 'nettoyage'. \\ Il est à noter que les deux types de disques peuvent être présent simultanément dans les appareils (les disques SSD étant beaucoup plus rapides mais plus chers, ils sont souvent utilisés pour le démarrage de l'ordinateur et couplés avec un disque dur magnétique plus lent mais qui se charge de stocker la plus grande partie des données).

---

[30] Rappelons ici que le responsable du traitement à une responsabilité et des obligations dans le choix du sous-traitant (art.28 du RGPD). La notoriété du fournisseur ne constitue pas une assurance suffisante. Le contrat écrit, obligatoire entre le responsable du traitement et le sous-traitant, aidera à garantir qu'un niveau de sécurité approprié est en place et mentionnera le plus précisément possible la méthode choisie, ses caractéristiques et les moyens à mettre en œuvre.

[31] Dans ce cadre, la coercivité désigne, en termes non savants, la force qui est nécessaire à un champ magnétique pour modifier des données stockées sur un support magnétique. Au plus elle est haute, au plus il sera difficile de modifier ('effacer') les données en utilisant une technique de démagnétisation.

3. Les différentes méthodes et techniques

3.1. Introduction

3.1.1. Précisions importantes

50. Faisons d'entrée de jeu une remarque importante, en précisant que le simple effacement (en appuyant sur la touche 'delete'/'suppr.' de votre clavier par ex.) de fichiers ou de répertoires via l'interface de votre appareil n'efface que les pointeurs vers ces fichiers et pas les données elles-mêmes. En effaçant les pointeurs, l'appareil rend la zone où se trouvaient les fichiers, à nouveau disponible pour l'écriture d'autres données. Par analogie, c'est comme si pour effacer le chapitre d'un livre, vous supprimiez dans la table des matières toute référence au dit chapitre. En parcourant le livre, vous pourrez donc retrouver le contenu du chapitre.

51. C'est pourquoi cette action, qui n'aboutit à aucun réel effacement, n'est pas commentée dans ce document.

52. Précisons encore que le formatage n'efface pas non plus les données, qu'il soit rapide (quick) ou standard (full)[32].

3.1.2. Trois niveaux de confidentialité

53. Dans la littérature spécialisée, les différentes techniques sont souvent classées en fonction du niveau de confidentialité (sécurité) désiré ou, autrement dit, de la probabilité de récupération des données initiales. On distingue trois niveaux de confidentialité associés à trois classes de techniques : clear (nettoyer), purge (purger) et destroy (détruire).

- Les techniques de niveau « clear » visent à empêcher une récupération des données effectuée à l'aide d'un logiciel. Elles offrent une confidentialité modérée (certaines données pourront être récupérées si l'on dispose du temps, des connaissances et des compétences nécessaires). Il s'agit de techniques purement logiques[33].

  Exemples : la réécriture (partielle) à l'aide de commandes standards (read and write) et la réinitialisation de l'appareil ou du support (état 'sortie usine' - souvent conseillé pour les appareils mobiles et les routeurs/commutateurs).

- Les techniques de niveau « purge » visent à empêcher une récupération des données effectuée à l'aide de techniques de laboratoire avancées. Elles offrent un niveau de confidentialité plus élevé et sont appropriées quand le support est destiné à être réutilisé dans un contexte de sécurité/confidentialité différent du contexte initial. Il s'agit de techniques logiques et physiques.

  Exemples : la réécriture à l'aide de commandes dédiées, la démagnétisation et l'effacement cryptographique (voir section 3.2.4.).

---

[32] La différence entre les deux tenant principalement au fait qu'un full format vérifiera tous les 'bad sectors' (secteurs défectueux), ce qui explique la longueur de l'opération par rapport à un quick format.

[33] Le terme 'logique' fait référence à une technique dont la réalisation des mécanismes se fait via un logiciel.

- Les techniques de type « destroy » offrent le niveau le plus élevé de confidentialité/sécurité. La récupération des données est en effet impossible, même à l'aide de techniques de laboratoire de pointe. Elles reposent sur la destruction physique et sont donc incompatibles avec une réutilisation du support. Notons qu'une technique rendant le support inutilisable, n'atteindra pas le niveau destroy si certaines données restent néanmoins récupérables.

  Exemples : l'incinération, le déchiquetage et le broyage.

54. Les différentes techniques présentées dans ce document ressortent toutes de l'une de ces trois classes. Le lecteur trouvera en Annexe A, un tableau reprenant les types de supports d'information les plus courants[34], associés aux différentes techniques qui peuvent leur être appliquées en fonction du niveau de confidentialité/sécurité requis (clear, purge et destroy).

55. Le niveau de confidentialité à atteindre puis le choix d'une technique permettant d'atteindre ce même niveau et ce en fonction du type de support, repose sur une analyse des risques préalable.

Techniques disponibles en fonction du niveau de confidentialité désiré		
Clear	Purge	Destroy
• Réécriture (commandes standard) • Réinitialisation (restauration des paramètres d'usine voir par.12)	• Réécriture (commandes dédiées/intégrées) • Démagnétisation • Effacement cryptographique	• Incinération • Déchiquetage • Broyage • Désintégration • Démagnétisation

56. Nous scinderons en deux groupes les méthodes utilisées, selon qu'elles débouchent sur une destruction physique du support d'information ou non.

3.1.3. Traitement non supervisé par le responsable du traitement

57. Lorsque la destruction ou le 'nettoyage' du support est sous-traité ou partiellement sous-traité et n'est donc pas effectué sous le contrôle de bout en bout du responsable du traitement, ce dernier devra obtenir des assurances quant au bon déroulement des différentes étapes du traitement. Pour y parvenir, nous préconiserons les mesures suivantes :

- L'utilisation de témoins oculaires (validés par le prestataire et/ou le responsable du traitement) ;

- Le transport des supports dans des véhicules sécurisés et verrouillés. Bien que la protection apportée par les sceaux de sécurité ne soit pas absolue[35] (elle pourra

[34] Pour une liste plus complète de supports, le lecteur pourra consulter l'Annexe A du « Guidelines for Media Sanitization » du "NIST Special Publication 800-88".

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

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

éventuellement être défaite par des attaquants entrainés et équipés), les véhicules pourront en être utilement pourvus ;

- La prise de photographies ou l'utilisation d'autres techniques de documentation à chaque étape du traitement ;

- La mise en place d'un processus continu sans arrêt impliquant un stockage temporaire ;

- Des procédures de contrôle et de sélection du personnel participant au traitement ;

- La délivrance d'un certificat de destruction par le sous-traitant (voir 6e partie).

58. Il est conseillé d'inclure ces mesures dans le contrat liant le responsable du traitement et le sous-traitant et d'y décrire, le cas échéant, les éléments constitutifs de la preuve de destruction (notamment la méthode utilisée et le résultat obtenu). À ce sujet, le lecteur pourra s'inspirer des clauses reprises dans un document[36] des services gouvernementaux du Nouveau Brunswick (Canada).

3.2. Le support de données est conservé

59. En préambule aux différentes techniques exposées dans ce chapitre, il est important de noter qu'en-dehors d'une méthode de destruction ne laissant aucune partie du support intacte (quelle que soit la nature du support, papier, magnétique ou autre), il est difficile de garantir que plus aucune donnée ne sera exploitable sur l'entièreté de la surface du support, y compris par des laboratoires spécialisés.

60. Si le risque que des données subsistent sur le support ou qu'elles puissent être reconstituées n'est pas acceptable pour le responsable du traitement (en tenant compte du risque pour les personnes concernées), une méthode aboutissant à la destruction du support sera préférée (voir chapitre 3.3.).

3.2.1. Effacement - réécriture (overwriting)

61. L'« effacement » (on parle aussi d'écrasement ou de réécriture) consiste à écrire, au même endroit que celui où se trouvent les données déjà présentes sur un support d'information, une ou plusieurs séries d'éléments d'information, déterminés, aléatoires ou les deux (selon le protocole choisi), afin de réduire la possibilité de pouvoir récupérer les données ainsi recouvertes (ou 'écrasées').

62. Il serait donc plus approprié de parler de méthode de « réécriture » que de méthode d'effacement[37] car l'information initiale ou des parties de cette information sont toujours potentiellement présentes sur le support, en fonction de l'efficacité de cette réécriture.

---

[36] Destruction sécuritaire des documents : Directives - annexe C, p.15 - Clauses contractuelles types sur la destruction sécuritaire des documents

[37] Notons que le terme « effacement » est régulièrement utilisé dans la littérature sur le sujet ou dans la description des logiciels utilisés pour la suppression sécurisée d'informations digitales.

63. La réécriture n'est évidemment pas applicable aux supports nativement non-(ré-)inscriptibles ou ne supportant plus l'écriture suite à un dommage (panne, destruction partielle, usure).

64. Cette méthode peut déboucher sur deux niveaux de confidentialité, à savoir 'clear' et 'purge'. Le niveau atteint sera fonction de la combinaison du type de support contenant les données, du logiciel utilisé (lié au hardware ou indépendant) et des commandes associées (standards ou dédiées). Le choix et la bonne utilisation du logiciel et des commandes dépendront eux-mêmes du niveau de connaissance informatique de la personne en charge de la procédure.

65. Les disques, qu'ils soient magnétiques (voir point 3.2.1.1.a) ou électroniques (voir point 3.2.1.1.b) comportent différentes zones. Certaines de ces zones sont à priori inaccessibles aux logiciels indépendants du hardware, au système d'exploitation ou au BIOS/UEFI[38], ce qui rend impossible le nettoyage de l'entièreté des zones de stockage du support.

66. \\ Parmi ces zones à priori inaccessibles, on trouve :

- Les secteurs 'Bad/unmapped/corrupted'
- L'espace 'over-provisioned'
- Les cellules 'trimmed'
- La 'Device Configuration Overlay' (DCO)
- La 'Host Protected Area' (HPA)
- La 'Garbage Collection' (GC)

3.2.1.1. Niveau 'clear' - Logiciels tiers

A. Disques durs magnétiques

67. \\ Le niveau 'clear' peut être atteint pour les disques durs (internes et externes) et les disquettes en utilisant des logiciels[39] tiers, indépendants du matériel, tels BitRaser, Blancco Drive Erasure, PartedMagic, Active@KillDisk ou encore le projet open source DBAN. Ces logiciels proposent souvent un large éventail de protocoles différents (jusqu'à plusieurs dizaines) parmi lesquels l'utilisateur non-averti, aura du mal à choisir.

---

[38] Le BIOS (Basic Input Output System) est un micrologiciel (firmware) stocké sur une puce mémoire et utilisé pour effectuer l'initialisation du matériel pendant le processus de démarrage et pour fournir des services d'exécution pour les systèmes d'exploitation et les programmes. Il est non volatile, ce qui signifie que ses paramètres sont enregistrés et récupérables même après la mise hors tension de l'appareil. Quant à l'UEFI, c'est essentiellement une version améliorée du BIOS.

[39] Cherchez dans votre moteur de recherche habituel (l'APD utilise actuellement startpage.com), les termes « data erasing » ou « data sanitization » pour trouver des informations sur les logiciels payants ou freewares offrant ce type de fonction.

68. Dans ce qui différencie ces différents protocoles on trouve d'une part, le nombre d'écrasements, c'est-à-dire le nombre de passes de réécritures successives que subira la surface du disque et d'autre part, la dernière étape du protocole, à savoir le contrôle de l'effet des passes de réécriture.

69. À titre d'exemple, le protocole DoD 5220.22-M, très souvent utilisé et présent sur tous les logiciels phare du marché, préconise l'écriture sur tous les espaces adressables du support, d'un caractère binaire (en l'occurrence 0), puis de son complément (1) et enfin d'un caractère binaire aléatoire (0/1). La vérification du résultat constitue la dernière étape[40] du protocole.

70. La version de ce protocole « d'effacement », toujours perçu comme un véritable standard et qui est livré dans la plupart des logiciels tiers, correspond à une version obsolète d'une norme du Département de la Défense américain (DoD) [41]. La triple réécriture du disque imposée par cette ancienne version du protocole est plus que suffisante pour empêcher la récupération des données par des logiciels disponibles dans le commerce (niveau 'clear'). Si l'efficacité des protocoles d'effacement semble logiquement et à priori liée au nombre de passes de réécriture que l'ensemble des zones du disque aura subie, cette logique est cependant dépassée.

71. En effet, depuis quelques années, un consensus se dégage (NIST, HMG British Standard, BSI-GS, CMRR[42]) pour affirmer que, suite à l'évolution technologique des supports (notamment liée à l'augmentation de leur densité donc de leur capacité), le nombre de passes de réécriture peut être réduit à 1, sans néanmoins augmenter la possibilité de récupérer les données sur le disque à partir de solutions logiques. Une passe de vérification doit cependant être impérativement exécutée.

72. Si une passe d'écriture et une passe de vérification sont suffisantes (hormis pour du matériel ancien datant d'avant 2000 ou d'âge inconnu), on peut donc, à fortiori, en conclure qu'un protocole proposant 3 passes de réécriture et une de vérification finale ou une vérification après chaque passe d'écriture (telle l'ancienne version du très populaire DoD 5220.22-M), est également suffisant.

73. \\ Par contre, bien qu'ils ne soient pas sensu stricto déconseillés, les protocoles proposant un nombre de passes plus élevé qu'une passe d'écriture et une passe de vérification peuvent être qualifiés, dans l'état actuel de nos connaissances et des techniques utilisées, d'inutiles[43].

---

[40] Dans la littérature, on parle plutôt de passe. Ainsi DoD 5220.22-M est un protocole en 4 passes, 3 consacrées à l'écriture (effacement/écrasement) et une à la vérification.

[41] Pour être précis, la version actuelle de ce protocole ne spécifie plus ces étapes et c'est donc à une version plus ancienne du protocole que ces logiciels font référence. Pour plus d'information : https://www.blancco.com/blog-dod-5220-22-m-wiping-standard-method/

[42] Extrait du "Tutorial on Disk Drive Data Sanitization" (p.8) du 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."

[43] Le protocole Gutmann (1996), réminiscence d'un passé révolu où les techniques employées pour l'écriture sur les disques durs permettaient théoriquement à des laboratoires spécialisés de retrouver des données écrasées, correspond à pas moins de 35 passes de réécriture plus une passe de vérification. Les disques durs actuels ont rendu ce protocole, par ailleurs très gourmand en ressources, totalement

74. Lorsqu'il s'agira de choisir un logiciel, préférez un logiciel qui a fait l'objet d'une analyse par un laboratoire indépendant et/ou qui répond aux exigences des agences gouvernementales spécialisées.

75. \\ Voici à titre d'exemples quelques liens vers des acteurs procédant à l'évaluation de produits ou services dans le domaine de la destruction de données :

- 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. Supports à mémoire flash

76. À la différence des disques et disquettes (voir point précédent 3.2.1.1.a), qui sont des supports de type magnétique, la mémoire flash est un support de type électronique. Cette mémoire, non volatile (elle ne s'efface pas en l'absence de courant, au contraire de la RAM par exemple) peut être effacée et reprogrammée électriquement.

77. Grâce notamment à des prix en baisse, d'excellentes performances et l'absence de pannes mécaniques, la mémoire flash est apparue au fil du temps comme une technologie de stockage d'information de plus en plus présente dans les appareils électroniques et les supports d'information. On peut donc en trouver dans les téléphones portables, ordinateurs, appareils photo numériques, clés USB, cartes mémoire, SSD (voir ci-après), calculatrices, appareils médicaux, jouets Hi-Tech, etc…

78. \\ En ce qui concerne plus spécifiquement les supports d'information, nous pouvons distinguer deux grandes familles d'appareils[44] contenant de la mémoire flash :

- les cartes mémoires dont il existe de très nombreux types (ex : Secure Digital SD, SDHC, SDXC, micro et mini SD, xD card, CompactFlash ou encore

---

obsolète*. Il figure cependant toujours dans la liste des protocoles offerts par les principaux logiciels du marché.

*Pour les spécialistes : ce protocole est devenu obsolète en même temps que l'apparition des disques haute-densité (à grande capacité) et que la technologie des disques durs est passée de la technique de codage MFM/RLL à des techniques PRML vers la fin des années 90.

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

MemoryStick). Elles sont destinées aux petits matériels tels que les appareils photo numériques ou les téléphones portables ;

- les disques SSD ou solid-state drives, que l'on peut traduire par disque statiques, disques à semi-conducteurs ou simplement disques électroniques. Ils sont disponibles dans de très nombreux formats et interfaces (PCIe, SATA, USB, etc…). Par extension de langage, tout type de support ne comportant pas de pièces 'en mouvement' (au contraire des disques durs magnétiques rotatifs par exemple) est parfois appelé SSD (RAM, ROM, Smard Cards, Flash).

NB : Depuis plusieurs années, les SSD sont tous basés sur de la mémoire flash (d'où la confusion entre les deux termes) mais cela n'a pas toujours été le cas (RAM) et cela pourrait à nouveau changer dans le futur.

Solid-State Drives (SSD) de type ATA ou SCSI

79. Nous avons vu que certaines zones des disques durs 'traditionnels' (voir point 3.2.1.1.a) sont inaccessibles aux logiciels tiers. Il faut souligner que pour la mémoire flash, une particularité technologique (voir par.81 et 82) liée à ce type de support vient accentuer ce problème d'accès.

80. C'est pourquoi, même si l'emploi de logiciels indépendants pour les disques 'électroniques' pourrait permettre d'atteindre le niveau de confidentialité 'clear' via une passe de réécriture (à fortiori via plusieurs), l'utilisation seule de ces logiciels tiers sera considérée comme non suffisante pour atteindre l'objectif recherché.

81. À titre d'information, la particularité technologique mentionnée au par.79 tient au fait que toute écriture sur ce type de support entraîne son usure. Ses composants ne sont donc garantis, par le constructeur, que pendant un nombre fini de cycles d'écriture/effacement (program/erase cycle ou p/e cycle). \\ Afin de prolonger la durée de vie des mémoires flash et éviter toute usure prématurée des cellules de certains blocs[45] par rapport à d'autres[46], les constructeurs ont mis au point des stratégies telles la répartition d'usure[47] (wear-leveling), des systèmes de fichiers dédiés ou l'affectation exclusive d'espaces de stockage au contrôleur SSD (overprovisioning)[48].

---

[45] Les mémoires flash sont découpées en blocs qui sont constituées de pages, elles-mêmes composées de cellules mémoire. L'écriture et la lecture se font à l'échelle de la page. Cependant, avant de pouvoir réécrire au même endroit, il faut réinitialiser (effacer) les cellules mémoire, ce qui ne se fait que par bloc entier (constitué en général de plusieurs centaines de pages). Il faudra donc copier le bloc entier à un autre endroit, effacer le bloc d'origine, puis écrire le contenu de l'ancien bloc avec les nouvelles pages.

[46] En l'occurrence, éviter l'usure prématurée des blocs qui sont souvent effacés par rapport à ceux qui stockent des données qui ne sont pas ou peu modifiées.

[47] Le principe est de copier sur les cellules déjà usées, des données qui ne sont jamais ou rarement modifiées et ce afin de répartir plus uniformément le nombre d'effacements/écritures par cellule (et donc l'usure).

[48] L'emploi de ces techniques et l'absence de pièce mécanique permettent néanmoins aux disques SSD actuels d'obtenir des garanties équivalentes aux disques durs.

82. L'emploi de ces techniques a donc pour conséquence la copie de mêmes données en de multiples endroits, dont des zones auxquelles les logiciels indépendants n'ont pas accès (exemples : bad blocks ou wear-leveling blocks).

Les clés USB

83. Connues sous de nombreux autres noms[49] et dont la mémoire flash est de moins bonne qualité que celle des SSD, elles rencontrent, tout comme les cartes mémoires[50] destinées aux petits matériels (ex. : appareils photo numériques et téléphones portables), les mêmes limitations au niveau 'clear' que les disques SSD.

C. Points d'attention

84. Rappelons que dans le cadre de la réécriture des supports par des logiciels tiers (niveau 'clear') :

- Le niveau de confidentialité atteint ne dépasse pas le niveau 'clear' ;
- Ces logiciels n'ont, à priori, pas accès à toutes les zones d'écriture du support ;
- Pour les supports à mémoire flash, la création de copies de blocs de données augmente les possibilités de récupération après effacement.

85. C'est pourquoi, en fonction du risque (principalement encouru par les personnes concernées), il peut être nécessaire de coupler l'effacement avec une autre technique telle que le chiffrement (voir par.126) ou la destruction physique (voir chapitre 3.2).

3.2.1.2. Niveau 'purge' - Commandes intégrées

86. Les supports de stockage ont, selon les modèles, des interfaces différentes (ATA, SCSI, NVMe). Ces interfaces, utilisées pour communiquer entre les systèmes hôtes et les périphériques de stockage, possèdent selon leur type, un ensemble différent de commandes pour nettoyer le support.

A. Disques durs magnétiques IDE/ATA

87. La plupart des disques durs[51] modernes de type IDE/ATA[52] (PATA[53], SATA[53], eSATA, … inclus) sont livrés avec les commandes de type « Secure Erase » (généralisé

---

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

[50] Liste des types de cartes : https://fr.wikipedia.org/wiki/Mémoire_flash#Types_de_cartes

[51] À distinguer des ATA SSD (solid-state drives).

[52] IDE est une interface standard, connue aussi sous l'acronyme ATA, permettant de relier des périphériques de stockage (disques durs, lecteurs CD/DVD,…) à la carte mère d'un PC. Même si le nom IDE est souvent utilisé de manière interchangeable avec ATA, IDE se réfère en fait uniquement aux spécifications électriques des signaux sur le câble de disque à 40/80 broches. ATA est le nom correct de la spécification entière.

[53] Quand SATA (Serial AT Attachment), la nouvelle norme ATA pour la transmission de donnée est apparue, les anciennes formes bien connues d'ATA ont été renommées rétroactivement PATA (Parallel ATA).

depuis 2001 pour les disques de plus 15GB). Secure Erase est le nom donné à un ensemble de commandes stockées dans et disponibles à partir du firmware[54] du disque.

88. Ces commandes intégrées[55], effacent (écrasent) toutes les données contenues sur un disque (y compris sur les secteurs marqués comme défectueux ou inaccessibles) et permettent d'atteindre un niveau de confidentialité 'purge'.

89. \\ Un logiciel tiers se distingue de ceux abordés à l'article 3.2.1.1. : HDDerase. Développé par le CMRR[42], cet utilitaire incorpore en effet la commande Secure Erase et peut donc atteindre certaines zones de stockage inaccessibles aux logiciels tiers traditionnels.

90. \\ Notons également sous Linux, le programme en ligne de commande 'hdparm' (NB: les programmes GParted et Parted Magic incluent tous deux hdparm).

Commandes ATA - précisions

91. Nous avons parlé jusqu'ici de la « commande » 'Secure Erase'. C'est le terme le plus fréquemment utilisé dans la littérature mais il l'est régulièrement de manière peu précise.

92. En effet, parmi les commandes du standard ATA, il faut plutôt parler de la commande 'Security Erase Unit' et c'est cette commande qui se décline en deux modes, à savoir le mode standard 'Secure Erase' ou 'Normal Erase' et le mode appelé 'Enhanced Secure Erase' ou 'Enhanced Erase'.

93. Le mode 'enhanced', qui cible "les secteurs qui ne sont plus utilisés en raison d'une réaffectation, n'est pas pris en charge par tous les supports ATA.

94. Bien que leur nom soit similaire, ces deux modes présentent des différences. Lorsque le mode d'effacement normal est sélectionné, la commande 'Security Erase Unit' écrit des zéros (en binaire) dans toutes les zones où des données ont été écrites par l'utilisateur.

95. Lorsque le mode d'effacement amélioré (enhanced) est sélectionné, la commande 'Security Erase Unit' écrit des données selon des schémas prédéfinis et réécrit également les secteurs du disque qui ne sont plus utilisés ou marqués inaccessibles pour l'utilisateur. L'implémentation de ce mode est optionnelle et n'est pas supporté par tous les constructeurs. Cependant, s'il est disponible, il sera préféré au mode standard.

---

[54] Le firmware ou micrologiciel est un logiciel intégré au matériel, qui fournit les instructions nécessaires au fonctionnement de ce même matériel.

[55] On ne peut pas exécuter ces commandes (commandes de micrologiciel) sur un disque dur comme on exécute, par exemple, des commandes dans Windows à partir de l'invite de commandes. Pour exécuter les commandes Secure Erase, il faudra utiliser un programme qui donne un accès direct (I/O) à l'interface ATA du disque dur et qui permet d'envoyer des commandes ATA à ce même lecteur. Même dans ce cas, l'utilisateur n'exécutera souvent pas la commande manuellement.

96. Du point de vue de la spécification ATA, ce sont deux commandes différentes et il est parfois difficile de savoir laquelle est implémentée par les constructeurs. De la même manière, si un support dit implémenter les deux commandes, il est possible qu'il associe les deux à une seule action/version.

97. Plus récemment, une autre commande ATA, 'Sanitize Device', a fait son apparition. Également optionnelle, elle n'est donc pas implémentée sur tous les supports. Tout comme la commande équivalente pour les interfaces SCSI et NVMe[56] ('sanitize', voir par.103), elle est composée des trois modes crypto scramble, block erase et overwrite, ce dernier, tentant de nettoyer toutes les zones de données utilisateur, y compris les blocs défectueux, de rechange et non alloués.

- Overwrite[57] permet à l'utilisateur de spécifier la ou les passes de réécriture qu'il veut appliquer (ex. : 3 passes, la 2e utilisant l'option 'invert'[57] et la 3e étant identique à la 1e)

- Crypto scramble lance l'effacement cryptographique qui modifie/supprime les clefs de chiffrement du support (voir section 3.2.4.) :

- Block erase est utilisé pour effacer les supports à mémoire flash.

98. Le logiciel en ligne de commande 'hdparm', déjà mentionné, intègre depuis 2016 (v.9.49) le jeu de fonctionnalités 'Sanitize Device'. Il offre une alternative aux utilisateurs méfiants qui préfèreraient ne pas se reposer sur les utilitaires des fabricants (et leur implémentation de qualité variable) pour 'nettoyer' leur supports.

99. Par ordre de préférence, lorsqu'elles sont supportées par le support de données, il sera donc préférable d'utiliser la commande 'sanitize' device', puis le mode 'Enhanced Secure Erase' et enfin le mode 'Secure Erase' (les deux modes de la commande Security Erase Unit').

Secure Erase - confusion

100. Tant certains appareils de destruction des supports d'information (voir chapitre 3.3), que certains logiciels de 'nettoyage', comportent les mots 'secure erase' (effacement sécurisé) dans leur nom ou annoncent qu'ils effacent en toute sécurité les données d'un disque dur ('it securely erases data').

101. Cependant, à moins que ces appareils et logiciels ne précisent, spécifiquement, qu'ils utilisent le mode 'Secure Erase' de la commande ATA 'Security Erase Unit', il est probable que ce ne soit pas le cas. En d'autres termes, bien que beaucoup de techniques d'effacement des données puissent être considérées comme 'sécurisées' par rapport à un *simple 'delete'*, toutes n'incluent pas la commande 'ATA Secure Erase

[56] La commande 'Sanitize' pour l'interface NVMe a également les trois modes, block erase, crypto erase et overwrite.

[57] Le mode 'overwrite ext' remplit la zone de données utilisateur avec un modèle de quatre octets. Les paramètres de ce mode incluent un nombre de réécritures multiples et la possibilité d'inverser le modèle à quatre octets entre des passes de réécriture consécutives (paramètre 'Invert').

Unit', qui seule permet d'atteindre le niveau de confidentialité 'purge' et donc d'aboutir à un effacement effectivement sécurisé.

102. Le cas échéant, au moment de choisir son logiciel, le lecteur sera attentif à ce point. \\ À titre d'exemples, citons le logiciel 'Secure Eraser' et la commande en ligne 'SDelete'[58] (Secure Delete), qui peuvent sembler prendre en charge Secure Erase, mais n'en font rien. Rappelons que des programmes comme HDDErase (voir par.89) ou hdparm (voir par.90) sont des exemples de programmes gratuits qui utilisent Secure Erase.

B. Disques durs magnétiques SCSI

103. La plupart des disques durs[59] de type SCSI[60] (interfaces Parallel SCSI, Serial Attached SCSI, Fibre Channel, USB Attached Storage et SCSI Express inclus[61]) supportent (sont fournies avec) la commande 'sanitize'[62].

104. À l'instar de la commande équivalente pour les interfaces ATA et NVMe, la commande 'sanitize', avec l'option 'overwrite', effectue une ou plusieurs passes de réécriture sur toutes les zones adressables[63] du disque et permet d'atteindre le niveau de confidentialité 'purge'. Les deux autres options ('block erase' et 'cryptographic erase') sont également semblables à celles des interfaces ATA et NVMe.

C. Remarques communes aux disques durs ATA et SCSI

105. Le résultat de ces commandes dédiées, issues du gestionnaire de disque[64] lui-même, est à priori plus fiable[65] que l'utilisation d'un logiciel tiers (voir article 3.2.1.1.) car le fabricant a une connaissance parfaite de son matériel et ces commandes prennent

---

[58] SDelete fait partie de la suite d'outils d'administration et de dépannage 'sysinternals' pour Windows. Extrait de la documentation des outils 'sysinternals' : "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] À distinguer des SCSI SSD (solid-state drives).

[60] SCSI (Small Computer System Interface) est un ensemble de standards décrivant la connexion physique et le transfert de données entre des ordinateurs et des périphériques. Les standards SCSI définissent des commandes, des protocoles, des interfaces électriques, optiques et logiques.

[61] Certaines interfaces ne respectent pas l'ensemble des standards SCSI mais implémentent néanmoins le protocole de commandes SCSI.

[62] Pour une description complète des commandes SCSI : https://www.t10.org - SCSI Block Commands (T10/BSR INCITS 506 - Rev.22 15/09/2020)

[63] Zone recevant une adresse unique (identifiant son emplacement sur le support) afin d'être accessible en lecture/écriture (secteur).

[64] Outil permettant d'effectuer les tâches usuelles d'administration des disques telles le formatage, la gestion des partitions (création, suppression, dimensionnement…), changer la lettre d'un lecteur, etc…

[65] Il semble que dans certains cas (dont il est difficile d'évaluer la fréquence) et du moins pour les interfaces ATA, ces commandes ne soient pas ou n'aient pas toujours été correctement implémentées par certains constructeurs. http://www.hddoracle.com/viewtopic.php?f=56&t=1412.

en compte l'ensemble des zones inscriptibles[66] du support qui sont invisibles pour le système d'exploitation et le BIOS/UEFI. Cette technique est aussi plus rapide que les logiciels tiers. Par ailleurs, les commandes intégrées sont aussi moins sensibles aux attaques de logiciels malveillants que les logiciels tiers.

106. Sachant que certaines implémentations problématiques de la commande 'sanitize' ont été signalées[65], que l'effacement se fasse via un logiciel tiers ou via une commande intégrée, il y aura toujours lieu de vérifier la bonne exécution des instructions[67], c'est-à-dire que la commande a débouché sur l'effacement attendu.

D. Solid State Drives (SSD)

107. Comme pour les disques durs magnétiques, la plupart des fabricants fournissent généralement des logiciels à utiliser avec leurs supports SSD (interfaces ATA, SCSI et NVM Express) dont notamment un outil de mise à jour du firmware[54], les commandes d'effacement sécurisé[68] et éventuellement un outil de clonage du support.

108. \\ À titre d'exemples, le lecteur trouvera ci-dessous les liens vers les outils SSD de quelques fournisseurs bien connus :

- Samsung Magician (secure erase est disponible dans la section Data Management)
- Western Digital SSD Dashboard (secure erase et sanitize sont disponibles dans la section Drive Management)
- Seagate : SeaTools SSD GUI (avec interface graphique - secure erase est disponible dans la section Operations - Maintenance - Erase) et SeaTools SSD CLI (sans interface graphique - la commande sanitize fournit les options block-erase et overwrite)
- Lenovo ThinkPad Drive Erase Utility : Cet utilitaire réinitialise la clé cryptographique des disques durs (HDD) pris en charge (Full Disk Encryption - FDE, voir article 3.2.4.2.) et efface le disque SSD (Solid State Drive).

109. Le site web du constructeur est le premier endroit où chercher un outil d'effacement sécurisé adapté. Cependant, ces outils ne permettent pas toujours l'exécution des commandes intégrées ou s'ils le permettent, la qualité du résultat de leur exécution est incertaine.

---

[66] La plupart des disques durs supportent la création d'espaces de stockage cachés qui ne sont pas connus du système d'exploitation ou du BIOS. Citons 2 exemples : la Host Protected Area (HPA) et le Device Configuration Overlay (DCO). https://site.aleratec.com/blog/2011/03/31/remember-hpa-dco-sanitizing-hard-drives/

[67] Les logiciels tiers permettent généralement d'inclure une passe de vérification, l'option la plus sûre restant l'emploi d'un logiciel spécialisé, de type data recovery tool ou disk editor.

[68] En pratique, quand la commande secure erase est exécutée, le contrôleur SSD applique simultanément une tension électrique à toutes les cellules de stockage et les réinitialise (libération des électrons stockés). La commande n'écrit donc rien sur le support.

110. Donc, au vu des caractéristiques des SSD et de ce qui précède, il sera indiqué, afin d'atteindre un niveau de sécurité/confidentialité suffisant, d'exécuter un 'nettoyage' additionnel selon une technique différente[69].

3.2.2. Anonymisation

111. \\ Une anonymisation, rendant impossible la ré-identification des personnes concernées, est au fur et à mesure, que l'accès à des bases de données de plus en plus grandes et en ligne s'intensifie, de moins en moins possible à assurer.

112. \\ C'est pourquoi, cette technique ne sera pas considérée comme présentant un niveau de confidentialité/sécurité suffisant. Et ce, indépendamment des ressources (temps et homme) nécessaires à son exécution, qui diminuent encore son intérêt par rapport aux autres techniques.

113. Si l'anonymisation a déjà été réalisée, il faudra, avant tout transfert d'un support d'information, avoir examiné la validité de la méthode employée et avoir, de préférence, réalisé un essai de ré-identification mené de préférence par du personnel indépendant de celui qui a procédé à l'anonymisation (qui se justifiera d'autant plus que les quantités de données sur le support seront grandes).

114. Enfin, n'oublions pas que modifier les données contenues sur un support (valeurs dans une base de données par exemple), ne les supprime pas nécessairement pour autant du support (pas d'écrasement des données).

3.2.3. Démagnétisation - dégaussage (degaussing)

115. La démagnétisation consiste à appliquer une force magnétique d'une puissance suffisante pour effacer toutes les données d'un support magnétique particulier. L'efficacité de cette technique est liée à l'intensité relative de la force magnétique offerte par l'appareil de démagnétisation et aux propriétés magnétiques du support de données.

116. Bien qu'elle soit une technique d'importance pour nettoyer les supports magnétiques, le lecteur pourra déduire de ce qui précède que la démagnétisation n'est pas efficace, vu leur nature, sur la plupart des dispositifs de mémoire flash, y compris les disques SSD donc. En effet, ils utilisent des circuits intégrés pour stocker les données au lieu de les stocker magnétiquement. Elle ne sera pas utilisée non plus sur des supports d'information mixtes constitués d'au moins un support non magnétique non volatile.

117. Ceci nous rappelle la nécessité d'une inventorisation correcte des supports, avec mention de leur type et de la méthode de nettoyage associée, car si l'on ne prend pas soin de distinguer les disques SSD des disques durs lors de la démagnétisation, les données stockées sur les SSD seront laissées intactes.

118. N'oublions pas que certains appareils peuvent intégrer les deux types de support (électronique et magnétique). Si la démagnétisation est envisagée pour ces

[69] En l'occurrence pour ATA, on fera suivre un block erase par un overwrite et cryptographic erase par un secure erase. Pour SCSI, on exécutera un sanitize-block erase après un cryptographic erase et enfin pour NVM Express, on lancera la commande user data erase après un cryptographic erase.

périphériques hybrides, on prendra soin d'également appliquer une technique de nettoyage adaptée au support de stockage électronique.

119. L'inventaire idéal (voir chapitre 2.3.) devra mentionner la force de démagnétisation nécessaire au 'nettoyage' du support, c'est-à-dire sa coercivité[31]. En effet, la coercivité peut être difficile à déterminer sur base uniquement des informations présentes sur l'étiquette du produit. Par conséquent, avoir consulté préalablement le fabricant de l'appareil pour obtenir ces informations peut s'avérer utile.

120. Il est important de vérifier systématiquement que la puissance adéquate est appliquée sur les supports (trop forte, le support risque d'être rendu inutilisable, et trop faible, les données risquent de ne pas être correctement 'nettoyées') et ce, d'autant que la puissance nécessaire évolue en même temps que la technologie. En effet, la coercivité des supports augmente en même temps que leur densité/capacité[70]. Les supports plus récents et de plus grande capacité nécessitent donc des dégausseurs plus puissants.

121. Selon l'intensité du dégaussage, le support peut-être rendu inutilisable. Dans ce cas, la démagnétisation devient également une technique de destruction (voir section 3.3.5.). Dans le même ordre d'idées, la démagnétisation pourra aussi être envisagée dans le cas d'un support endommagé et qui ne peut donc plus être 'nettoyé' par une méthode nécessitant le fonctionnement du support.

122. Les dégausseurs ne fonctionnant pas tous de la même manière, il faudra s'assurer que les opérateurs qui en font usage connaissent leurs modes de fonctionnement spécifiques. Ainsi, certains appareils ne requièrent qu'une seule passe tandis que d'autres exigent des passes multiples, de même certains modèles nécessitent que les supports d'information soient démontés et d'autres pas.

123. À titre informatif, la NSA publie une liste actualisée de dégausseurs permettant de 'nettoyer' de manière sûre bandes et disques durs magnétiques. Les appareils répertoriés dans ce document[71] sont listés face à la coercivité du périphérique de stockage qu'ils peuvent effacer en toute sécurité.

3.2.4. L'effacement cryptographique (cryptographic erase - crypto-erase - CE)

124. C'est la dernière des techniques de « nettoyage » préservant le support qui est présentée car, bien qu'étant une technique à part entière, elle est souvent utilisée en complément d'autres.

---

[70] Afin d'augmenter la densité de stockage magnétique, la surface affectée à chaque bit doit être réduite. Pour cela, il faut utiliser des matériaux magnétiques à coercivité accrue pour éviter que les informations ne s'effacent du fait des interactions avec des bits proches. Ceci rend l'enregistrement des bits plus difficile, car il nécessite un champ magnétique plus élevé. Ce qui explique aussi qu'avec l'augmentation des capacités, il devient plus difficile de démagnétiser (la puissance nécessaire augmente) les supports concernés.

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

125. Le but des méthodes présentées dans ce document est, in fine, de rendre définitivement inaccessibles les données contenues sur un support. Le chiffrement[72] de celles-ci peut, de prime abord, également atteindre cet objectif en rendant ces données incompréhensibles à tout qui n'a pas accès à la clef de déchiffrement. C'est cette étape supplémentaire, c'est-à-dire la destruction définitive de la clé permettant le déchiffrement, qui constitue la différence entre le chiffrement et l'effacement cryptographique et permet à cette technique d'être une technique de « nettoyage ».

126. Le chiffrement est bien sûr très utile dans de nombreux autres cas de figure liés à la protection des données. C'est en effet, une mesure phare pour contrer une perte de confidentialité, en cas de vol, d'accès non autorisé ou de perte du support. Le chiffrement est d'ailleurs cité dans le RGPD[73], comme un moyen potentiel d'atténuer les risques pour les personnes concernées, et dispensant dans certains cas de la communication d'une violation de données aux personnes concernées (art.34.3.a du RGPD)[74]. Mais ceci n'entre pas dans le cadre de l'analyse faisant l'objet du présent document.

3.2.4.1. Commandes intégrées

127. Tant les groupes de commandes ATA/IDE (option 'crypto scramble') que SCSI (option 'cryptographic erase') abordées à l'article 3.2.1.2., comprennent des commandes spécifiques activant l'effacement cryptographique des données situées sur le support. Elles ne sont cependant pas implémentées sur tous les supports de tous les constructeurs.

128. Si cette technique est utilisée, le NIST (guidelines SP.880-88r1) recommande de procéder ensuite à une réécriture du support, soit via les autres commandes intégrées, soit à l'aide d'un logiciel tiers (voir article 3.2.1.1.). Ceci afin de diminuer le risque potentiel engendré par une clé de déchiffrement encore présente et accessible sur le support suite à une destruction inefficace ou absente.

129. NB : nous avons vu (par.92) que 2 commandes ATA distinctes, portant un nom similaire, existaient et présentaient des différences pour des opérations de réécriture (Secure Erase et Enhanced Secure Erase). Quand elles sont employées pour le

---

[72] Le chiffrement d'un support d'information repose le plus souvent sur une clé d'authentification et une clé de chiffrement des données. La clé de chiffrement est la clé avec laquelle les données sont effectivement chiffrées et déchiffrées. La clé d'authentification repose sur le mot de passe ou la passphrase de l'utilisateur et sert à déchiffrer la clé de chiffrement des données (qui à son tour déchiffre les données). Avec cette approche à deux niveaux, l'utilisateur peut donc modifier son mot de passe sans que cela nécessite de chiffrer à nouveau toutes ses données, car la clé de chiffrement reste inchangée (elle sera à re-chiffrée à l'aide du nouveau mot de passe de l'utilisateur).

[73] Le chiffrement est cité aux art.6§4.e (licéité), art.32§1.a (sécurité) et art.34§3.a (communication à la personne concernée) du RGPD.

[74] Article 34.3.a du RGPD : « La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie: a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement; »

chiffrement du support, que l'une ou l'autre soit utilisée, elles donneront le même résultat.

3.2.4.2. SEDs

130. Bon nombre de supports d'information contiennent des mécanismes intégrés d'« auto-chiffrement ». Ils sont qualifiés, dans leur ensemble, de "hardware-based full disk encryption" (FDE) et plus particulièrement de « self-encrypting devices » (SEDs[75]), lorsqu'il s'agit de disques durs ou de solid state drives (SSD). L'auto-chiffrement implique que toutes les données écrites sur le support soient chiffrées par le support avant leur écriture et déchiffrées par le support au moment de leur lecture[76]. La clé de chiffrement n'est connue que du support mais elle peut néanmoins être changée par un utilisateur autorisé. Si la clef est modifiée, toute donnée préalablement écrite avec la clef initiale devient indéchiffrable. Le changement de clé peut donc servir à 'détruire' les données en les rendant irrécupérables (indéchiffrables).

131. La technique de l'effacement cryptographique est donc facile et surtout rapide à exécuter sur les SEDs puisque la phase de chiffrement a déjà été effectuée.

132. Les SEDs qui respectent le standard OPAL[77] du Trusted Computing Group[78] utilisent l'algorithme de chiffrement AES[79] (Advanced Encryption Standard) avec des clés de 128 ou 256 bits. Pour ces supports, l'effacement cryptographique est appelé « PSID Revert » car il nécessite, avant le lancement de la commande proprement dite et l'effacement des clefs, l'introduction d'un identifiant unique propre à chaque support : le PSID[80] ou Physical Security ID.

3.2.4.3. Failles de sécurité des SEDs

133. \\ Un autre point d'attention réside dans la publication d'une étude mettant en lumière une faille de sécurité dans le mécanisme intégré d'« auto-chiffrement » des SSD et permettant de contourner ce chiffrement pour peu que l'on ait accès physiquement au support d'information.

---

[75] À titre d'exemple, voici le lien vers le guide technique détaillé (EN) relatif à l'implémentation de la sécurité et au chiffrement complet des modèles SED de la marque Seagate :

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

[76] Dans la pratique, pour les supports FDE, les données sont toujours chiffrées (via la clé de chiffrement des données) lorsqu'elles sont stockées sur le support, même s'il n'y a pas de mot de passe défini (dans le cas, par exemple, d'un nouveau disque ou d'un utilisateur qui ne désire pas mettre de mot de passe).

[77] Ensemble de spécifications pour les lecteurs à auto-chiffrement développé par le TCG visant à protéger la confidentialité des données stockées.

[78] Le TCG est un groupement d'entreprises créé pour développer et promouvoir les standards et technologies de l'informatique de confiance (trusted computing) qui doit permettre aux fabricants de matériel d'avoir le contrôle sur ce qui peut fonctionner sur leurs systèmes et refuser l'exécution de logiciels non validés (non signés). Parmi ses membres, on trouve Western Digital, Samsung, Seagate, HP, Toshiba, Lenovo, Dell ou Microsoft.

[79] L'AES chiffre le texte en clair, par blocs de 128 bits à la fois, à l'aide de clés symétriques de 128, 192 ou 256 bits. Une clé symétrique est une clé qui sert à la fois à chiffrer un texte et à déchiffrer ce même texte.

[80] Le PSID est un identifiant unique composé de 32 caractères alphanumériques qui se trouve le plus souvent imprimé sur l'étiquette du support.

134. En fonction de l'analyse des risques, une solution de chiffrement logiciel, tels les logiciels open source VeraCrypt (pour Windows, Mac OSX et Linux) et LUKS (Linux Unified Key Setup), pourra être préférée à la solution basée sur le matériel.

135. Il est à noter que certains constructeurs tiennent compte de ces potentielles violations des disques SSD et émettent des avertissements (ex. : Samsung).

3.2.4.4. Points d'attention

136. Cette technique (chiffrement suivi de l'effacement cryptographique) peut être utilisée sur d'autres supports (qui ne sont pas des SEDs ou ne supportant pas les commandes intégrées), en employant des logiciels de chiffrement tiers et en supprimant définitivement les clefs, une fois le chiffrement effectué. La phase de chiffrement préalable du support peut cependant être un processus très chronophage (plusieurs heures, en fonction de la capacité du support, de sa vitesse d'écriture/lecture et de la puissance de calcul affectée à l'opération).

137. Par opposition, le chiffrement à la volée des SEDs rend la technique de l'effacement cryptographique très rapide et empêche, quasi immédiatement, l'accès aux données contenues sur le support.

138. Dans le cas de l'effacement cryptographique, il faut par ailleurs être sûr qu'aucune donnée à caractère personnel n'ait été écrite avant le chiffrement à la volée car celles-ci ne seront pas protégées par l'effacement cryptographique.

139. Dans l'analyse des risques préalable au choix de cette technique, le responsable devra tenir compte des développements technologiques futurs qui peuvent rendre moins sûres les méthodes de chiffrement actuels.

140. L'opération de chiffrement, exécutée pour empêcher l'accès aux données contenues sur le support, devra être effectuée selon une procédure validée par le responsable du traitement.

3.2.4.5. Risques

141. Une fois chiffrées, les données, bien qu'enregistrées sous une autre forme, sont toujours présentes sur le support. L'emploi de cette technique implique donc que l'algorithme de chiffrement soit suffisamment robuste que pour résister au déchiffrement sans connaissance de la clef et, d'autre part, que la clef initiale (c.à.d. avant sa modification/destruction) ne soit, en aucune manière, récupérable, tant sur le support lui-même qu'ailleurs (pensez aussi aux éventuels backups). Ces exigences sont communes aux techniques utilisant du chiffrement.

142. Cette procédure prévoira que :

- L'algorithme de chiffrement utilisé soit reconnu et sûr[81,82] (ne pas utiliser d'algorithme obsolète tel DES ou 3DES par exemple) ;

- Les clés de chiffrement utilisées soient de longueur suffisante[83,82] ;

- Les clés de chiffrement utilisées soient gérées correctement (qu'elles ne se trouvent pas sur le support et en tout état de cause, pas en clair) ;

- Le chiffrement soit appliqué à l'entièreté du support ou à une subdivision logique de celui-ci (par opposition au chiffrement de répertoires ou fichiers individuels).

- Notons que la plupart des techniques de chiffrement modernes répondent à ces exigences.

143. Parallèlement aux risques liés aux évolutions technologiques, l'effacement cryptographique, ou plus exactement le chiffrement, présente également des risques intrinsèques liés à une éventuelle faiblesse du mot de passe protégeant la clé d'authentification (le cas échéant), la présence des clefs en mémoire, l'existence de données non chiffrées dans des fichiers temporaires ou encore, à la faiblesse du protocole de chiffrement utilisé. De plus, la certitude que les clés de chiffrement sont effectivement rendues inaccessibles de manière définitive, peut être difficile à obtenir[84].

144. Notons enfin que, en ce qui concerne les zones inaccessibles du support, les logiciels de chiffrement indépendants du matériel sont soumis aux mêmes limitations que les logiciels tiers de 'nettoyage' (voir article 3.2.1.1.).

145. C'est pourquoi, à l'instar du NIST, nous recommandons de procéder à la suite d'un effacement cryptographique, à un effacement/réécriture du support (avec vérification). Ceci afin de, notamment, diminuer le risque potentiel engendré par une clé de déchiffrement encore présente et accessible sur le support suite à une destruction inefficace ou absente.

Idéalement

146. Dans le meilleur de mondes, les fabricants de SEDs ou de supports offrant des commandes de type 'secure erase' devraient fournir, dans le détail, toute l'information nécessaire sur les commandes implémentées et surtout garantir le résultat de l'effacement, de préférence contractuellement. Rien n'empêche d'ailleurs le responsable du traitement de demander des assurances écrites à ce sujet au moment de l'achat de ces supports.

---

[81] \\ À titre d'exemple, l'annexe B1 du référentiel général de sécurité publié par l'ANSSI recommande le mécanisme de chiffrement symétrique AES (liens en Annexe C).

[82] L'ENISA (European Union Agency for Cybersecurity) publie également des documents relatifs aux algorithmes, longueurs de clé, paramètres et protocoles de chiffrement recommandés sur son site web.

[83] \\ À titre d'exemple, l'annexe B1 du référentiel général de sécurité publié par l'ANSSI recommande une taille minimum de clé symétrique de 128 bits (liens en Annexe C).

[84] Voir à ce sujet, la section 4.7.3 (Verification of Sanitization Results) des guidelines SP.880-88r1 du NIST, où est abordé p.21 le cas spécifique du cryptographic erase.

3.3. Le support de données est détruit

147. Notons d'emblée qu'il existe un certain nombre de cas où la destruction physique du support d'information devra être préférée à son 'nettoyage' :

- Si le support est défectueux ;
- Si le lecteur est défectueux ;
- Si l'équipement nécessaire pour accéder aux données n'est plus disponible ;
- Si le type de support rend le 'nettoyage' impossible, tels que les médias WORM (write once, read many - exemple : cd-rom non-réinscriptible) ;
- Si l'étape de vérification qui clôt les méthodes 'purge' ou 'clear' ne donne pas des résultats sûrs ou qu'elle échoue (pour des raisons connues ou inconnues).

148. Indépendamment de préoccupations environnementales, il peut être plus économique de procéder à la destruction des supports que de 'les nettoyer' en vue d'un réemploi.

149. Notons enfin que la destruction chimique ne sera pas considérée dans le présent document. Même si certains agents chimiques sont à même d'attaquer les supports de données et de les détruire, cette technique rarement utilisée est de plus, dangereuse pour la santé et nocive pour l'environnement.

3.3.1. Segmentation des techniques

150. A) Certaines techniques de destruction n'endommagent que partiellement le support.

- En conséquence, les données stockées sur les parties intactes peuvent rester accessibles. C'est le cas des techniques de déformation abordées à la section suivante 3.3.2.

151. B) D'autres techniques, telles le déchiquetage, le broyage ou la désintégration mettent le support en pièces (voir section 3.3.3.).

- Il est important de se rendre compte que dans ce cas aussi, les données sont toujours présentes sur le support visé. Elles sont simplement divisées en parties plus petites. Si l'on sait qu'un disque dur peut contenir des Téraoctets de données, on réalisera aisément qu'un fragment de plateau de disque dur, d'à peine un cm^2, pourra encore contenir plusieurs Giga-octets de données.
- Le niveau de sécurité/confidentialité apporté par une fragmentation du support, sera lié à la taille des fragments obtenus. Plus les fragments seront petits, plus la reconstruction des données nécessitera de ressources et de temps. Ce lien (taille des fragments - sécurité/confidentialité), est au cœur de la norme DIN 66399, abordée à la section 3.3.6.

152. C) Enfin, un 3e groupe de techniques permet la destruction intégrale du support et à fortiori des données qu'il contient.

- Le résultat est atteint en changeant l'état du support, c'est-à-dire, en passant de l'état solide à l'état gazeux (sublimation) ou à l'état liquide (fusion).

3.3.2. Déformation physique

153. Un grand nombre de techniques différentes sont couvertes par l'expression 'techniques de déformation[85] physique'. Elles peuvent être mises en œuvre, tant par d'imposants appareils industriels, que par des outils courants tels un marteau, une cloueuse à air comprimé, une perceuse ou encore une presse.

154. Parmi ces techniques, on trouvera notamment :

- Le pliage (folding / bending) ;
- Le découpage (cutting) ;
- Et le forage / perforation / poinçonnage (drilling / puncturing / punching / piercing).

155. Les benders utilisent un coin métallique pour plier un support (essentiellement des disques durs) sur sa longueur avec un angle de 90 degrés. Le coin métallique, pressé avec une grande force, endommage les plateaux, les têtes de lecture, le moteur électrique et l'électronique du disque dur de sorte qu'il ne soit plus accessible via son interface.

156. Pour ce qui est de la perforation, si l'image du technicien utilisant sa foreuse pour faire des trous dans un disque dur, vient immédiatement à l'esprit, cela n'est néanmoins pas la méthode préconisée par le secteur ITAD (IT Asset Disposition). Des machines dédiées à cette méthode existent en effet. Un perforateur utilise une broche en acier trempé pour percer les supports. Lors du perçage d'un disque dur, les plateaux, les têtes de lecture, le moteur électrique et l'électronique du disque dur sont endommagés de sorte qu'il n'est plus accessible via son interface.

157. Certains appareils proposent en option un module qui peut également détruire les SSD (Solid State Drive) par perforation. Selon le modèle, le SSD est percé à plusieurs endroits avec des broches métalliques ou fissuré en forme de vague.

158. Ces techniques ont en commun de n'endommager que partiellement le support et de laisser accessibles les données stockées sur les parties non affectées par la déformation.

159. En conséquence, ces techniques ne permettent pas d'atteindre le niveau de confidentialité « destroy », même si elles peuvent rendre les données impossibles à récupérer via l'interface des supports et que ceux-ci ne peuvent plus être utilisés pour un stockage ultérieur. Le support n'est en effet pas considéré comme 'détruit' tant

[85] En anglais : deformation

que la récupération de données est possible, même si cela nécessite des techniques de laboratoire de pointe.

160. À titre de confirmation, dans son document de référence[86] sur le sujet, la NSA ('National Security Agency' des États-Unis) ne cite les techniques de déformation que comme des mesures complémentaires[87] et néanmoins hautement recommandées, à un dégaussage de disques dur magnétiques. La déformation seule, n'est donc pas validée par la NSA comme méthode de 'nettoyage'.

3.3.3. Déchiquetage, broyage et désintégration[88]

161. Bien que ces techniques soient différentes, elles débouchent toutes les trois sur une désagrégation du support, en le transformant en composants plus petits. La taille des débris sera dépendante de la technique, des matériaux composant le support et des caractéristiques techniques de l'appareil utilisé pour ce faire.

162. Les déchiqueteuses, par exemple, existent dans une large gamme de tailles et selon le modèle, pourront réduire en pièces, à peu près n'importe quoi, du pneu au disque dur ou SSD, en passant par du papier ou un canapé. La taille moyenne des débris sera fonction du modèle tandis que leur taille individuelle dépendra des matériaux entrant dans leur composition. Ainsi, pour un disque dur, les morceaux en plastique du boîtier seront à priori plus grands que les morceaux des plateaux.

163. Le choix d'une technique plutôt qu'une autre, est secondaire par rapport à la taille des débris obtenus. C'est pourquoi nous ne nous appesantirons pas, au-delà de la simple description, sur les techniques elles-mêmes.

164. Comme spécifié par la norme ISO/IEC 21964, « dans ce contexte (destruction du support), détruire en toute sécurité signifie détruire les supports de données contenant les données à caractère personnel, de telle sorte que la récupération des informations les concernant soit impossible ou ne soit possible qu'avec des dépenses considérables (en termes de personnel, de ressources matérielles et de temps) ».

3.3.3.1. Déchiquetage

165. Les déchiqueteuses sont constituées de cylindres juxtaposés portant des couteaux en acier trempé, qui tournent en sens opposé pour couper, déchirer et extruder les matériaux. Pour les matériaux qui nous intéressent plus spécialement, on trouve des déchiqueteuses n'acceptant que des supports minces, tels les supports optiques (CD, DVD, Blu-Ray), les supports de mémoire (clés USB, cartes mémoire), les bandes magnétiques (audio, vidéo, données), les cartes magnétiques ou à puce de tout type, alors que d'autres acceptent également smartphones, tablettes, disques durs et éventuellement SSDs et enfin d'autres appareils dédiés à la destruction du papier.

---

[86] NSA/CSS Storage Device Sanitization Manual

[87] La NSA évalue malgré tout, la capacité de certains appareils à déformer le ou les plateaux d'un disque dur (magnétique) en 30 secondes ou moins, par pliage (bending), poinçonnage (punching) ou gaufrage (waffling). Les appareils répondant à ces critères sont rassemblés dans le document 'NSA/CSS Evaluated Products List for Hard Disk Drive Destruction Devices'

[88] En anglais : shredding, crushing et desintegration

166. Une déchiqueteuse de papier est un dispositif mécanique utilisé pour couper le papier en bandes ou en particules. Notons qu'elle peut aussi être utilisée pour détruire les supports flexibles tels que les disquettes, une fois que les supports sont physiquement retirés de leurs conteneurs extérieurs. La taille des lambeaux doit être suffisamment petite pour qu'il y ait une assurance raisonnable, proportionnelle à la confidentialité des données, que les données ne puissent pas être reconstruites. Pour être approuvées par la NSA, les déchiqueteuses papier doivent être capables de réduire les documents papier en fragments mesurant au maximum un millimètre sur cinq millimètres[89]. Des appareils de type désintégrateurs peuvent aussi détruire des documents papier (voir par.178)

Solid State Drives - SSDs

167. Rappelons encore une fois que les disques durs (magnétiques) et les SSDs (électroniques) ont des caractéristiques techniques fort différentes et ne peuvent donc être, à priori, 'nettoyés'/détruits de la même manière.

168. Les déchiqueteuses non spécifiquement adaptées à ces supports produiront des débris de trop grande taille que pour détruire de manière sécurisée les données sur les puces à semi-conducteurs haute densité.

169. Les normes de sécurité de la NSA exigent que les disques durs soient réduits à une taille de particules finale de deux millimètres, soit, soient démagnétisés puis détruits physiquement (broyeurs ou déchiqueteurs). Cette deuxième option n'est pas envisageable pour les SSDs. Cependant, selon une étude menée par la firme Blancco (déc. 2018), bon nombre d'organisations (33% aux USA et au Canada) n'ont pas de processus différent pour traiter ces 2 types de support.

170. Avec une densité de stockage de données toujours plus grande, la taille des puces sur les SSDs se réduit. Un déchiquetage à des tailles plus grandes que ces composants peuvent donc laisser totalement intactes les informations contenues sur le support.

171. Pour rendre la reconstruction des données encore plus difficile, le matériau déchiqueté peut être mélangé avec un matériau non sensible du même type (papier déchiqueté ou support flexible déchiqueté), une plus grande quantité de débris augmentant d'autant la difficulté de reconstruction. Ceci est d'ailleurs valable également pour toutes les techniques et natures des résidus de destruction.

3.3.3.2. Broyage

172. Les broyeurs/concasseurs utilisent plutôt la force de compression pour écraser le support en le brisant en morceaux (exemples : entre deux mâchoires, dont une fixe - jaw crusher ou par percussion - impact crusher).

173. Le terme de broyeur est parfois utilisé pour « des appareils capables de réduire la couche porteuse de données d'un disque optique en fine poussière tout en laissant intact le disque lui-même qui sera recyclé ou éliminé. Toutefois, on ne peut utiliser

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

cette méthode pour les DVD puisque leur couche porteuse d'information est prise en sandwich au centre » (source : BCSS[90]). Cependant, il s'agira dans ce cas plutôt d'une technique de meulage (abrasion). Nous rajouterons que le problème est identique pour les disques Blu-Ray.

174. Toujours à propos des supports optiques, signalons que la NSA publie également, comme pour les disques durs[87] et d'autres types de supports[91], une liste d'appareils validés[92] pour la destruction par fragmentation. Pour y figurer les appareils doivent fournir des résidus dont le côté ne dépasse pas :

- Pour les CD, une longueur de 5 millimètres ;
- Pour les DVD et Blu-Ray, une longueur de 2 millimètres.

3.3.3.3. Désintégration

175. On utilise souvent le terme de désintégration/désintégrateur quand la taille des fragments obtenus est inférieure ou égale à deux millimètres de côté. Cette taille est liée aux prescrits de la NSA, mentionnés dans le document NSA/CSS Storage Device Sanitzation Manual. Si le matériel a été testé par la NSA et répond aux exigences du manuel, il sera intégré dans la liste NSA/CSS Evaluated Products List for Hard Disk Drive Destruction Devices.

176. En parallèle, il est recommandé de désintégrer les supports (tant HD que SSD) en lots avec d'autres périphériques de stockage.

177. Les désintégrateurs de disques utilisent la technologie de fraisage (milling) au couteau pour couper le support en morceaux, et ce en continu jusqu'à ce que ces derniers soient suffisamment petits pour passer au travers d'un tamis de dimensionnement des déchets spécifié. La désintégration est plus lente que le déchiquetage mais la taille des débris est plus petite et le niveau de sécurité/confidentialité atteint, plus élevé.

178. Les désintégrateurs de papier (différents des déchiqueteuses papier - voir par.166) doivent, pour être approuvés par la NSA, produire des lambeaux dont la taille des côtés ne dépasse pas trois millimètres sur cinq millimètres[93].

3.3.3.4. Remarques

179. Il est à noter que les outils de traduction sont assez peu précis, pouvant donner plusieurs traductions différentes à une même technique dans une même phrase. Les sites web abordant la destruction physique de supports d'information (y compris certains constructeurs) mélangent aussi assez fréquemment les noms des appareils

---

[90] Document de la BCSS (Banque Carrefour de la Sécurité Sociale) : Ligne directrice sécurité de l'information & vie privée - Effacement des supports d'information électroniques (mars 2017) p.7

[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

et techniques, voir utilisent des noms sans lien avec la technologie employée (destroyer, dissambly device, cracker, …).

180. Nous avons vu, par exemple que pour qu'un support d'information de type disques durs et SSDs soit considéré par la NSA comme 'nettoyé' adéquatement via une technique de désagrégation, deux conditions doivent être remplies : il faut que les résidus ne fassent pas plus de 2mm de côté et d'autre part que l'appareil employé figure dans la liste des appareils approuvés (on n'y trouve que des sociétés américaines). Il en va différemment de la norme DIN 66399.

181. Cette norme spécifie, en fonction de la taille des résidus, quel niveau de sécurité est atteint par une méthode quelconque de destruction, et ceci pour six grandes classes de support d'information (ex. : papier, optique, électronique ou magnétique), mais nous y reviendrons à la section 3.3.6.

182. Le responsable du traitement gardera à l'esprit, que lorsqu'il choisit de faire appel à un prestataire externe afin d'éliminer ses supports par les techniques abordées au chapitre 3.3., une fois la destruction effectuée, ce prestataire les recyclera probablement ou les déposera dans une décharge.

183. Cela signifie que les données, si les supports n'ont pas été détruits de manière sécurisée, seront à nouveau potentiellement accessibles à des tiers. Les restes des supports pourraient même se retrouver dans différentes parties du monde s'ils sont vendus à des entreprises de gestion des déchets ou de recyclage. L'incinération élimine ce risque.

3.3.4. Incinération

184. L'incinération, quoique plus rarement utilisée et ayant un impact environnemental important, est une technique efficace car, si menée à bien dans des incinérateurs[94] adéquats, elle garantit à elle seule, la destruction totale et irréversible des données et des supports. Ceux-ci peuvent consister en de gros incinérateurs de déchets, comme en de plus petits incinérateurs mobiles et compacts que des entreprises spécialisées peuvent amener sur le site du responsable du traitement qui en fait la demande. Certains modèles mobiles sont dédiés à l'élimination du papier mais d'autres sont capables de faire fondre le métal.

185. Dans le cadre de leur transformation digitale, bon nombre d'organisations numérisent des documents pour les stocker en ligne ou les archiver et se retrouvent ensuite avec les originaux à éliminer. Lorsque les quantités de papier à éliminer sont grandes, l'incinération peut être une alternative au déchiquetage.

186. D'autres types de support peuvent être détruits par cette technique. Dans son manuel relatif au nettoyage des supports, la NSA cite ainsi les bandes magnétiques, les disquettes, les supports optiques, les supports électroniques et le papier, comme pouvant être détruits de manière sécurisée par incinération, pour autant que le matériel ait été réduit à l'état de cendres. Pour ce qui est des disques durs, elle précise que le revêtement des plateaux internes devra être réduit en cendres et/ou les plateaux internes devront être physiquement déformés par l'action de la chaleur.

[94] Unité qui permet une combustion presque totale des constituants combustibles d'un déchet.

187. Si l'incinération se produit en-dehors du contrôle du responsable du traitement, ce dernier s'assurera qu'un traitement des supports, offrant une chaîne de traçabilité complète, est mis en place par le ou les prestataires externes.

3.3.5. Démagnétisation - dégaussage (degaussing)

188. La démagnétisation, déjà présentée en tant que technique de 'nettoyage' (avec conservation du support - voir section 3.2.3.), permet également de détruire (rendre inutilisable) les supports magnétiques si ceux-ci sont soumis à une force magnétique suffisante[95], et ce quel que soit leur système d'exploitation et interface, même s'ils sont endommagés.

189. Insistons à nouveau sur le fait que la démagnétisation n'est, par contre, pas efficace, sur les dispositifs de mémoire flash dont les disques SSD. De même, cette technique n'est pas adaptée aux supports papier et optiques.

190. La démagnétisation soumet les supports magnétiques à un champ magnétique puissant qui peut être créé soit par des aimants puissants, soit par une décharge électromagnétique.

191. Il est recommandé de faire suivre la démagnétisation par une autre technique de destruction ; Ceci permettra d'atteindre le plus haut niveau de confidentialité/sécurité, palliera à une défaillance du démagnétiseur ou à un oubli du technicien et fournira une vérification visuelle que le support a été détruit et est prêt à être éliminé. Dans ces conditions et moyennant l'utilisation d'un appareil[96] approuvé[71], la NSA valide la technique au niveau 'purge'.

3.3.6. La norme DIN 66399

192. La norme DIN 66399 du Deutsches Institut für Normung, intitulée « Büro- und Datentechnik - Vernichten von Datenträgern »[97] spécifie, en fonction de la taille des débris résultant de la destruction du support, quel niveau de sécurité est atteint par des appareils dont l'usage prévu est de détruire les supports de données.

193. Très populaire en Europe, elle tient moins compte de la technique employée que des résultats de celle-ci, et ce pour six grandes classes de support d'information.

194. Cette norme (payante[98]) ou plus exactement cette série de normes est constituée de trois parties[99] :

- Part 1 : Principles and definitions (publication 10/12) ;

---

[95] Exemples de dégausseurs capables de détruire des disques durs et bandes magnétiques

[96] Le démagnétiseur est un aimant finement réglé qui entre en contact avec d'autres supports magnétiques et qui peut détruire la signature magnétique de toute donnée stockée.

[97] Institut allemand de normalisation - « Office machines - Destruction of data carriers »

[98] Chaque partie coûte quelques dizaines d'euros.

[99] Partie 1 : Principes et définitions, Partie 2 : Exigences pour l'équipement de destruction des supports de données et Partie 3 : Processus de destruction des supports de données.

- 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. Quoi qu'ayant été remplacée depuis 2012 par la norme DIN 66399, la classification[100] liée à la norme obsolète DIN 32357 (1995), qui s'appliquait exclusivement au papier, est encore souvent citée dans le descriptif des appareils concernés (essentiellement des déchiqueteuses - paper shredders).

196. La norme DIN 66399 définit des classes de protection, des catégories de supports et des niveaux de sécurité.

Trois classes de protection

197. Elles déterminent dans quelle mesure les données doivent être protégées, en fonction d'une évaluation du type de données présentes sur le support. L'exigence de protection/sécurité se scinde en catégories normale, haute et très haute :

- Classe de protection 1 - Exigence de sécurité normale pour des données internes. La perte de données aurait un impact négatif sur l'organisation ou présenterait un risque d'usurpation d'identité pour les personnes concernées ;

- Classe de protection 2 - Exigences de sécurité plus élevée pour des données confidentielles. La perte de données aurait un impact très négatif sur l'organisation ou pourrait enfreindre ses obligations légales ou présenter un risque de nature financière ou sociale pour les personnes concernées ;

- Classe de protection 3 - Exigences de protection très élevées pour des données très confidentielles et secrètes. La perte de données pourrait avoir des conséquences irréparables pour l'organisation ou présenter un risque pour la santé et la sécurité ou les libertés individuelles des personnes concernées.

Six catégories de supports de données

198. La norme divise les différents types de supports de données en 6 catégories ou classes :

- Classe P (paper) - Format original (papier, films radiographiques) ;

- Classe F (microfilm) - Format réduit (microfilm) ;

- Classe O (optique) - Supports de données optiques (CD, DVD, Blu-Ray) ;

- Classe T (tape) - Supports de données magnétiques (bandes, disquettes, cartes de crédit) ;

[100] La norme DIN 32757 définit 5 niveaux de sécurité. On rencontre aussi dans la littérature un 6e niveau non-officiel 'Level 6 - Highest Security'. Ces niveaux de sécurité sont liés à la finesse du déchiquetage du matériau et expriment donc le niveau de sécurité offert par les déchiqueteuses.

- Classe H (hard drive) - Disques durs magnétiques ;

- Classe E (electronic) - Supports de données électroniques (clé USB, SSD, cartes mémoire, cartes à puce, mémoire flash de smartphones et tablettes, cartes mémoire d'appareils photo numériques).

Sept niveaux de sécurité

199. Les sept niveaux de sécurité sont dérivés des trois classes de protection, chacune des classes couvrant trois niveaux de sécurité :

- Classe de protection 1 - Niveaux de sécurité 1, 2 et 3

- Classe de protection 2 - Niveaux de sécurité 3, 4 et 5

- Classe de protection 3 - Niveaux de sécurité 5, 6 et 7

200. Ces niveaux de sécurité déterminent la quantité d'efforts et de ressources qu'il faudra déployer si l'on voulait récupérer les données à partir d'un support détruit (plus le niveau de sécurité est élevé, plus les débris devront être petits) :

- Niveau de sécurité 1 - La récupération des données nécessite un effort simple (concerne des documents généraux à rendre illisible).

  Autrement dit, le niveau 1 est sélectionné pour des données ordinaires, pour lesquelles peu ou pas de protection est nécessaire (par exemple des brochures et journaux) et dont la reconstitution éventuelle à partir du support détruit ne présenterait aucun problème de protection des données ;

- Niveau de sécurité 2 - La récupération des données nécessite un effort et des outils particuliers (concerne des documents internes à rendre illisibles) ;

- Niveau de sécurité 3 - La récupération des données nécessite un effort considérable en main-d'œuvre, temps et outils (concerne des données sensibles/confidentielles ainsi que des données à caractère personne soumises à des exigences de protection élevées) ;

- Niveau de sécurité 4 - La récupération des données nécessite un effort exceptionnel et des outils inhabituels (concerne des données hautement sensibles/confidentielles ainsi que des données à caractère personnel soumises à des exigences de protection élevées) ;

- Niveau de sécurité 5 - Récupération des données possible uniquement avec des outils inhabituels (concerne des données confidentielles d'une importance fondamentale pour une organisation ou les personnes concernées) ;

- Niveau de sécurité 6 - La récupération des données est peu probable avec l'état actuel de la technologie (concerne des données confidentielles soumises à des exigences de protection hors de l'ordinaire) ;

- Niveau de sécurité 7 - La récupération des données est impossible avec l'état actuel de la technologie (concerne des données strictement confidentielles soumis à des exigences de protection les plus élevées).

Autrement dit, le niveau 7 est sélectionné pour des données 'top-secret' (services secrets, documents militaires), quand la possibilité de reconstitution des données à partir du support détruit doit être absolument exclue (selon l'état actuel des connaissances).

Tableaux

201. Nous pouvons regrouper l'ensemble de ces éléments dans un tableau permettant de trouver le niveau de destruction nécessaire.

	Classe de protection 1		Classe de protection 2			Classe de protection 3	
Catégorie de support	Niveau de sécurité 1	Niveau de sécurité 2	Niveau de sécurité 3	Niveau de sécurité 4	Niveau de sécurité 5	Niveau de sécurité 6	Niveau de sécurité 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. À titre d'exemples, voici les niveaux de sécurité recommandés pour les catégories de supports H et P :

H – Disques durs magnétiques	
Niveau de sécurité	**État / Taille max. résidus**
H-1	Hors-service
H-2	Endommagé
H-3	Déformé
H-4	2000 mm²
H-5	320 mm²
H-6	10 mm²
H-7	5 mm²

P – Format original (papier)	
Niveau de sécurité	**État / Taille max. résidus**
P-1	Largeur de bande 12 mm ou 2000 mm²
P-2	Largeur de bande 6 mm ou 800 mm²
P-3	Largeur de bande 2 mm ou 320 mm²
P-4	160 mm²
P-5	30 mm²
P-6	10 mm²
P-7	5 mm²

203. Note : au niveau H1, le disque peut être hors-service pour raison mécanique ou électronique.

Exemples d'interprétation

204. Bon nombre de constructeurs et revendeurs accolent à la description de leurs appareils de destruction de supports des références telles « E-1 / H-3 » ou « T-1 / E-2 / H-3 ». Il s'agit, selon les constructeurs, des niveaux de sécurité en fonction de la classe de support de la nome DIN 66399 que le matériel peut atteindre. Voici quelques exemples d'interprétation de ces niveaux de sécurité :

- Un disque dur relevant de la catégorie de support «H» (voir tableau ci-dessus) et comportant des données de nature sensible ou confidentielle nécessitant un niveau de sécurité 3 (c'est-à-dire le niveau H-3) devra être déformé afin de répondre aux exigences de la norme DIN 66399

- Si un appareil de destruction annonce atteindre le niveau P-5 (voir tableau ci-dessus), cela signifie qu'il répond, pour les supports au format original (ex. : papier - catégorie de supports de données « P ») au niveau de sécurité 5 et donc qu'il est capable de fragmenter le support en particules de 30 mm^2. Un tel appareil permettra donc de répondre aux exigences de la norme DIN pour des données hautement confidentielles (par exemple des documents médicaux). Une fois détruites par cet appareil, ces données ne pourront plus être reconstituées au moyen de techniques usuelles.

- Un microfilm appartenant à la catégorie de support «F» (tableau non-fourni ci-dessus), de nature très confidentielle et qui nécessite un niveau de sécurité 5 (c'est-à-dire le niveau F-5) devra être déchiqueté à une taille de particule de maximum 1 mm^2.

Utilisation de la norme DIN en pratique

205. Étapes à suivre pour déterminer le niveau de sécurité à atteindre et la taille maximum des résidus après destruction du support afin de sélectionner l'appareil de destruction adéquat :

A. Parmi les 3 classes de protection, choisissez celle correspondant au niveau de confidentialité/sécurité des données contenues sur les supports à détruire (document interne, confidentiel ou très confidentiel)

B. La classe de protection sélectionnée vous offre alors un choix parmi 3 niveaux de sécurité (plus le niveau de sécurité sélectionné est élevé, plus les résidus seront petits).

C. Sélectionnez ensuite le type de support à détruire (papier, électronique, bandes magnétiques, ...)

D. Reliez maintenant le support de données et le niveau de sécurité. Vous pourrez alors utiliser ces informations pour sélectionner un destructeur de documents approprié.

DIN et ISO

206. En 2018, l'ISO/IEC JTC101 a normalisé au niveau international la norme DIN 66399 développée en 2013. Numérotée ISO/CEI 21964, cette norme est désormais référencée par les organisations au niveau mondial en ce qui concerne les exigences de destruction des données. Les matériaux référencés dans les niveaux de sécurité sont identiques à ceux référencés dans la norme DIN 66399.

207. Les 3 parties de la norme DIN (voir par.194) correspondent aux 3 parties de la norme ISO suivantes :

[101] Joint Technical Committee de l'International Organization for Standardization (ISO) et de l'International Electrotechnical Commission.

- 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

Comparaison DIN - NSA - NIST

208. D'une manière générale, la norme DIN 66399 n'est pas aussi exigeante que les lignes directrices et standards du NIST ou de la NSA.

209. Ainsi au contraire de la norme DIN, la NSA recommande de faire précéder la destruction de disques dures (magnétique et électroniques) d'une démagnétisation. De plus la destruction doit se faire avec des appareils approuvés par la NSA.

210. Par ailleurs, la démagnétisation, à l'instar de toute technique n'aboutissant pas à une fragmentation du support, n'est pas prise en compte par la norme DIN, alors que la NSA d'une part, l'intègre et recommande de la faire suivre par une technique de déformation ou de destruction et que le NIST d'autre part, l'intègre au niveau « purge » (et indirectement au niveau « destroy », vu les dégâts irréparables que la technique peut occasionner).

211. En ce qui concerne les niveaux de sécurité mêmes, le NIST requiert, par exemple pour les supports papier, un déchiquetage qui produit des résidus ne dépassant pas 1 mm x 5 mm de côté, ou une pulvérisation/désintégration à l'aide d'un appareil équipé d'un écran de sécurité[102] de 2.4 mm. Seul le dernier niveau de sécurité de DIN (P-7) répond à cette exigence (taille maximum des résidus de 5 mm^2).

212. Une autre particularité, associée à chaque niveau de sécurité de la norme DIN et absente des lignes directrices et standards du NIST et de la NSA, vient aussi en diminuer le niveau d'exigence. Il s'agit de l'écart ou déviation admissible qui est l'écart autorisé par rapport à la taille de particule recommandée pour chaque niveau de sécurité de a norme DIN.

213. Par exemple, le niveau de sécurité H5 (voir tableau par.202) de la norme DIN, spécifie une taille maximum des résides de 320 mm^2 mais les spécifications complètes de ce niveau stipulent en fait que seules 90% de ces particules doivent être inférieures ou égales à cette taille et autorise que 10% d'entre elles atteignent les 800 mm^2. Cela en soi, tendrait à disqualifier H5 comme acceptable pour des données confidentielles d'une importance fondamentale pour une organisation ou la personne concernée.

214. Cet écart admissible est défini à chaque niveau de sécurité pour chaque type de support.

[102] Le support est découpé en continu jusqu'à ce que les particules résultantes soient suffisamment petites que pour passer à travers un tamis de dimensionnement spécifique.

215. En résumé, la norme DIN 66399 est facile à lire et utile au monde de l'entreprise mais est sans doute moins indiquée pour des supports comportant des données hautement confidentielles et nécessitant un haut niveau de sécurité, que les lignes directrices et standards du NIST et de la NSA.

4. Cas particuliers

216. Il n'est pas toujours possible pour le responsable du traitement de procéder à l'effacement ou à la destruction des supports d'information.

217. C'est le cas lorsque les supports ne lui appartiennent pas. On pensera par exemple au matériel informatique sous contrat de location (imprimantes/photocopieurs, infrastructure serveur chez le prestataire de service IT, cloud computing ou encore système de vidéosurveillance avec enregistrement).

218. Le responsable du traitement doit alors s'assurer que le contrat prévoit la possibilité d'effacer les données ou de détruire les supports selon une méthode qui l'agrée et dont il aura la possibilité de vérifier la bonne exécution et son résultat. Si l'adaptation contractuelle ou le contrôle s'avèrent difficiles, le responsable du traitement peut aussi négocier un rachat des supports contenus dans les appareils.

219. Nous ne saurions trop insister sur la nécessiter d'aborder les points relatifs à la protection des données avant la signature du contrat. Cela s'avère souvent difficile par après.

220. C'est le cas aussi lorsqu'un appareil contenant un support d'information (ou le support lui-même) doit être réparé, remplacé ou subir un entretien en-dehors de votre périmètre de contrôle. Vous devez alors évaluer le risque associé à un accès aux données par le prestataire de services. Rappelons encore que le RGPD se focalise sur l'impact d'une perte de confidentialité pour les personnes concernées (les personnes auxquelles les données se rapportent).

221. Si cette opération présente un risque pour les personnes concernées, elle devra rester sous le contrôle du responsable du traitement (par ex. réparation sur place ou achat d'un support de replacement afin de garder celui qui est défectueux[103]).

[103] Précisons que certains fournisseurs (dont HP, Dell et Lenovo) proposent la possibilité de souscrire à une garantie additionnelle de type « keep your drive » permettant au client de conserver un support défectueux qui doit être remplacé.

5. Vérification

222. La dernière étape de la procédure, avant la délivrance d'un document attestant du nettoyage ou de la destruction (voir 6e partie « Enregistrement »), consiste à vérifier la destruction des données, ce qui doit permettre de garantir que celles-ci ont été correctement nettoyées ou détruites. Elle est indispensable car les sources de défaillance possibles sont multiples. Pensons aux erreurs humaines (ex. : disque non-traité mis dans la pile des disques traités, manque de formation, envie d'aller vite), aux erreurs 'matériel' (ex. : couteau d'une déchiqueteuse endommagé ou défaillance d'un des composants situés entre le logiciel d'effacement et les données sur les disques) et aux erreurs 'logiciel' (absence de mise à jour, qualité du logiciel).

223. Lorsque le responsable du traitement fait appel à un sous-traitant pour les opérations de nettoyage ou destruction, cela nécessitera de discuter avec ce dernier des modalités de vérification et éventuellement de les définir contractuellement.

224. La vérification est idéalement exécutée par une personne indépendante et n'ayant pas pris part à la destruction ou au nettoyage proprement dit des supports de donnés. En suivant la même logique, lorsqu'un logiciel est utilisé pour le nettoyage des données, la partie vérification devrait être assurée par un logiciel différent de celui utilisé pour le nettoyage.

225. Ce processus de contrôle qualité est documenté au même titre que les autres étapes de la procédure de destruction/nettoyage. Par exemple, le nombre d'échantillons à tester sera prévu dans la documentation.

226. En parallèle à cette documentation, le responsable du traitement doit disposer d'un système d'information qui permet, à la demande, de produire une preuve de conformité (c'est-à-dire confirmer l'effacement réussi des données) et ce, support par support.

227. Nous terminerons cette 5e partie par quelques informations sur la vérification propres à différentes techniques de 'nettoyage'.

Effacement - réécriture

228. Selon son étendue, le résultat de la vérification pourra être plus ou moins fiable, la meilleure assurance d'un 'nettoyage' effectif des données étant généralement obtenue par une lecture complète de toutes les zones accessibles du support, afin de vérifier que l'on y trouve bien les valeurs (nombres binaires 0 ou 1) attendues, c'est-à-dire celles décidées dans le paramétrage de la passe de réécriture.

229. Cette lecture de vérification, n'est évidemment possible que lorsque le support n'est pas détruit.

230. Même si la vérification est un processus chronophage, le pourcentage de la surface du support à vérifier devrait, en fonction du temps disponible, être aussi grand que possible, et en tous cas ne devrait pas être inférieur à 10% (ce qui est par ailleurs souvent le pourcentage proposé par défaut par les logiciels tiers).

231. Les logiciels tiers et les commandes intégrées offrent des possibilités de vérification. Cependant, si l'on désire procéder à une vérification manuelle et

indépendante de l'outil employé pour le nettoyage, on pourra utiliser un 'disk editor' (souvent couplé à un 'hex editor'). Ces logiciels sont par ailleurs le plus souvent utilisés pour la récupération de données et la criminalistique numérique (digital forensics). \\ À titre d'exemples, nous citerons trois de ces logiciels : Active@ Disk Editor et HxD (freewares) ainsi que WinHex (logiciel commercial bien connu).

232. Pour les niveaux 'clear' et 'purge', que ce soit avec les logiciels tiers ou lorsqu'une commande intégrée de réécriture est utilisée, la vérification devra permettre de confirmer que les valeurs attendues (voir par.228) sont présentes sur le support. Dans le cas où plusieurs passes de réécriture ont été appliquées, ce sont les valeurs de la dernière passe qui seront recherchées.

Effacement cryptographique

233. Dans le cas de l'effacement cryptographique, la vérification la plus efficace consistera à lire des emplacements aléatoires avant l'effacement, puis à nouveau après l'effacement cryptographique pour comparer les résultats.

234. Ce qui implique que si l'effacement cryptographique est suivi d'une autre technique (destruction par ex.), la vérification devra être effectuée avant cette dernière. Une vérification via un échantillonnage rapide sera également effectuée après l'application de la technique supplémentaire.

Déchiquetage, broyage, désintégration

235. Pour les supports ayant été réduits en pièces, une vérification de la taille des résidus sera effectuée visuellement ou à l'aide d'un tamis correspondant à la taille maximum acceptée ou d'un autre instrument de mesure (ex. pied à coulisse digital de haute précision).

Démagnétisation

236. L'assurance d'une démagnétisation correcte repose essentiellement sur la sélection d'un dégausseur efficace, sur son emploi approprié et sur une vérification ponctuelle périodique des résultats pour s'assurer qu'il fonctionne comme prévu.

6. Enregistrement

237. La preuve de destruction est un élément essentiel de la chaîne de traçabilité. En conformité avec le principe de responsabilité (accountability) du RGPD (art.5.2), elle permettra au responsable du traitement de démontrer son respect des principes en matière de traitement des données à caractère personnel, dont ceux relatifs à la limitation de la conservation et à l'intégrité et à la confidentialité (art.5.1.e et f - voir Annexe B).

238. Il est donc important d'enregistrer et conserver les informations relatives au bon déroulement du nettoyage et/ou de la destruction et à la technique (et donc au niveau de confidentialité/sécurité sélectionné) et ce, que la procédure soit effectuée en interne ou avec l'aide d'un sous-traitant. La preuve de destruction/nettoyage est en général délivrée par la personne en charge de l'opération (sous l'autorité du sous-traitant ou du responsable du traitement) et validée par une personne désignée par le responsable du traitement.

239. Quoique cette preuve soit souvent appelée 'certificat' de destruction par les différents acteurs du secteur, nous lui préférerons les termes d'attestation ou déclaration, pour leur connotation moins officielle[104].

Sous-traitance

240. Lorsqu'il est fait appel à un sous-traitant pour un nettoyage et/ou une destruction de supports d'information, ces derniers peuvent être rassemblés et conservés par le responsable du traitement en un lieu dont l'accès n'est pas sécurisé, jusqu'à ce que le sous-traitant les récupère. L'entreposage temporaire de ces supports n'exclut alors pas la possibilité de perte ou de vol. C'est pourquoi, il pourra être utile de comparer la liste des supports qui ont été stockés et la liste des supports qui sont effectivement pris en charge par le prestataire externe. Nous rappellerons à nouveau la nécessité de désigner un ou des responsables pour chaque étape du traitement dont notamment celles de la collecte des supports et de leur entreposage.

241. Le processus de nettoyage proprement dit peut s'effectuer sur le site du responsable du traitement ou en-dehors (selon les possibilités techniques du sous-traitant ou la demande du responsable du traitement). Dans le cas d'un traitement hors-site, il faudrait idéalement qu'un agent du responsable du traitement soit physiquement présent pendant tout le processus de destruction, afin de s'assurer que les supports aient été effectivement bien détruits. Sans cela, la « preuve de destruction » remise par le sous-traitant pourrait ne pas correspondre à la réalité et ne pas constituer un document probant. Le responsable du traitement pourra également faire appel à des huissiers de justice pour contrôler et enregistrer l'ensemble des opérations.

242. Comme déjà mentionné au par.58, la délivrance par le sous-traitant d'une attestation de nettoyage/destruction doit faire partie de l'accord contractuel conclu avec lui. Si des données qui devaient être traitées en vertu du contrat sont plus tard

[104] Le Larousse définit un certificat comme un « document écrit, officiel ou dûment signé d'une personne autorisée qui atteste un fait ».

retrouvées, l'attestation pourra constituer une preuve que le sous-traitant a commis une faute.

L'attestation

243. Une preuve de nettoyage/destruction se présentera sous la forme d'une attestation détaillée pour chaque support qui a été traité. Qu'elle soit sous format papier ou digital, c'est un élément critique qui doit permettre de valider que les données ont été rendues irrécupérables à partir du support qui a été nettoyé.

244. Elle répertorie généralement chaque périphérique de stockage par numéro de série, décrit le niveau de confidentialité/sécurité visé (clear, purge, destroy, H-1, P-5, ...), la technique de nettoyage utilisée (démagnétisation, déchiquetage, effacement cryptographique, ...), les outils utilisés pour y parvenir, la méthode de vérification utilisée et son résultat ainsi que d'autres éléments d'information par exemple liés à la date, au lieu et aux personnes impliquées.

245. Synthétiquement, l'attestation de destruction comportera des informations relatives :

- À la date et au lieu de la procédure ;
- À l'organisation, la personne procédant à la destruction (identification) ;
- Au support de données et au matériel incorporant ce support (n° de série, type, ...) ;
- À la technique employée (outils logiciels et matériels, niveau de confidentialité/sécurité, norme de référence, méthode, ...) ;
- À la vérification (méthode) et à son résultat final ;
- À la destination du support (réutilisation, élimination, retour au fournisseur, ...) ;
- À la validation de l'attestation (coordonnées de la personne vérifiant l'attestation, cette personne étant différente de celle ayant procédé à la destruction).

246. L'attestation doit être conservée et pouvoir être produite à la demande. Bien que la Banque carrefour de la sécurité sociale (BCSS) préconise une durée de conservation de l'attestation « d'au moins 2 ans[105] », nous estimons prudent de tenir compte des délais de prescription légaux[106]. Ces délais seront généralement de 5[107] ou 10 ans[108].

---

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

[106] Les délais de prescription sont détaillés aux articles 2262bis et suivants du Code civil.

[107] Actions personnelles dérivant d'un évènement extracontractuel : 5 ans (Art. 2262 bis §1er, al. 2 et 3 Code civil)

[108] Actions personnelles dérivant de l'exécution d'un contrat : 10 ans (art. 2262 bis §1er, al. 1 Code civil).

247. En effet, tant que le délai de prescription n'est pas expiré, une personne ou une organisation ayant subi un dommage du fait d'un nettoyage déficient des données ou d'une destruction insuffisante d'un support de données, peut saisir les cours et tribunaux afin d'obtenir la condamnation du responsable du traitement à l'indemnisation de son dommage voire à d'autres sanctions.

Annexe A : Techniques recommandées pour les principaux types de support

Supports magnétiques Floppy Disks	**Clear**	⇨ **Réécriture** (écrasement) du support à l'aide d'un logiciel approuvé par l'organisation puis valider (vérification). Le niveau Clear doit se traduire par au moins une passe d'écriture avec une valeur de données fixe (ex.: tous des zéros). Facultatif : plusieurs passes d'écriture ou des valeurs plus complexes peuvent éventuellement être utilisées.
	Purge	⇨ **Démagnétisation** du support à l'aide d'un dégausseur approuvé par l'organisation (éventuellement, se référer à la liste des appareils approuvés par la NSA.
	Destroy	⇨ **Incinération** du support : le support doit être réduit en cendres. ⇨ **Déchiquetage - Désintégration** (éventuellement, se référer à la liste des appareils approuvés par la NSA). La norme DIN préconise pour les niveaux T2 une taille de débris de max. 2000 mm^2, T3 max. 320 mm^2, T4 max. 160 mm^2, T5 max. 30 mm^2, T6 max. 10 mm^2 et T7 max. 2.5 mm^2
Disques optiques CD/DVD/BD	**Clear**	Pas disponible.
	Purge	Pas disponible.
	Destroy	⇨ **Meulage** (abrasion). Suppression des couches contenant des informations du support à l'aide d'un dispositif commercial de meulage de disque optique. Cette technique n'est pas adaptée aux DVD et Blu-Ray (voir par.173). ⇨ **Incinération** du support : le support doit être réduit en cendres. ⇨ **Déchiquetage - Désintégration - Broyage** La NSA cite la taille maximum de débris de 2mm de côté pour les DVD et Blu-Ray et 5mm de côté pour les CD (voir par.174) (éventuellement, se référer à la liste des appareils approuvés par la NSA). La norme DIN préconise pour les niveaux O1 une taille de débris de max. 2000 mm^2, O2 max. 800 mm^2, O3 max. 160 mm^2, O4 max. 30 mm^2, O5 max. 10 mm^2, O6 5 mm^2 et O7 max. 0,2 mm^2.

Supports magnétiques ATA Hard Drives	**Clear**	⇨ **Réécriture** (écrasement) du support à l'aide d'un logiciel approuvé par l'organisation puis valider (vérification). Le niveau Clear doit se traduire par au moins une passe d'écriture avec une valeur de données fixe (ex.: tous des zéros). Facultatif : plusieurs passes d'écriture ou des valeurs plus complexes peuvent éventuellement être utilisées.
	Purge	Dans l'ordre de préférence : ⇨ **1. Commande Sanitize Device** : Si elle est prise en charge, utilisez l'une des commandes de l'ensemble de fonctionnalités ATA Sanitize Device (préférable à la commande Secure Erase). Une ou les deux options suivantes peuvent être disponibles : **1.a) Réécriture** (commande overwrite ext). Appliquez une passe d'écriture avec une valeur de données fixe (ex.: tous des zéros). Une seule passe d'écriture devrait suffire pour purger le support. Facultatif: au lieu d'une passe d'écriture, utilisez trois passes d'écriture, en tirant parti de l'option 'invert' afin que la deuxième passe d'écriture soit la version inversée du modèle spécifié. **1.b) Effacement cryptographique** (commande crypto scramble ext). Facultatif : Une fois l'effacement cryptographique appliqué avec succès, utilisez la commande overwrite pour écrire un passage de zéros ou un motif pseudo-aléatoire sur le support. Si cette commande n'est pas prise en charge, la procédure Secure Erase ou Clear peut également être appliquée après l'effacement cryptographique. ⇨ **2. Commande Secure Erase** : Si elle est prise en charge, utilisez la commande Secure Erase Unit, en mode 'enhanced'. ⇨ **3. Effacement cryptographique** via la classe de sous-système de sécurité Opal (voir par.132), si les commandes intégrées ne sont pas disponibles. Facultatif : Une fois l'effacement cryptographique appliqué avec succès, utilisez la commande overwrite pour écrire un passage de zéros ou un motif pseudo-aléatoire sur le support. Si cette commande n'est pas prise en charge, la procédure Secure Erase ou Clear peut également être appliquée après l'effacement cryptographique. ⇨ **4. Démagnétisation** du support à l'aide d'un dégausseur approuvé par l'organisation (éventuellement, se référer à la liste des appareils approuvés par la NSA. Il est recommandé d'endommager le disque dur en déformant ses plateaux internes avant de s'en débarrasser.

	Destroy	⇨ **Incinération** du support : le support doit être réduit en cendres. Le revêtement des plateaux internes doit être réduit en cendres et/ou les plateaux internes doivent être physiquement déformés par la chaleur. ⇨ **Déchiquetage - Désintégration** La NSA cite la taille maximum de débris de 2mm de côté et recommandé une destruction en lots avec d'autres périphériques de stockage (éventuellement, se référer à la liste des appareils approuvés par la NSA). La norme DIN préconise pour le niveau H1 un support mécaniquement/ Électroniquement inopérable, pour le niveau H2 un support endommagé et H3 déformé. Elle préconise une taille de débris de max. pour le niveau H4 de 2000 mm^2, H5 max. 320 mm^2, H6 max. 10 mm^2 et H7 max. 5 mm^2

Supports magnétiques SCSI Drives	**Clear**	⇨ **Réécriture** (écrasement) du support à l'aide d'un logiciel approuvé par l'organisation puis valider (vérification).
	Purge	⇨ **Commande Sanitize** (voir commande Sanitize Device pour ATA Hard Drives) ⇨ **Démagnétisation** du support à l'aide d'un dégausseur approuvé par l'organisation (éventuellement, se référer à la liste des appareils approuvés par la NSA. Il est recommandé d'endommager le disque dur en déformant ses plateaux internes avant de s'en débarrasser.
	Destroy	⇨ **Incinération** du support : le support doit être réduit en cendres. Le revêtement des plateaux internes doit être réduit en cendres et/ou les plateaux internes doivent être physiquement déformés par la chaleur. ⇨ **Déchiquetage - Désintégration** La NSA cite la taille maximum de débris de 2mm de côté et recommandé une destruction en lots avec d'autres périphériques de stockage (éventuellement, se référer à la liste des appareils approuvés par la NSA). La norme DIN préconise pour le niveau H1 un support mécaniquement/ Électroniquement inopérable, pour le niveau H2 un support endommagé et H3 déformé. Elle préconise une taille de débris de max. pour le niveau H4 de 2000 mm^2, H5 max. 320 mm^2, H6 max. 10 mm^2 et H7 max. 5 mm^2
Papier	**Clear**	Pas disponible.
	Purge	Pas disponible.
	Destroy	⇨ **Incinération** du support : le support doit être réduit en cendres. ⇨ **Déchiquetage - Désintégration** Le NIST préconise une taille de débris produits par les déchiqueteurs de 5 mm^2 max. et l'utilisation d'un tamis de 2,4 mm pour les désintégrateurs (éventuellement, se référer à la liste des désintégrateurs approuvés par la NSA et des déchiqueteurs approuvés par la NSA). La norme DIN préconise pour le niveau P1 une largeur de bande de max. 12 mm et pour P2 de 6 mm. Elle préconise pour les niveaux P3 une taille de débris de max. 320 mm^2, P4 max. 160 mm^2, P5 max. 30 mm^2, P6 max. 10 mm^2 et P7 max. 5 mm^2.

Supports Flash - USB Removable Drives - Memory Cards - Solid State Drives	**Clear**	⇨ **Réécriture** (écrasement) du support à l'aide d'un logiciel approuvé par l'organisation puis valider (vérification). Pour les Solid State Drives ATA & SCSI, USB Removable Media et Memory Cards : ⇨ **Réécriture** (écrasement) du support à l'aide d'un logiciel approuvé par l'organisation puis valider (vérification). Le niveau Clear doit se traduire par au moins une passe d'écriture avec une valeur de données fixe (ex.: tous des zéros). Facultatif : plusieurs passes d'écriture ou des valeurs plus complexes peuvent éventuellement être utilisées. Pour les ATA Solid State Drives (uniquement) : ⇨ **Commande Secure Erase** : Si elle est prise en charge, utilisez la commande Secure Erase Unit, en mode 'enhanced'.
	Purge	A) Solid State Drives ATA ⇨ **1. Commande Sanitize Device** : Si elle est prise en charge, utilisez l'une des commandes de l'ensemble de fonctionnalités ATA Sanitize Device (préférable à la commande Secure Erase), Une ou les deux options suivantes peuvent être disponibles : **1.a) Commande Block Erase** Facultatif : une fois la commande appliquée avec succès, écrivez des 1 binaires dans la zone adressable par l'utilisateur du support, puis effectuez un deuxième block erase. **1.b) Effacement cryptographique** (commande crypto scramble ext). Facultatif : Une fois l'effacement cryptographique appliqué avec succès, utilisez la commande block erase. Si cette commande n'est pas prise en charge, la procédure Secure Erase ou Clear peut également être appliquée après l'effacement cryptographique. ⇨ **2. Effacement cryptographique** via la classe de sous-système de sécurité Opal (voir par.132), si les commandes intégrées ne sont pas disponibles. Facultatif : Une fois l'effacement cryptographique appliqué avec succès, utilisez la commande block erase. Si cette commande n'est pas prise en charge, la procédure Secure Erase ou Clear peut également être appliquée après l'effacement cryptographique. B) Solid State Drives SCSI ⇨ **1. Commande Sanitize** : Si elle est prise en charge, utilisez l'une des commandes de l'ensemble de fonctionnalités SCSI

		Sanitize. Une ou les deux options suivantes peuvent être disponibles : **1.a) Commande Block Erase** **1.b) Effacement cryptographique** (commande cryptographic erase). Facultatif : Une fois l'effacement cryptographique appliqué avec succès, utilisez la commande block erase. Si cette commande n'est pas prise en charge, la procédure Secure Erase ou Clear peut également être appliquée après l'effacement cryptographique. ⇨ **2. Effacement cryptographique** via la classe de sous-système de sécurité Opal (voir par.132), si les commandes intégrées ne sont pas disponibles. Facultatif : Une fois l'effacement cryptographique appliqué avec succès, utilisez la commande block erase. Si cette commande n'est pas prise en charge, la procédure Secure Erase ou Clear peut également être appliquée après l'effacement cryptographique. C) Supports USB amovibles et Memory Cards - Pas disponible La plupart de ces supports ne prennent pas en charge les commandes intégrées ou si elles sont prises en charge, les interfaces ne sont pas prises en charge de manière standardisée.
	Destroy	⇨ **Incinération** du support : le support doit être réduit en cendres. ⇨ **Déchiquetage - Désintégration** La NSA cite la taille maximum de débris de 2mm de côté et recommandé une destruction en lots avec d'autres périphériques de stockage (éventuellement, se référer à la liste des appareils approuvés par la NSA). La norme DIN préconise pour les niveaux E3 une taille de débris de max. 160 mm^2, E4 max. 30 mm^2, E5 max. 10 mm^2, E6 1 mm^2 et P7 max. 0,5 mm^2.

Annexe B : Extraits du RGPD

Article 5 : **Principes relatifs au traitement des données à caractère personnel**

1. Les données à caractère personnel doivent être:

   a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);

   b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);

   c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

   d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude); 4.5.2016 L 119/35 Journal officiel de l'Union européenne FR.

   e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en oeuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

   f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui- ci est respecté (responsabilité).

Article 32 *:* **Sécurité du traitement**

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles

appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:

a) la pseudonymisation et le chiffrement des données à caractère personnel;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

4. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre.

Article 33 : **Notification à l'autorité de contrôle d'une violation de données à caractère personnel**

1. En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

2. Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

3. La notification visée au paragraphe 1 doit, à tout le moins:

   a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;

   b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

   c) décrire les conséquences probables de la violation de données à caractère personnel;

   d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

4. Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

5. Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.

Article 34 : **Communication à la personne concernée d'une violation de données à caractère personnel**

1. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).

3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:

   a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement;

b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser;

c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie.

Annexe C : Références

Références principales :

- « Guidelines for Media Sanitization » du 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 de la National Security Agency américaine (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)

Autres références :

- 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 » du « 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
(« Media Sanitization Guidelines » de l'IRS)
- 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
(« Ligne directrice sécurité de l'information & vie privée relative à l'effacement des supports d'information électroniques de la Sécurité Sociale »)
- 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
  et ses annexes 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