Gegevensbeschermingsautoriteit

Aanbeveling inzake technieken om gegevens op te schonen en gegevensdragers te vernietigen

WAARSCHUWING: dit document heeft als doel om aanvullende uitleg te verschaffen bij de geldende regels en stelt de verwerkingsverantwoordelijke niet vrij van zijn verplichtingen en verantwoordelijkheden die voortvloeien uit zowel de AVG als andere toepasselijke teksten. Rekening houdend met zijn behoeften en de risicoanalyse die hij uitvoert of overweegt, is het zijn keuze om een beroep te doen op het ene of het andere instrument en de ene of de andere methode. Hierbij houdt hij rekening met de ontwikkeling van de kennis en de technieken. De verschillende instrumenten en merken die in dit document worden genoemd, worden enkel als voorbeeld genoemd. De autoriteit doet geen uitspraken over feit of deze de AVG en andere voorschriften naleven, noch over de kwaliteit en de toepassing ervan.

INHOUDSOPGAVE

Samenvatting

De Gegevensbeschermingsautoriteit (GBA) vervult vele taken, waaronder de taak om burgers, bedrijven en overheidsactoren te informeren over bepaalde onderwerpen die verband houden met gegevensbescherming. Van deze onderwerpen zijn die met betrekking tot de 'veilige' verwijdering van gegevens of gegevensdragers zeker aan de orde van de dag.

Ongeacht hun beweegredenen, willen de verwerkingsverantwoordelijken deze ingreep goed uitvoeren, maar soms hebben ze er geen duidelijk zicht op wat een bevredigend resultaat is (met name wat betreft de bescherming van persoonsgegevens) en hoe een dergelijk resultaat kan worden bereikt.

De schaarste, of zelfs afwezigheid, op internationaal niveau van referentiedocumenten over dit onderwerp, zelfs op Europees en nationaal niveau, in combinatie met de wens van de GBA om de belanghebbende partijen een nuttige leidraad te bieden in de vorm van duidelijke, actuele en uitgebreide richtsnoeren, zijn de redenen voor deze aanbeveling.

In dit document worden de verschillende bestaande "opschoningstechnieken" voorgesteld (overschrijven, cryptografisch wissen, demagnetiseren, enz.) voor verschillende soorten dragers (HD, SSD, papier, enz.) waarmee het ofwel onmogelijk is om toegang te krijgen tot de gegevens op een beschermde drager (wissen zonder mogelijkheid tot reconstructie en codering) ofwel de vernietiging van de drager (zonder mogelijkheid tot reconstructie) wordt bewerkstelligd.

De aanbeveling bespreekt deze werkwijze (opschoning en vernietiging) ook op een bredere manier door de verschillende aspecten ervan in detail te beschrijven, zowel juridisch (in het bijzonder met betrekking tot de AVG) als technisch of organisatorisch, en onderzoekt de werkwijze van vóór de aankoopfase van de dragers tot aan de verificatie en de registratie van de resultaten.

Tot slot wordt in een samenvattende tabel, naargelang het type drager, een overzicht gegeven van de aanbevolen opschonings- en vernietigingstechnieken om het gewenste niveau van vertrouwelijkheid te bereiken.

Hoewel de principes en concepten die in dit document worden besproken van nature vrij duurzaam zijn, worden er enkele instrumenten, methodes of voorbeelden voorgesteld die, gezien de evolutie van de kennis en de technieken in het veld, wellicht sneller moeten worden bijgewerkt. Paragrafen of delen van de tekst waar het om kan gaan, worden voorafgegaan door de letters "\\" (dubbele backslash).

1. Inleiding

01. In het kader van zijn activiteiten wordt de verwerkingsverantwoordelijke[1] geconfronteerd met tal van situaties waarin hij ervoor moet zorgen dat de overdracht van gegevensdragers naar een andere omgeving niet leidt tot de ongeoorloofde bekendmaking van de gegevens op deze dragers.

Deze situaties waarin de verwerkingsverantwoordelijke een beslissing moeten nemen over de 'opschoning[2]' van gegevens houden vaak verband met het einde van de levenscyclus van de gegevens of van de dragers of met het hergebruik ervan in een andere beveiligingscontext[3].

02. Bijvoorbeeld:

- Verwijdering van buiten gebruik gestelde computerapparatuur (in de breedste zin van het woord[4]) ;
- Een kopieerapparaat voor herstelling opsturen;
- De opruiming van het papieren archief;
- Dossiers van de HR-afdeling sorteren;
- Computers aan een liefdadigheidsinstelling schenken;
- De teruggave van pc's in het kader van een leasingcontract;
- Het einde van het huurcontract voor een multifunctionele printer;
- Of de verkoop, na afschrijving, van bedrijfsdesktops en -laptops aan het personeel.

---

[1] Artikel 4.7 van de AGV definieert de 'verwerkingsverantwoordelijke' als een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking [] vaststelt.

[2] De Engelse uitdrukking 'data sanitization', die met deze behandeling overeenkomt, omvat het begrip 'grondige opschoning' (desinfectie, sanering), waarbij er geen enkel spoor van de gegevens wordt achtergelaten. Wij vertalen het eenvoudigweg als 'opschoning' van gegevens of gegevensdragers. Het Amerikaanse National Institute of Standards and Technology (NIST) definieert 'media sanitization' als een algemene term voor acties die worden ondernomen om gegevens die op dragers werden geschreven met gewone en buitengewone middelen onherstelbaar te maken.

[3] Wordt deze drager aan een derde partij gegeven of verkocht? Gooien we de drager weg of hergebruiken we hem intern? Als de drager als dusdanig wordt hergebruikt, moet de verwerkingsverantwoordelijke ervoor zorgen dat de drager wordt gebruikt in een beveiligingscontext die minstens gelijkwaardig is aan de context waarin de drager voordien werd gebruikt (bv.: een beleid inzake de toegang tot informatie dat vergelijkbaar is met het beleid dat in de oorspronkelijke omgeving van de drager werd gevoerd, of zelfs strenger was).

[4] Zoals pc's, servers, printers met harde schijven, verwijderbare dragers (USB-sticks, dvd's, externe harde schijven enz.) of mobiele apparaten (laptops, tablets, gsm's enz.).

03. De beweegredenen van de verwerkingsverantwoordelijke kunnen uiteenlopend zijn, zoals de noodzaak om gegevens die in zijn ogen van bijzonder belang zijn of die als 'vertrouwelijk' zijn geclassificeerd, de wens om zich van de concurrentie te onderscheiden, de vrees voor een sanctie[5] en/of de bereidheid om de geldende wetgeving na te leven.

In dit verband herinneren we eraan dat de verwerkingsverantwoordelijke, op straffe van sanctie[6], verplicht is om te voldoen aan artikel 5.1.e van de AVG. Dit artikel bepaalt dat persoonsgegevens 'worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is'. Als deze termijn wordt overschreden, moet de verwerkingsverantwoordelijke de gegevens dus anonimiseren of definitief vernietigen[7] (zie uitzonderingen in hetzelfde artikel).

04. We merken op dat, als de bescherming van gegevens die uit hun oorspronkelijke omgeving worden genomen, een groeiende zorg is voor allerhande organisaties, dit deels is omdat de bescherming ervan binnen deze organisatie toeneemt. Een strenger beleid voor de controle op de toegang tot de gegevens vermindert de kans dat een onbevoegde persoon direct toegang heeft tot de gegevens. Als gevolg hiervan zal deze persoon in de verleiding komen om zich tot andere kanalen te wenden om toegang tot de informatie te krijgen. Kanalen die minder inspanningen vergen, zoals gegevens oproepen op dragers die de gecontroleerde omgeving van de organisatie verlaten of die zich in een omgeving met een lager vertrouwelijkheids-/beveiligingsniveau bevinden.

05. Wat de geldende wetgeving betreft, onthouden we in het kader van dit document met name de Europese algemene verordening gegevensbescherming (AVG[8]) en in het bijzonder artikel 32 (zie bijlage B) over de beveiliging van de verwerking en

---

[5] We herinneren eraan dat de AVG voor een inbreuk op de bepalingen inzake de verplichtingen van de verwerkingsverantwoordelijke/verwerker, waaronder met name artikel 32 (beveiliging), voorziet in administratieve boetes tot 10 miljoen euro of, in het geval van een onderneming, tot 2 % van de totale wereldwijde jaaromzet van het voorgaande boekjaar, waarbij het hoogste bedrag van toepassing is (artikel 83.4.a van de AVG).

De hoogste administratieve boetes die tot op heden (11/2020) in het kader van de AVGD op het gebied van beveiliging werden opgelegd, bedragen nu al miljoenen euro's. Zo heeft de Britse toezichthoudende autoriteit (ICO), in overeenstemming met de andere Europese gegevensbeschermingsautoriteiten (in toepassing van het samenwerkingsmechanisme waarin de AVG voorziet, het 'één-loketmechanisme' of 'one-stop shop'), boetes opgelegd van bijna 21 miljoen euro aan de Marriott hotelgroepen bijna 22 miljoen aan British Airways voor beveiligingsinbreuken (overtreding van artikel 5.1.f en 32 - zie bijlage B).

[6] Zie bijvoorbeeld de door de Deense autoriteit opgelegde boete van 160.000 euro aan een taxibedrijf dat telefoongegevens van mensen die een taxi hadden gereserveerd, meer dan twee jaar had bijgehouden en de boete (200.000 euro) van deze zelfde autoriteit aan een meubelzaak omdat ze haar klantgegevens niet had gewist na de installatie van nieuwe computerapparatuur.

[7] Een tijdelijke organisatie moet gegevens verzamelen van een bepaald aantal leden om een petitie te kunnen indienen, waarbij de leden als echte mensen moeten worden geauthenticeerd. Na authenticatie moet deze organisatie, die geen enkel ander doel nastreeft, geen persoonlijke gegevens bewaren en moet ze daarom alle gegevens en het petitiemateriaal dat ze bevat, verwijderen, aangezien alleen het aantal gevalideerde ondertekenaars van belang is (verwijdering na het bereiken van de doeleinden).

[8] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG. De AVG is van kracht sinds 25 mei 2018.

artikelen 33 en 34 (zie bijlage B) over inbreuken in verband met persoonsgegevens. We vermelden eveneens artikel 5.1.f inzake de verplichting om persoonsgegevens te beschermen tegen onder meer de ongeoorloofde verwerking en het verlies ervan door middel van passende technische of organisatorische maatregelen.

06. We herinneren eraan dat artikel 4.12 van de AGV een inbreuk in verband met persoonsgegevens definieert als 'een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens'.

07. De verwerkingsverantwoordelijken en de verwerkers[9], die verplicht zijn om hun wettelijke verplichtingen na te komen, moeten bijgevolg alle gepaste technische en organisatorische maatregelen nemen om de vertrouwelijkheid van de persoonsgegevens[10] op de informatiedragers die ze willen opschonen, te garanderen.

08. De gegevensbeschermingsautoriteit (GBA), die verantwoordelijk is voor de naleving van de grondbeginselen van de bescherming van persoonsgegevens, waarbij de beginselen van beveiliging en vertrouwelijkheid[11] essentiële elementen zijn, wil met dit document de verwerkingsverantwoordelijken en de verwerkers helpen om deze beginselen na te leven.

09. Hiertoe worden er in dit document verschillende 'opschoningstechnieken' voorgesteld die ofwel de toegang tot de gegevens op een bewaarde drager onmogelijk maken (wissen zonder mogelijkheid tot herstel en versleuteling of encryptie), ofwel leiden tot de vernietiging van de drager (zonder mogelijkheid tot herstel).

10. De verwerkingsverantwoordelijke maakt zijn keuze uit deze reeks technieken, waarbij hij met name rekening houdt met het soort drager, het latere gebruik ervan en het vertrouwelijkheidsniveau van de gegevens.

Beperkingen

11. Enkel de technieken die leiden tot de 'opschoning' van de volledige drager of de vernietiging ervan worden in dit document besproken. Bestanden, mappen of indelingen specifiek wissen, wordt dus niet besproken.

---

[9] Artikel 4.8 van de AVG definieert 'verwerker' als 'een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt'.

[10] Artikel 4.1 van de AVG definieert 'persoonsgegevens' als 'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon'.

[11] De verwerkingsverantwoordelijke en de verwerker moeten de beveiliging en vertrouwelijkheid van de door hen verwerkte informatie garanderen. Ze moeten er met name voor zorgen dat enkel bevoegde personen toegang tot deze informatie hebben.

12. Volgende elementen worden niet in dit document besproken:

- Gevallen waarin de toegang tot dragers/gegevens, met het oog op het wissen of vernietigen ervan, niet mogelijk is, zoals opslag in de cloud of materiaal uit een PCaaS-contract[12]. Het is aan de verwerkingsverantwoordelijke om, voordat hij zijn cloudaanbieder of andere aanbieder van externe opslag kiest, te overwegen welke dienst deze aanbiedt om de gegevens veilig te verwijderen;

- Gegevens uit voertuigen verwijderen (navigatiegegevens, gegevens uit de synchronisatie van contacten met gsm ...) tijdens een herstelling in de garage of aan het einde van een leasingcontract bijvoorbeeld;

- Gegevens van gsm's verwijderen via specifieke software of gecentraliseerd beheer (bv.: Active Directory). Apple heeft een online procedure voor het verwijderen van persoonlijke gegevens voor de iPhone en iPad[13] online gezet, en Google voor Android-toestellen[14];

- Fabrieksinstellingen herstellen. De verwerkingsverantwoordelijke zorgt er echter voor dat het niet-vluchtige geheugen geen persoonsgegevens meer bevat[15];

- Het gebruik van besturingssysteemsregistratiesoftware[16] voor het herinstalleren van toestellen.

Doelgroep

13. Dit document is bedoeld voor verwerkingsverantwoordelijken en verwerkers[17] (zowel in de publieke als in de privésector), hun informatiebeveiligingsadviseurs en gegevensbeschermingsfunctionarissen (data protection officer of DPO in het Engels)

---

[12] 'Personal Computer as a Service', ook bekend als 'Device as a Service': een model voor levenscyclusbeheer van apparaten waarbij een organisatie maandelijks abonnementsgeld betaalt aan een leverancier om apparatuur en bijbehorende beheerdiensten te leasen.

Bv.: beschrijving van het PCaaS-aanbod van Dell https://www.delltechnologies.com/en-us/services/pc-as-a-service.htm en de optionele 'PCaaS Data Sanitization' dienst https://www.dell.com/learn/us/en/uscorp1/legal~dienst-omschrijvingen~en/documenten~pcaas-data-sanitisatie-sd-en.pdf

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

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

[15] Via deze functie keert het apparaat terug in de toestand waarin het zich bevond toen het de fabriek verliet (meestal gelijkwaardig aan de toestand toen het apparaat werd aangeschaft). Het betreft vooral het niet-vluchtige geheugen (dat niet wordt gewist als er geen stroom is) dat in kaarten en randapparatuur is ingebouwd. Zo kan het beheer op afstand, dat in een moederbord is geïntegreerd, bijvoorbeeld IP-adressen, gebruikersnamen, wachtwoorden of certificaten bevatten. Bijgevolg kan het, om deze gegevens te wissen, nodig zijn om met meerdere interfaces te communiceren om de status van het apparaat volledig te resetten. Dit kan de BIOS/UEFI-interface zijn[38] en de interface voor beheer op afstand.

[16] Software die een 'snapshot' (momentopname) van het besturingssysteem vastlegt dat op een apparaat is geïnstalleerd en het gebruikt bij soortgelijke apparaten (pc's, servers, gsm's,...).

[17] Volgens art. 32 van de AVG moeten zowel de verwerkingsverantwoordelijke als de verwerker passende technische en organisatorische maatregelen nemen om de constante vertrouwelijkheid van de verwerkingssystemen en -diensten te waarborgen. Dit document kan interessant zijn voor een verwerker die zijn diensten aan een verwerkingsverantwoordelijke wil aanbieden.

of elke andere persoon of organisatie die de toegang tot persoonsgegevens onmogelijk moet of wil maken.

Doelstellingen

14. Het doel van dit document is om :

- De doelgroep te helpen bij de formalisering en implementatie van de verschillende stappen om een weloverwogen keuze voor een geschikte 'opschoningstechniek' te maken;

- Informatie te verschaffen over de verschillende beschikbare methoden en technieken, de vertrouwelijkheidsniveaus ervan en de te verwachten resultaten, afhankelijk van het soort drager;

- De doelgroep te helpen om aan bepaalde vereisten van de AVG te voldoen, onder meer de vereisten met betrekking tot accountability (de verantwoordingsplicht uit artikel 5.2 van de AVG) en de vereisten met als doel om de ongeoorloofde bekendmaking van gegevens te voorkomen.

2. Voorlopige principes en concepten

15. De 'opschoning' of vernietiging van een gegevensdrager[18]:

- is toegestaan (volgens een interne procedure en/of toepasselijk recht);
- is gepast (onomkeerbaar, in overeenstemming met de risicoanalyse en de hieruit voortvloeiende vereisten inzake beveiliging/vertrouwelijkheid);
- verloopt onder toezicht van de verwerkingsverantwoordelijke (in geval van verwerking, zie sectie 3.1.3. voor bijkomende maatregelen);
- is gedocumenteerd (bewijs van vernietiging, zie deel 6);
- en wordt op het juiste moment uitgevoerd (rekening houdend met wettelijke termijnen, problemen in verband met opslag).

2.1. Inventarisatie en classificatie van informatie

16. Om te kunnen bepalen welke methode hij moet gebruiken om het risico op ongeoorloofde bekendmaking van de gegevens het best te beperken, moet de verwerkingsverantwoordelijke op de hoogte zijn van het volgende:

2.1.1. De aard en categorieën van de gegevens op de drager

17. Hij moet op zijn minst weten of er al dan niet persoonsgegevens op de drager staan en als dit het geval is, kan het ook nuttig zijn om:

- Aan te geven welke van deze gegevens 'gevoelig' zijn (die tot een bepaalde categorie behoren[19]) of betrekking hebben op strafrechtelijke veroordelingen of strafbare feiten (artikel 10 van de AVG);
- Een onderscheid te maken tussen gegevens die zijn gecodeerd[20], en/of gepseudonimiseerd[21];

---

[18] We merken op dat we de termen 'informatie' of 'gegevens' zonder onderscheid gebruiken, zonder te weten of de drager het eerste of het tweede of beide bevat. De gegevens zijn ruwe gegevens, die na analyse worden gebruikt om informatie te verkrijgen. Informatie wordt geïnterpreteerd en geeft betekenis aan de gegevens. Zo worden het gegeven '21122021' informatie als we weten dat het een datum betreft (21 december 2021).

[19] Art.9.1 van de AVG somt deze bijzondere categorieën van persoonsgegevens op. Het betreft gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

[20] Versleutelde gegevens zijn gegevens die onbegrijpelijk zijn gemaakt voor diegenen die niet over de juiste decoderingssleutel beschikken.

[21] Artikel 4.5 van de AVG definieert 'pseudonimisering' als 'het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen

- De gegevens in te delen naargelang het risico dat een ongeoorloofde bekendmaking van sommige of alle persoonsgegevens die zich op de drager bevinden, voor de betrokkene zou betekenen. Bij de inschatting van het risico raden we aan om rekening te houden met een bekendmaking van alle gegevens op een drager of in een apparaat. Dit komt vaak overeen met de realiteit op het terrein. Wanneer bijvoorbeeld een databaseserver wordt gehackt, worden meestal alle databases tegelijkertijd geopend.

18. De procedure die de verwerkingsverantwoordelijke heeft ingesteld om de juiste 'opschoningsmethode' te bepalen, kan immers geheel of gedeeltelijk zijn gebaseerd op de informatie die is ontwikkeld in par. 17.

19. Wij wijzen er hier op dat geanonimiseerde gegevens[22] niet meer voldoen aan de definitie van persoonsgegevens voor zover deze niet meer aan een geïdentificeerde of identificeerbare natuurlijke persoon kunnen worden gekoppeld.

20. De aard en categorieën van de gegevens moeten, in overeenstemming met een door de verwerkingsverantwoordelijke gevalideerd beleid, worden gekoppeld aan een techniek die het mogelijk maakt om het vereiste vertrouwelijkheidsniveau te bereiken (clear, purge of destroy - zie sectie 3.1.2.).

21. Het is daarom noodzakelijk om over een inventarisatie en classificatie van de informatie te beschikken[23].

2.1.2. De aard en kenmerken van de drager

22. Er zijn vele soorten (harde schijven, SSD's, magnetische banden, diskettes, IPhones, SD-kaarten, microfilms ...) en klassen (optisch, elektronisch, magnetisch, niet-overschrijfbaar, papier...) van dragers.

23. Het is logisch dat de zeer uiteenlopende technische en fysieke kenmerken van deze informatiedragers van invloed zijn op de keuze van de 'opschoningsmethode'. Trouwens, niet alle technieken zijn beschikbaar voor alle soorten en klassen van dragers. We denken bijvoorbeeld aan demagnetiseren van een papieren drager of overschrijven van een niet-overschrijfbare drager.

---

dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld'.

[22] Uittreksel uit overweging 26 van de AVG: [...] 'De gegevensbeschermingsbeginselen dienen derhalve niet van toepassing te zijn op anonieme gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.' [...]

[23] De inventarisatie van de activa en de classificatie van de informatie vormen een integraal onderdeel van een informatiebeheersysteem. Zo classificeert ISO 27002-maatregel 8.2.1 (Activabeheer) informatie in termen van waarde, gevoeligheid voor bekendmaking of wijziging, wettelijke vereisten of kriticiteit. NB: maatregel 6.5.2.1 van ISO 27701 (additional implementation guidance for 8.2.1 of ISO 27002) geeft, hoewel deze betrekking heeft op persoonsgegevens, weinig verduidelijking over een specifieke classificatie.

24. De classificatie van de gegevens en de aard van de drager zijn de belangrijkste criteria die worden gebruikt om de verwerking van de dragers en de te gebruiken methode te bepalen. Om deze keuze te maken, zal de classificatie als eerste filter dienen. De classificatie verschaft namelijk informatie over het gevoeligheids-/vertrouwelijkheidsniveau van gegevens en over het risico voor de betrokkenen in geval van ongeoorloofde bekendmaking. Overwegingen op basis van het soort en de klasse van drager worden in een tweede stap gebruikt.

25. Andere aanvullende factoren kunnen in aanmerking worden genomen, zoals kosten, milieueffecten, toekomstige bestemming[3] of de duur van het proces.

2.2. Stappen in de verwerking

26. Samenvattend kunnen de belangrijkste stappen in de 'opschonings-' en vernietigingsoperaties als volgt worden weergegeven:

A. Beleid (beveiliging en vertrouwelijkheid)

27. De eerste stap is de opstelling van een door de directie gevalideerd document waarin de volledige problematiek van 'data sanitization', inclusief alle bestaande gegevensdragers binnen de organisatie aan bod komt. Dit document beschrijft meer bepaald de context, de te bereiken doelstellingen, de goedkeuringsprocedure voor de 'opschoning' of vernietiging (inclusief back-ups) en de verschillende stadia van de verwerking. Ook worden de verantwoordelijkheden van de betrokken partijen (en van het management) voor de uitvoering, maar ook de controle van de verschillende stadia van de verwerking (keten van verantwoordelijkheden) in detail beschreven. Het is belangrijk dat elke fase, zonder uitzondering, onder de verantwoordelijkheid van een daartoe aangewezen persoon wordt geplaatst (zie bijv. par.240).

28. De verantwoordelijkheid van de betrokken partijen gaat verder dan de eigenlijke opschonings-/vernietigingsprocedure. Het kan nuttig zijn om te bepalen wie verantwoordelijk is voor reputatieschade en eventuele sancties als in een later stadium blijkt dat bepaalde gegevensdragers niet volgens de gevalideerde procedure werden verwerkt.

29. De auteurs van het document zorgen voor volledige 'top-down' ondersteuning van de hiërarchie. Vooral binnen dwingende gebieden zoals beveiliging en vertrouwelijkheid is de steun van de directie van essentieel belang. Zo niet is het beleid niets meer dan papier waarvan de inhoud niet wordt toegepast. Zorg ervoor dat de verantwoordelijkheid voor de 'opschoning' van de dragers wordt toegewezen aan een lid van de organisatie met een passend bevoegdheidsniveau.

30. De verantwoordelijke(n) voor de uitvoering moet(en) er ook voor zorgen dat het beleid bekend is bij alle betrokken actoren[24], dat het goed wordt uitgevoerd in de

[24] https://www.realwire.com/releases/More-than-half-of-enterprises-fail-to-communicate-data-sanitization-policies: Hoewel 96 % van de directeurs van de geraadpleegde organisaties een beleid inzake gegevensopschoning heeft, moet 31 % dit beleid nog naar het hele bedrijf communiceren. 20 % van de respondenten gelooft ook niet dat het beleid van hun organisatie volledig is. Algemeen gesproken, heeft 56 % geen beleid inzake gegevensopschoning dat regelmatig en doeltreffend naar de volledige organisatie wordt gecommuniceerd, waardoor het risico op mogelijke gegevensinbreuken toeneemt.

praktijk en zo nodig wordt bijgewerkt[25]. Het is belangrijk dat ook deze uitvoering van de instructies en de resultaten ervan worden gecontroleerd.

31. Uit een rapport[26] van het bedrijf Blancco blijkt dat de leemte tussen de creatie, de communicatie en de uitvoering van het beleid inzake drageropschoning gevoelige gegevens in gevaar kan brengen. De studie identificeert de volgende risico's:

- geen directe verantwoordelijkheid nemen om informaticamiddelen te wissen;
- materiaal laten rotten in opslagruimtes zonder het te hebben beveiligd;
- gegevens buiten de site wissen zonder volledig toezicht op de controleketen;
- vage aanduiding van de eigenaars van het beleid inzake gegevensopschoning.

B. Inventarisatie

32. Stel een volledige inventaris op van alle apparatuur die u hebt voor 'opschoning' of vernietiging hebt aangeduid. Bepaal het soort drager. Als u dit nog niet hebt gedaan, stelt u een inventaris op van de gegevens op de te verwerken gegevensdragers om deze volgens een relevante classificatie te sorteren, d.w.z.;

- afhankelijk van de aard van de persoonsgegevens die erop staan,
- en of de bekendmaking ervan een groot risico zou inhouden voor de rechten en vrijheden van de betrokkenen (zoals a priori het geval is voor de gegevens van speciale categorieën uit artikel 9 van de AVG).

33. Als de verwerkingsverantwoordelijke de inhoud van de informatiedrager niet kent (beschadigde drager of verouderde technologie, gebrek aan tijd of personeel enz.), zal hij de drager behandelen alsof deze persoonsgegevens bevat waarvan de bekendmaking een groot risico zou inhouden voor de rechten en vrijheden van de betrokkenen.

34. We herinneren er bovendien aan dat de AVG vereist dat de verwerkingsverantwoordelijken een register bijhouden van de verwerkingsactiviteiten (voor persoonsgegevens), met inbegrip van een beschrijving van de categorieën van verwerkte persoonsgegevens (artikel 30.1.c).

35. Als de verwerkingsverantwoordelijke van dit document een instrument van conformiteit wil maken dat verder gaat dan een eenvoudig register bevat het idealiter informatie zoals de aard van de drager die voor de verwerking werd gebruikt, de vernietigings- of opschoningstechniek en de aanleiding (vervanging of veroudering

[25] Net als alle andere beleidslijnen moet ook dit beleid deel uitmaken van een cyclus die eveneens een bijwerkingsfase omvat. Er kunnen vele redenen zijn waarom een beleid moet worden bijgewerkt. We denken aan een verandering in de beveiligings-/vertrouwelijkheidscontext binnen de organisatie of een technische evolutie (bijvoorbeeld coërcitiekracht van een degausser die aan de evolutie van de dragers moet worden aangepast, zie par. 0).

[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/

van de apparatuur, vertrek van een collega, bereikte doelstelling, verstreken wettelijke termijnen enz.).

C. Risicoanalyse

36. Het komt er in hoofdzaak op neer om het risico te bepalen dat een onbevoegd persoon toegang krijgt tot persoonsgegevens op de informatiedrager, wat een schending van de gegevens en een inbreuk op artikel 5.1.f en 32.2 van de AVG vormt (zie bijlage B). Houd ook rekening met de mogelijke beveiligingsgebreken die inherent zijn aan elke techniek[27].

37. We merken op dat de bezorgdheid van de AVG (en de GBA) betrekking heeft op de gevolgen van de bekendmaking van

- 'persoonsgegevens' (en niet van alle gegevens van de organisatie),
- gegevens over de betrokkene (d.w.z. de persoon op wie de gegevens betrekking hebben) en niet over de organisatie.

38. Hoewel de risicoanalyse een essentiële stap is, kan de verwerkingsverantwoordelijke, bijgestaan door zijn gegevensbeschermingsfunctionaris, ook een 'gegevensbeschermingseffectbeoordeling' uitvoeren (GBEB, artikel 35 van de AVG[28]), ongeacht of deze al dan niet verplicht is.

- De GBEB zal de verwerkingsverantwoordelijke helpen om de juiste vragen te stellen;
- Ze zal informatie bevatten die nuttig is om het register van verwerkingsactiviteiten in te vullen (artikel 30 van de AVG);
- Ze zal helpen om te voldoen aan de gegevensbeschermingsverplichting vanaf de ontwerpfase (artikel 25 van de AVG - gegevensbescherming door ontwerp). Aangezien het doel van de GBEB is om, ook vóór de verwerking, vast te stellen welke maatregelen er moeten worden genomen om de risico's voor de rechten en vrijheden van de betrokkenen aan te pakken, kan de GBEB in dit verband waardevolle hulp bieden.

39. Als uit de GBEB blijkt dat de verwerking nog steeds een hoog risico inhoudt, nadat de verwerkingsverantwoordelijke maatregelen heeft genomen om de vastgestelde risico's te beperken, moet de verwerkingsverantwoordelijke de gegevensbeschermingsautoriteit raadplegen voordat hij de verwerking uitvoert (artikel 36 van de AVG).

---

[27] Zoek op internet naar kwetsbaarheden die verband houden met de geselecteerde techniek of tool. U kunt bijvoorbeeld de CVE-lijst(Common Vulnerabilities and Exposures) raadplegen. Deze lijst bevat het grootste aantal publiek bekende kwetsbaarheden op het vla van cybersecurity. Andere bronnen van belang: Exploit Database, U.S. National Vulnerability Database (NVD) van het NIST, packet storm.

[28] Zie ook de aanbeveling uit eigen beweging met betrekking tot de gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging (CO-AR-2018-001) van de voormalige Privacycommissie (https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2018.pdf).

D. Beveiligingsmaatregelen

40. De volgende stap is de implementering van de technische en organisatorische maatregelen die eventuele geïdentificeerde risico's tot een aanvaardbaar niveau (voor de organisatie en voor de betrokkenen) beperken.

41. Deze stap omvat ook de identificatie van acties die snel en doeltreffend kunnen worden ondernomen om op een mogelijke schending van gegevens te reageren. Als persoonsgegevens tijdens de 'opschoning' van de dragers of zelfs nadat u de organisatie hebt verlaten, worden gecompromitteerd, kunt u nog steeds verantwoordelijk worden gesteld voor de schending (u blijft verantwoordelijk voor de verwerking tot het einde van de levenscyclus van de gegevens).

E. Evaluatie

42. Vervolgens moet er worden beoordeeld in welke mate de ondernomen acties het gestelde doel (verlies van vertrouwelijkheid voorkomen) hebben bereikt. Kies indien nodig een andere techniek.

F. Documentatie

43. De afzonderlijke stappen moeten in detail worden gedocumenteerd. Het accountabilitybeginsel van de AVG (verantwoordingsplicht uit artikel 5.2) houdt inderdaad in dat de verwerkingsverantwoordelijke moet kunnen aantonen dat hij de regels inzake gegevensbescherming naleeft. In het bijzonder moet hij het volgende documenteren: de motivering[29] van de gekozen methode, de beschrijving van de genomen maatregelen (stappen van de methode, inclusief verificatie) en het bewijs van de correcte uitvoering ervan (bijvoorbeeld door de afgifte van een document met alle informatie over de 'opschoning' of de vernietiging van de drager en, na een verificatiestap, het resultaat - mislukking of succes).

44. Met het oog op de transparantie ten opzichte van de betrokkenen bevelen wij de verwerkingsverantwoordelijke aan om, naast de informatie die krachtens de artikelen 13, 14 en 15 van de AVG moet worden verstrekt, ook bepaalde aanvullende informatie te verstrekken. Zo kan hij, naast de bewaartermijn van de gegevens (artikel 13.2.a, artikel 14.2.a en artikel 15.1.d), hen dus moeiteloos en met behulp van de reeds beschikbare documentatie concreter informeren over wat er met hun gegevens zal gebeuren zodra deze termijn is verstreken.

45. We raden de verwerkingsverantwoordelijke eveneens aan om dezelfde transparante houding aan te nemen in zijn communicatie met de betrokkene met betrekking tot artikel 17 van de AVG (recht op gegevenswissing).

[29] De motivering kan zijn gebaseerd op een afweging van de belangen van de verwerkingsverantwoordelijke en de rechten en belangen van de betrokkene en/of een beoordeling van het risico dat inherent is aan de verwerking, rekening houdend met de stand van de techniek en de kosten van de uitvoering in verhouding tot de risico's en de aard van de te beschermen persoonsgegevens.

G. Voorbeeld

46. Hieronder vindt u een meer concreet voorbeeld dat de belangrijkste stappen van een gegevensopschoning en/of vernietiging van een drager illustreert:

1. U overweegt om een aantal computers in uw organisatie te vervangen en deze te verkopen aan een bedrijf dat oude computers herstelt en ze vervolgens doorverkoopt.

2. U hebt tijdens de inventarisatiefase vastgesteld dat de dragers in de pc's harde schijven van het type ATA met een capaciteit van 500 GB zijn. Op de schijven staan de HR-dossiers van het personeel. Deze dossiers bevatten speciale categorieën van persoonsgegevens (gevoelige gegevens zoals lidmaatschap bij een vakbond of gegevens met betrekking tot ziekteverzuim).

3. Volgens uw beveiligings-/vertrouwelijkheidsbeleid moeten persoonsgegevens te allen tijde onder uw controle blijven. Gegevens mogen de fysieke en/of logische perimeter van uw bedrijf niet verlaten.

4. Tijdens de risicoanalyse vergelijkt u de verschillende methoden die aan deze doelstelling voldoen (wissen, opslaan, vernietigen).

5. Gezien de aard van de gegevens, de tijd die nodig is om de harde schijven te wissen, de mogelijkheid dat sommige gegevens toegankelijk blijven, de lage doorverkoopwaarde van de pc's bent u van mening dat het risico voor de organisatie (bv. reputatie, financieel, gerechtelijke procedures enz.) en het risico voor de rechten en vrijheden van de betrokkenen (bv. identiteitsdiefstal, oplichterij, phishing, chantage, discriminatie enz.) niet de moeite waard zijn.

6. Om het risico tot een aanvaardbaar niveau te beperken, kiest u daarom voor de fysieke vernietiging van de dragers en neemt u de volgende maatregelen:

A. Ongeacht of de vernietiging binnen de organisatie of door een externe partner wordt uitgevoerd, benoemt u de verantwoordelijken voor dit project: de operationele manager is een lid van de IT-afdeling terwijl de DP instaat voor de algemene supervisie. Deze persoon geeft aan het eind van de procedure een positief (of negatief) advies, met in het achterhoofd dat een definitieve beslissing, of het nu gaat om de keuze van de opschoningsmethode, het bereikte vertrouwelijkheidsniveau of het akkoord om de dragers vrij te geven/over te dragen, altijd bij de verwerkingsverantwoordelijke (de directie van uw organisatie) ligt. Het kan nuttig zijn om in het register van verwerkingsactiviteiten naar deze beslissing(en) te verwijzen;

B. U besluit dat de vernietiging binnen uw organisatie en in aanwezigheid van de projectmanager moet worden uitgevoerd;

C. U kiest[30] een gespecialiseerde externe partner, die kwaliteitsgaranties biedt en de vertrouwelijkheid naleeft en die met behulp van mobiele apparatuur de

[30] We herinneren eraan dat de verwerkingsverantwoordelijke een verantwoordelijkheid en verplichtingen heeft bij de keuze van verwerker (art. 28 van de AVG). De bekendheid van de leverancier vormt geen voldoende waarborg. Het schriftelijke, bindende contract tussen de

door u gekozen techniek kan implementeren. U controleert bij de dienstverlener of de technische kenmerken van de gebruikte apparatuur (bv. maximale grootte van de vernietigde restanten) voldoen aan de vereisten van uw beveiligings-/vertrouwelijkheidsbeleid.

7. U controleert of de vernietiging volgens de vastgestelde procedure is uitgevoerd en of de gegevens daadwerkelijk niet meer bruikbaar zijn. U verzamelt en bewaart het bewijs van de daadwerkelijke vernietiging van de dragers (voor alle dragers of voor elke drager afzonderlijk), evenals alle informatie die nuttig kan zijn om aan te tonen dat u de wettelijke verplichtingen naleeft.

2.3. In de beste van alle werelden

47. In een perfecte wereld hebt u al nagedacht over de 'veilige opschoning' van uw dragers, nog vóór u ze koopt, en hebt u de leverancier van deze dragers hierover reeds aangesproken. Voor organisaties die een bestek moeten opstellen, kan dit specificaties inhouden voor wiscommando's die in de hardware zijn ingebouwd (indien van toepassing - zie de artikelen 3.2.1.2. en 3.2.4.1.) en de bijstand van de leverancier en de levering van bepaalde gerelateerde informatie vereisen (bv. uitvoeringstijd, beschrijving van ondersteunde commando's en van de opties ervan of uitgesloten gebieden). Dit moet de geïnformeerde keuze voor een opslagdrager of een apparaat met een opslagdrager vergemakkelijken, op basis van de mogelijkheden inzake veilig wissen die het product biedt.

48. Ook het feit dat u op het moment van de aankoop over alle noodzakelijke technische informatie beschikt, zal niet enkel de 'inventarisatiefase' van de verwerking vergemakkelijken, maar ook de 'risicoanalysefase' waarin u de verschillende beschikbare wistechnieken vergelijkt op basis van de kenmerken van de drager.

49. Als u bijvoorbeeld op de hoogte bent van de coërciviteit[31] van een magnetische drager kunt u demagnetisering (zie sectie 3.2.3.) opnemen in of uitsluiten uit de lijst van beschikbare technieken. Of als de operationeel verantwoordelijke weet dat er twee verschillende soorten schijven (harde/magnetische en SSD/elektronische) in de pc's van de organisatie zitten, weet dat hij een onderscheid moet maken bij de keuze van de 'opschoningmethode'. \\ Opgemerkt moet worden dat beide soorten schijven tegelijkertijd in de apparaten aanwezig kunnen zijn (SSD-schijven zijn veel sneller maar duurder, ze worden vaak gebruikt voor het opstarten van de computer en gekoppeld aan een tragere magnetische harde schijf, die zorgt voor de opslag van het grootste deel van de gegevens).

---

verwerkingsverantwoordelijke en de verwerker zal ertoe bijdragen dat er een passend beveiligingsniveau is en zal zo nauwkeurig mogelijk de gekozen methode, de kenmerken ervan en de uit te voeren middelen vermelden.

[31] In deze context verwijst coërciviteit, in lekentaal, naar de kracht die een magnetisch veld nodig heeft om gegevens die op een magnetische drager zijn opgeslagen, te veranderen. Hoe hoger de coërciviteit, hoe moeilijker het zal zijn om de gegevens te wijzigen ('wissen') met behulp van demagnetisering.

3. De verschillende methoden en technieken

3.1. Inleiding

3.1.1. Belangrijke verduidelijkingen

50. Laten we beginnen met een belangrijke opmerking. Als u bestanden of mappen eenvoudigweg via de interface van uw apparaat wist (bijvoorbeeld door op de 'delete' toets op uw toetsenbord te drukken), verwijdert u enkel de pointers naar deze bestanden en niet de gegevens zelf. Door de pointers te wissen, maakt het apparaat het gebied waar de bestanden zich bevonden opnieuw beschikbaar om andere gegevens te schrijven. Bekijk het als volgt: het is alsof u, als u een hoofdstuk in een boek wilt wissen, alle verwijzingen naar dit hoofdstuk in de inhoudsopgave zou verwijderen. Maar als u door het boek bladert, vindt u de inhoud van het hoofdstuk toch terug.

51. Deze actie leidt er dus niet toe dat gegevens daadwerkelijk worden gewist en wordt bijgevolg niet in dit document opgenomen.

52. We merken ook op dat formattering eveneens geen gegevens wist, of het nu een snelle (quick) of volledige (full) formatering betreft[32].

3.1.2. Drie niveaus van vertrouwelijkheid

53. In de vakliteratuur worden de verschillende technieken vaak geclassificeerd volgens het gewenste vertrouwelijkheidsniveau (beveiliging) of, met andere woorden, volgens de kans om de oorspronkelijke gegevens te herstellen. We onderscheiden drie vertrouwelijkheidsniveaus die verband houden met drie klassen van technieken: clear (opschonen), purge (verwijderen) en destroy (vernietigen).

- De technieken van het niveau 'clear' zijn bedoeld om te voorkomen dat gegevens via speciale software worden hersteld. Deze technieken bieden een middelmatig vertrouwelijkheidsniveau (sommige gegevens kunnen worden hersteld als u over de nodige tijd, kennis en vaardigheden beschikt). Het betreft hier puur softwarematige technieken[33].

  Voorbeelden: het apparaat of de drager (gedeeltelijk) overschrijven met behulp van standaardcommando's (read and write) en resetten (fabrieksinstelling - vaak aanbevolen voor mobiele apparaten en routers/schakelaars).

- De technieken van het niveau 'purge' zijn bedoeld om te voorkomen dat gegevens met behulp van laboratoriumtechnieken worden hersteld. Deze technieken bieden een hoger vertrouwelijkheidsniveau en zijn geschikt als de drager opnieuw zal worden gebruikt in een andere beveiligings-/vertrouwelijkheidscontext dan de oorspronkelijke context. Het betreft hier softwarematige en fysieke technieken.

[32] Het belangrijkste verschil tussen de twee is dat een volledige formattering alle 'bad sectors' (beschadigde sectoren) controleert, waardoor deze actie langer duurt dan een snelle formattering.

[33] De term 'softwarematig' verwijst naar een techniek waarbij de mechanismen via software worden uitgevoerd.

Voorbeelden: overschrijven met behulp van specifieke commando's, demagnetiseren en cryptografisch wissen (zie sectie 3.2.4.).

■ De technieken van het niveau 'destroy' bieden het hoogste vertrouwelijkheids-/beveiligingsniveau. Gegevensherstel is inderdaad onmogelijk, zelfs met behulp van geavanceerde laboratoriumtechnieken. Deze technieken zijn gebaseerd op fysieke vernietiging en zijn daarom onverenigbaar met hergebruik van de drager. We merken op dat een techniek die de drager onbruikbaar maakt, niet van het niveau 'destroy' is als sommige gegevens nog steeds herstelbaar zijn.

Voorbeelden: verbranden, versnipperen en verpletteren.

54. Alle technieken in dit document behoren tot een van deze drie klassen. In bijlage A vindt u een tabel met de meest voorkomende soorten informatiedragers[34], samen met de verschillende technieken die erop kunnen worden toegepast afhankelijk van het vereiste vertrouwelijkheids-/beveiligingsniveau (clear, purge en destroy).

55. Het te bereiken vertrouwelijkheidsniveau en vervolgens de keuze van een techniek om dit niveau te bereiken, afhankelijk van het soort drager, is gebaseerd op een voorafgaande risicoanalyse.

Beschikbare technieken volgens het gewenste vertrouwelijkheidsniveau		
Clear	Purge	Destroy
• Overschrijven (standaardcommando's) • Resetten (fabrieksinstellingen herstellen, zie par.1212)	• Overschrijven (specifieke/geïntegreerde commando's) • Demagnetiseren • Cryptografisch wissen	• Verbranden • Versnipperen • Verpletteren • Desintegreren • Demagnetiseren

56. We splitsen de gebruikte methoden in twee groepen, afhankelijk van het feit of ze al dan niet leiden tot de fysieke vernietiging van de informatiedrager.

3.1.3. Verwerking zonder toezicht van de verwerkingsverantwoordelijke

57. Als de vernietiging of 'opschoning' van de drager (gedeeltelijk) wordt uitbesteed en dus niet onder de end-to-end controle van de verwerkingsverantwoordelijke wordt uitgevoerd, moet deze laatste zekerheid krijgen over het goede verloop van de verschillende fasen van de verwerking. Hiertoe bevelen we de volgende maatregelen aan:

■ Een beroep doen op ooggetuigen (gevalideerd door de dienstverlener en/of de verwerkingsverantwoordelijke);

[34] Voor een meer volledige lijst van dragers verwijzen we naar bijlage A van de 'Guidelines for Media Sanitization' in het 'NIST Special Publication 800-88'.

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

- Transport van dragers in beveiligde en afgesloten voertuigen. Hoewel de bescherming van een verzegeling niet absoluut is[35] (deze kan worden aangevallen door getrainde en uitgeruste aanvallers), kunnen ze daarmee uitgerust worden;

- Foto's maken of het gebruik van andere documentatietechnieken in elke fase van de verwerking;

- De implementatie van een non-stop continu proces met tijdelijke opslag;

- Procedures voor de controle en selectie van personeel dat bij de verwerking is betrokken;

- De afgifte van een attest van vernietiging door de verwerker (zie deel 6).

58. We raden aan om deze maatregelen in het contract tussen de verwerkingsverantwoordelijke en de verwerker op te nemen en om, in voorkomend geval, de elementen te beschrijven die het bewijs van vernietiging vormen (met name de gebruikte methode en het verkregen resultaat). In dit verband verwijzen we naar de bepalingen in een document[36] van de overheidsdiensten van New Brunswick (Canada).

3.2. De gegevensdrager wordt bewaard

59. Als inleiding op de verschillende technieken die in dit hoofdstuk worden geschetst merken we op dat, afgezien van een vernietigingsmethode die geen enkel deel van de drager intact laat (ongeacht de aard van de drager - papier, magnetisch of ander), het moeilijk is om te garanderen dat er op het volledige oppervlak geen enkel gegeven meer bruikbaar is, ook niet door gespecialiseerde laboratoria.

60. Als het risico dat er gegevens op de drager blijven staan of dat deze kunnen worden hersteld niet aanvaardbaar is voor de verwerkingsverantwoordelijke (rekening houdend met het risico voor de betrokkenen) gaat de voorkeur uit naar een methode die leidt tot de vernietiging van de drager (zie hoofdstuk 3.3.).

3.2.1. Wissen - overschrijven (overwriting)

61. 'Wissen' (ook wel overschrijven of herschrijven genoemd) bestaat erin dat een of meerdere reeksen (bepaalde, willekeurige of beide - al naargelang het gekozen protocol) gegevenselementen op dezelfde plaats als de gegevens die al op een gegevensdrager staan, worden geschreven. Dit verkleint de kans dat de overschreven gegevens kunnen worden hersteld.

62. Bijgevolg zou het beter zijn om te spreken van 'overschrijven' dan van 'wissen'[37]. De oorspronkelijke informatie of delen ervan bevinden zich mogelijk nog altijd op de drager, afhankelijk van de doeltreffendheid van deze 'overschrijving'.

---

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

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

[37] We merken op dat de term 'wissen' in de literatuur regelmatig bij dit onderwerp of in de beschrijving van software om digitale informatie op een veilige manier te verwijderen, wordt gebruikt.

63. Overschrijven is uiteraard niet van toepassing op dragers die van nature niet over- of beschrijfbaar zijn of die ten gevolge van schade (storing, gedeeltelijke vernietiging, slijtage) niet langer beschrijfbaar zijn.

64. Deze methode kan leiden tot twee niveaus van vertrouwelijkheid, namelijk 'clear' en 'purge'. Het bereikte niveau is afhankelijk van de combinatie van het soort drager waarop de gegevens staan, de gebruikte software (hardwaregerelateerd of autonoom) en de bijbehorende commando's (standaard of specifiek). De keuze en het juiste gebruik van de software en de commando's hangen dan weer af van het niveau van computerkennis van de persoon die verantwoordelijk is voor de procedure.

65. Schijven, of ze nu magnetisch (3.2.1.1.a) of elektronisch (3.2.1.1.b) zijn, hebben verschillende gebieden. Sommige van deze gebieden zijn a priori ontoegankelijk voor hardware-onafhankelijke software, het besturingssysteem of BIOS/UEFI[38]. Bijgevolg is het onmogelijk om alle opslaggebieden van de drager op te schonen.

66. \\ Voorbeelden van deze gebieden zijn:

- 'Bad/unmapped/corrupted' sectoren
- De 'over-provisioned' ruimte
- De 'trimmed' cellen
- De 'Device Configuration Overlay' (DCO)
- De 'Host Protected Area' (HPA)
- De 'Garbage Collection' (GC)

3.2.1.1. 'Clear' niveau - Software van derden

A. Magnetische harde schijven

67. \\ Het 'clear' niveau is mogelijk voor harde schijven (intern en extern) en diskettes door gebruik te maken van [39]hardware-onafhankelijke software van derden, zoals BitRaser, Blancco Drive Erasure, PartedMagic, Active@KillDisk of het open source DBAN-project. Deze software biedt vaak een breed scala aan verschillende protocollen (tot enkele tientallen) waardoor de ongeïnformeerde gebruiker vaak door de bomen het bos niet meer ziet.

---

[38] BIOS (Basic Input Output System) is firmware die op een geheugenchip is opgeslagen en wordt gebruikt om tijdens het opstartproces een hardware-initialisatie uit te voeren en om runtime-services voor besturingssystemen en programma's te leveren. Het is niet-vluchtig, wat betekent dat de parameters ervan worden opgeslagen en kunnen worden opgehaald, zelfs nadat de stroom is uitgeschakeld. UEFI is in wezen een verbeterde versie van BIOS.

[39] Zoek via uw gebruikelijke browser (de GBA gebruikt momenteel startpage.com) naar de termen 'data erasing' of 'data sanitization' om informatie te vinden over betalende software of freeware die dit soort functies biedt.

68. Wat deze verschillende protocollen onderscheidt, is enerzijds het aantal 'wisacties', d.w.z. het aantal opeenvolgende keren dat de schijfoppervlakte kan worden overschreven en anderzijds de laatste stap van het protocol, d.w.z. de controle van het effect van de overschrijving.

69. Bijvoorbeeld, het DoD 5220.22-M-protocol, dat zeer vaak wordt gebruikt en in alle toonaangevende software op de markt aanwezig is, beveelt aan om op alle adresseerbare ruimtes van de drager een binair karakter (in dit geval 0), dan de aanvulling (1) en ten slotte een willekeurig binair karakter (0/1) te schrijven. De verificatie van het resultaat vormt de laatste stap[40] van het protocol.

70. De versie van dit 'wisprotocol', die nog steeds als de norm wordt gezien en die in de meeste software van derden wordt geleverd, komt overeen met een verouderde versie van een norm van het Amerikaanse ministerie van Defensie (DoD)[41]. Het feit dat er drie keer kan worden overschreven, wat deze oude versie van het protocol voorschrijft, is meer dan genoeg om te voorkomen dat gegevens worden hersteld met behulp van op de markt beschikbare software ('clear' niveau). Alhoewel de doeltreffendheid van de wisprotocollen logisch lijkt en a priori is gekoppeld aan het aantal keer dat alle gebieden van de schijf worden overschreven, is deze logica echter achterhaald.

71. In de afgelopen jaren is er inderdaad een consensus ontstaan (NIST, HMG British Standard, BSI-GS, CMRR[42]) die bevestigt dat, zelfs als een schijf maar 1 keer wordt overschreven, de kans dat de gegevens op de schijf met behulp van softwarematige oplossingen worden gerecupereerd, niet toeneemt. Dit is het gevolg van technologische ontwikkelingen bij de dragers, met name in verband met de toename van hun dichtheid en dus hun capaciteit. Het is echter absoluut noodzakelijk dat er een controle-pass wordt uitgevoerd.

72. Als één schrijf-pass en één controle-pass voldoende zijn (behalve voor oud materiaal van vóór 2000 of van onbekende leeftijd), kunnen we dus concluderen dat een protocol dat 3 overschrijf-passes en één laatste controle-pass of een controle na elke schrijf-pass (zoals de oude versie van het zeer populaire DoD 5220.22-M) aanbiedt, eveneens voldoende is.

73. \\ Anderzijds kunnen protocollen die een hoger aantal passes aanbieden dan de schrijf-pass en de controle-pass bij de huidige stand van onze kennis en gebruikte technieken, als nutteloos worden gekwalificeerd[43], hoewel ze stricto sensu niet worden afgeraden

---

[40] In de literatuur spreken we eerder van pass. Zo is DoD 5220.22-M een 4-pass protocol, waarvan er 3 zijn gewijd aan het schrijven (wissen/overschrijven) en 1 aan de controle.

[41] Om precies te zijn, specificeert de huidige versie van dit protocol deze stappen niet meer. Deze softwareprogramma's verwijzen dus naar een oudere versie van het protocol. Voor meer informatie: https://www.blancco.com/blog-dod-5220-22-m-wiping-standard-method/.

[42] Uittreksel uit de 'Tutorial on Disk Drive Data Sanitization' (pag. 8) van het 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] Het Gutmann-protocol (1996), een herinnering aan een vervlogen tijdperk waarin de technieken die werden gebruikt om op harde schijven te schrijven, in theorie de mogelijkheid boden aan

74. Als u een software moet kiezen, geeft u best de voorkeur aan software die door een onafhankelijk laboratorium werd geanalyseerd en/of aan de vereisten van gespecialiseerde overheidsinstellingen voldoet.

75. \\ Hieronder vindt u bij wijze van voorbeeld enkele links naar actoren die zijn betrokken bij de evaluatie van producten of diensten op het gebied van gegevensvernietiging:

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

B. Flash-geheugendragers

76. In tegenstelling tot schijven en diskettes (zie het vorige punt 3.2.1.1.a), die magnetische dragers zijn, is het flashgeheugen een elektronische drager. Dit niet-vluchtige geheugen (het wordt niet gewist als de stroom wordt uitgeschakeld, in tegenstelling tot bijvoorbeeld RAM) kan elektrisch worden gewist en geherprogrammeerd.

77. Mede dankzij dalende prijzen, uitstekende prestaties en het feit dat er zich geen mechanische storingen voordoen, is het flashgeheugen in de loop van de jaren ontstaan als een technologie voor informatieopslag die steeds meer aanwezig is in elektronische apparaten en informatiedragers. Flashgeheugens zijn te vinden in gsm's, computers, digitale camera's, USB-sticks, geheugenkaarten, SSD's (zie hieronder), rekenmachines, medische apparatuur, hitech speelgoed enz.

78. \\ Wat meer specifiek de informatiedragers betreft, kunnen we twee belangrijke families van apparaten[44] met een flashgeheugen onderscheiden:

---

gespecialiseerde laboratoria om gewiste gegevens te recupereren, komt overeen met niet minder dan 35 overschrijf-passes en één controle-pass. Dankzij de harde schijven van vandaag is dit protocol, dat ook zeer ressource-intensief was, volledig achterhaald*. Het staat echter nog steeds op de lijst van protocollen die de belangrijkste softwarepakketten op de markt aanbieden. *Voor specialisten: dit protocol werd achterhaald op het moment dat de high-density schijven (met grote capaciteit) verschenen en de technologie op het vlak van harde schijven aan het eind van de jaren 90 een beweging maakte van een MFM/RLL-coderingstechniek naar PRML-technieken.

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

- Geheugenkaarten, waarvan er veel verschillende soorten zijn (bv.: Secure Digital SD, SDHC, SDXC, micro- en mini-SD, xD card, CompactFlash of MemoryStick). Deze zijn bedoeld voor kleine apparatuur zoals digitale camera's of gsm's;

- SSD's of Solid State Drives, die we kunnen vertalen als statische schijven, halfgeleiderschijven of gewoon elektronische schijven. Ze zijn beschikbaar in vele formaten en interfaces (PCIe, SATA, USB enz.). Bij wijze van taaluitbreiding wordt elk soort drager dat geen 'bewegende' onderdelen heeft (in tegenstelling tot bijvoorbeeld roterende magnetische harde schijven) soms SSD genoemd (RAM, ROM, Smard Cards, Flash).

NB: Sinds enkele jaren zijn SSD's allemaal gebaseerd op het flashgeheugen (vandaar de verwarring tussen de twee termen). Dit is echter niet altijd het geval geweest (RAM) en kan in de toekomst weer veranderen.

Solid-State Drives (SSD) van het type ATA of SCSI

79. We vermeldden reeds dat sommige gebieden van 'traditionele' harde schijven (3.2.1.1.a) ontoegankelijk zijn voor software van derden. In geval van het flashgeheugen is er nu een technologische bijzonderheid (zie par. 81 en 82) die verband houdt met dit soort drager en die dit toegangsprobleem in de verf zet.

80. Zelfs als zou het gebruik van onafhankelijke software voor 'elektronische' schijven het mogelijk maken om het 'clear' vertrouwelijkheidsniveau te bereiken via één overschrijf-pass (en a fortiori via meerdere passes) zal het gebruik van enkel deze software van derden bijgevolg als onvoldoende worden beschouwd om het gewenste doel te bereiken.

81. Ter informatie: de technologische bijzonderheid die in par. 79 wordt genoemd, is dat elk schrijfactiviteit op dit soort drager slijtage veroorzaakt. De fabrikant garandeert de componenten bijgevolg enkel voor een beperkt aantal schrijf-/overschrijfcycli (program/erase cyclus of p/e-cyclus). \\ Om de levensduur van flashgeheugens te verlengen en vroegtijdige slijtage van de cellen van sommige blokken[45] in vergelijking met andere[46] te voorkomen, hebben fabrikanten strategieën ontwikkeld zoals slijtageverdeling[47] (wear-leveling), specifieke bestandssystemen of de exclusieve toewijzing van opslagruimte aan de SSD-controller (overprovisioning)[48].

---

[45] Flashgeheugens zijn verdeeld in blokken die zijn opgebouwd uit pagina's. En deze pagina's bestaan dan weer uit geheugencellen. Schrijven en lezen gebeurt op paginaniveau. Voordat u echter op dezelfde plaats kunt overschrijven, moet u de geheugencellen resetten (wissen). En dit gebeurt enkel in volledige blokken (meestal bestaande uit enkele honderden pagina's). U moet dus het volledige blok naar een andere locatie kopiëren, het originele blok wissen en de inhoud van het oude blok met de nieuwe pagina's overschrijven.

[46] Vermijd in dit geval vroegtijdige slijtage van de blokken die vaak worden gewist in vergelijking met de blokken die gegevens opslaan en die niet of slechts lichtjes worden gewijzigd.

[47] Het principe is om gegevens die nooit of zelden worden gewijzigd, naar reeds versleten blokken te kopiëren om het aantal keer dat u een cel wist/overschrijft (en dus de slijtage) gelijkmatiger te verdelen.

[48] Door het gebruik van deze technieken en het feit dat er geen mechanische onderdelen zijn, bieden de huidige SSD-schijven garanties die gelijkwaardig zijn aan deze van harde schijven.

82. Het gebruik van deze technieken leidt er dus toe dat dezelfde gegevens naar meerdere locaties worden gekopieerd, inclusief gebieden waartoe onafhankelijke software geen toegang heeft (bijvoorbeeld bad blocks of wear-leveling blocks).

USB-sticks

83. USB-sticks, die bekendstaan onder vele andere namen[49] en waarvan het flashgeheugen van mindere kwaliteit is dan SSD's, hebben net als[50] geheugenkaarten voor kleine apparaten (bv. digitale camera's en gsm's) dezelfde beperkingen op het 'clear' niveau als SSD's.

C. Aandachtspunten

84. We herinneren eraan dat, in het kader van het overschrijven van dragers door software van derden ('clear' niveau):

- Het bereikte vertrouwelijkheidsniveau niet hoger is dan het 'clear' niveau;
- Deze software a priori geen toegang heeft tot alle schrijfgebieden van de drager;
- In geval van dragers met flashgeheugen het maken van kopieën van gegevensblokken de kans op herstel na het wissen, verhoogt.

85. Bijgevolg kan het, afhankelijk van het risico (vooral voor de betrokkenen), nodig zijn om het wissen te combineren met een andere techniek zoals versleuteling (zie par. 0) of fysieke vernietiging (zie hoofdstuk 3.2).

3.2.1.2. 'Purge' niveau - Geïntegreerde commando's

86. Opslagdragers hebben, al naargelang het model, verschillende interfaces (ATA, SCSI, NVMe). Deze interfaces worden gebruikt om te communiceren tussen hostsystemen en opslagapparaten en hebben, afhankelijk van het type, een verschillende set van commando's om de drager op te schonen.

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

[50] Lijst van soorten kaarten: https://en.wikipedia.org/wiki/Memory_card.

A. Disques durs magnétiques IDE/ATA

87. De meeste moderne harde schijven[51] van het type IDE/ATA[52] (inclusief PATA[53], SATA[53]...) worden geleverd met 'Secure Erase' commando's (sinds 2001 overal toegepast bij schijven van meer dan 15 GB). Secure Erase is de naam voor een set commando's die zijn opgeslagen in en beschikbaar zijn via de firmware[54] van de schijf.

88. Deze geïntegreerde commando's[55] wissen (overschrijven) alle gegevens op een schijf (inclusief sectoren die als beschadigd of ontoegankelijk zijn gemarkeerd) en maken het mogelijk om een 'purge' vertrouwelijkheidsniveau te bereiken.

89. \\ Software van derden is anders dan de software die in artikel 3.2.1.1. wordt besproken: HDDerase. Dit door het CMRR[42] ontwikkelde hulpprogramma bevat het 'Secure Erase' commando en kan daarom bepaalde opslagruimtes bereiken die niet toegankelijk zijn voor traditionele software van derden.

90. \\ We vermelden eveneens (binnen Linux) het online commandoprogramma 'hdparm' (NB: de programma's GParted en Parted Magic bevatten beide hdparm).

ATA-commando's - details

91. Tot nu toe hebben we het over het 'Secure Erase' commando gehad. Deze term wordt in de literatuur het meest gebruikt, maar regelmatig op een onnauwkeurige manier.

92. Binnen de ATA-standaardcommando's spreken we echter beter van 'Security Erase Unit'. Dit commando heeft twee modi, de standaardmodus 'Secure Erase' of 'Normal Erase' en de modus 'Enhanced Secure Erase' of 'Enhanced Erase'.

93. De 'Enhanced' modus zich richt op 'sectoren die als gevolg van een herindeling niet meer worden gebruikt'. Niet alle ATA-dragers ondersteunen echter deze modus.

94. Hoewel hun namen vergelijkbaar zijn, zijn er verschillen tussen de twee modi. Als de normale wismodus is geselecteerd, schrijft het commando 'Security Erase Unit' nullen (in binair) in alle gebieden waar de gebruiker gegevens heeft geschreven.

---

[51] Te onderscheiden van ATA SSD's (Solid State Drives).

[52] IDE is een standaardinterface, ook bekend onder het acroniem ATA, waarmee opslagapparaten (harde schijven, cd/dvd-drives ...) op het moederbord van een pc kunnen worden aangesloten. Hoewel de naam IDE vaak door elkaar met ATA wordt gebruikt, verwijst IDE eigenlijk alleen naar de elektrische specificaties van de signalen op de schijfkabel met 40/80 pinnen. ATA is de juiste naam voor de volledige specificatie.

[53] Toen SATA (Serial AT Attachment), de nieuwe ATA-standaard voor gegevenstransmissie, verscheen, werden de oude, bekende vormen van ATA met terugwerkende kracht omgedoopt tot PATA (Parallel ATA).

[54] Firmware of microsoftware is software die in de hardware is geïntegreerd en die instructies geeft die noodzakelijk zijn voor de werking van deze hardware.

[55] U kunt deze commando's (firmwarecommando's) niet op dezelfde manier op een harde schijf uitvoeren als bijvoorbeeld commando's in Windows vanaf de commandoprompt. Om 'Secure Erase' commando's uit te voeren, moet u een programma gebruiken dat directe toegang (I/O) biedt tot de ATA-interface van de harde schijf en die het mogelijk maakt om ATA-commando's naar dezelfde drive te sturen. Zelfs in dit geval zal de gebruiker het commando vaak niet manueel uitvoeren.

95. Als de verbeterde wismodus (enhanced) is geselecteerd, schrijft het commando 'Security Erase Unit' gegevens volgens vooraf gedefinieerde patronen en overschrijft het ook gebieden van de schijf die niet langer worden gebruikt of die als ontoegankelijk voor de gebruiker zijn gemarkeerd. De implementatie van deze modus is optioneel en wordt niet door alle fabrikanten ondersteund. Als deze modus echter beschikbaar is, krijgt hij de voorkeur op de standaardmodus.

96. Vanuit het oogpunt van de ATA-specificatie zijn dit twee verschillende commando's en is het soms moeilijk te weten welke de fabrikanten hebben geïmplementeerd. Ook als een drager zogezegd beide commando's implementeert, is het mogelijk dat hij beide met een enkele actie/versie associeert.

97. Recent is er een ander ATA-commando, 'Sanitize Device', verschenen. Ook dit commando is optioneel en bijgevolg niet op alle dragers geïmplementeerd. Net zoals het gelijkwaardige commando voor SCSI- en NVMe-interfaces[56] ('sanitize', zie par. 103) bestaat dit commando uit de drie modi 'crypto scramble', 'block erase' en 'overwrite'. Deze laatste modus probeert om alle gebieden met gebruikersgegevens op te schonen, inclusief defecte, reserve- en niet-toegewezen blokken.

- Overwrite[57] biedt de gebruiker de mogelijkheid om de overschrijfpass(es) te specificeren die hij wil toepassen (bv.: 3 passes, waarbij de 2e de optie 'invert'[57] gebruikt en de 3e identiek is aan de 1e)

- Crypto scramble initieert de actie 'cryptografisch wissen' die de encryptiesleutels van de drager wijzigt/verwijdert (zie sectie 3.2.4.) :

- Block erase wordt gebruikt om dragers met flashgeheugen te wissen.

98. De reeds genoemde online commandosoftware 'hdparm' integreert sinds 2016 (v.9.49) de functie 'Sanitize Device'. Deze software biedt een alternatief voor argwanende gebruikers die liever niet afhankelijk zijn van de besturingssoftware van de fabrikanten (en de implementatie van variabele kwaliteit) om hun dragers 'op te schonen'.

99. Bijgevolg raden we aan om, in volgorde van voorkeur en als ze door de gegevensdrager worden ondersteund, eerste het commando 'Sanitize Device' te gebruiken, vervolgens de 'Enhanced Secure Erase' modus en als laatste de 'Secure Erase' modus (de twee modi van het commando 'Security Erase Unit').

Secure Erase - verwarring

100. Zowel apparaten die gegevensdragers vernietigen (zie hoofdstuk 3.3.) als 'opschoningssoftware' kunnen de woorden 'secure erase' (veilig wissen) in hun naam bevatten of verkondigen dat ze veilig gegevens van een harde schijf wissen ('it securely erases data').

---

[56] Het 'Sanitize' commando voor de NVMe-interface heeft eveneens de drie modi 'block erase', 'crypto erase' en 'overwrite'.

[57] De 'overwrite ext'' modus vult het gebied voor gebruikersgegevens in met een patroon van vier bytes. De parameters in deze modus omvatten een aantal meervoudige overschrijvingen en de mogelijkheid om het patroon van vier bytes tussen opeenvolgende overschrijfpasses om te keren ('Invert' parameter).

101. Tenzij deze apparaten en software echter specifiek aangeven dat ze gebruikmaken van de 'Secure Erase' modus van het ATA-commando 'Security Erase Unit' is dit waarschijnlijk niet het geval. Met andere woorden, hoewel veel technieken voor het wissen van gegevens als 'veilig' kunnen worden beschouwd in tegenstelling tot een *eenvoudige 'delete'* bevatten ze niet allemaal het ATA-commando 'Secure Erase Unit'. Dit is echter de enige manier om het 'purge' vertrouwelijkheidsniveau te bereiken en om gegevens daadwerkelijk op een veilige manier te wissen.

102. Bij de keuze van de software moet de lezer hier dus de nodige aandacht aan besteden. \\ Bij wijze van voorbeeld vermelden we de software 'Secure Eraser' en het online commando 'SDelete'[58] (Secure Delete), dat Secure Erase lijkt te ondersteunen, maar dit in werkelijkheid niet doet. We herinneren eraan dat programma's zoals HDDErase (zie par. 88) of hdparm (zie par. 89) voorbeelden zijn van gratis programma's die gebruikmaken van Secure Erase.

B. Magnetische harde schijven van het type SCSI

103. De meeste harde schijven[59] van het type SCSI[60] (inclusief Parallell SCSI, Serial Attached SCSI, Fibre Channel, USB Attached Storage en SCSI Express[61]) ondersteunen (worden geleverd met) het 'sanitize' commando[62].

104. Net als bij het gelijkwaardige commando voor ATA- en NVMe-interfaces voert het 'sanitize' commando, met de optie 'overwrite', een of meerdere overschrijfpasses uit op alle adresseerbare gebieden[63] van de schijf. Dit commando maakt het 'purge' vertrouwelijkheidsniveau mogelijk. De twee andere opties ('block erase' en 'cryptographic erase') zijn ook vergelijkbaar met de ATA- en NVMe-interfaces.

---

[58] SDelete maakt deel uit van de reeks administratie- en probleemoplossingstools 'sysinternals' van Windows.
Uittreksel uit de documentatie van de 'sysinternals' tools: 'Secure delete applications overwrite a deleted file's on-disk data using techniques that are shown to make disk data unrecoverable, even using recovery technology that can read patterns in magnetic media that reveal weakly deleted files. SDelete (Secure Delete) is such an application. You can use SDelete both to securely delete existing files, as well as to securely erase any file data that exists in the unallocated portions of a disk (including files that you have already deleted or encrypted).'

[59] Te onderscheiden van SCSI SSD's (Solid State Drives).

[60] SCSI (Small Computer System Interface) is een reeks standaarden die de fysieke verbinding en gegevensoverdracht tussen computers en randapparatuur beschrijven. SCSI-standaarden definiëren commando's, protocollen, elektrische, optische en logische interfaces.

[61] Sommige interfaces voldoen niet aan alle SCSI-standaarden, maar implementeren desondanks het SCSI-commandoprotocol.

[62] Voor een volledige beschrijving van SCSI-commando's: https://www.t10.org - SCSI Block Commands(T10/BSR INCITS 506 - Rev.22 15/09/2020)

[63] Gebied dat een uniek adres krijgt (met vermelding van de locatie op de drager) zodat het mogelijk is om er te lezen/schrijven (sector).

C. Gemeenschappelijke opmerkingen voor harde schijven van het type ATA en SCSI

105. Het resultaat van deze specifieke commando's, die afkomstig zijn van de schijfbeheerder[64] zelf, is a priori betrouwbaarder[65] dan het gebruik van software van derden (zie artikel 3.2.1.1.). De fabrikant heeft namelijk een perfecte kennis van zijn hardware en deze commando's houden rekening met alle schrijfbare gebieden[66] van de drager die niet zichtbaar zijn voor het besturingssysteem en BIOS/UEFI. Deze techniek is ook sneller dan software van derden. Bovendien zijn de geïntegreerde commando's ook minder gevoelig voor malware-aanvallen dan software van derden.

106. Als u weet dat de implementatie van het 'sanitize' commando in enkele gevallen problematisch was[65] en dat de wisactie via software van derden of via een geïntegreerd commando wordt uitgevoerd, hebt u alle reden om de correcte uitvoering van de instructies te controleren[67], d.w.z. of het commando daadwerkelijk de verwachte wisactie heeft uitgevoerd.

D. Solid State Drives (SSD's)

107. Net als bij magnetische harde schijven leveren de meeste fabrikanten doorgaans software die met hun SSD-dragers (ATA-, SCSI- en NVM Express-interfaces) kunnen worden gebruikt, inclusief een firmware-updatetool[54], de commando's voor 'veilig wissen'[68] en eventueel een tool om de drager te clonen.

108. \\ Bij wijze van voorbeeld vindt u hieronder links naar de SSD-tools van enkele bekende leveranciers:

- Samsung Magician (veilig wissen is beschikbaar in de sectie Data Management);
- Western Digital SSD Dashboard (secure erase en sanitize zijn beschikbaar in de sectie Drive Management);

---

[64] Tool om gebruikelijke administratietaken op schrijven uit te voeren, zoals formatteren, beheer van indelingen (aanmaken, verwijderen, aanpassen ...), de letter van een drive wijzigen, enz.

[65] Het lijkt alsof in sommige gevallen (waarvan de frequentie moeilijk te beoordelen is) en in ieder geval voor ATA-interfaces, de fabrikanten deze commando's niet of niet altijd correct implementeren http://www.hddoracle.com/viewtopic.php?f=56&t=1412.

[66] De meeste harde schijven ondersteunen de creatie van verborgen opslagruimtes die niet bekend zijn bij het besturingssysteem of BIOS. Twee voorbeelden zijn de Host Protected Area (HPA) en de Device Configuration Overlay (DCO) https://site.aleratec.com/blog/2011/03/31/remember-hpa-dco-sanitizing-hard-drives/.

[67] Software van derden biedt over het algemeen de mogelijkheid om één controle-pass te integreren. De veiligste optie blijft echter het gebruik van gespecialiseerde software, zoals een data recovery tool of een disk editor.

[68] In de praktijk zal bij de uitvoering van het 'secure erase' commando de SSD-controller gelijktijdig alle opslagcellen onder spanning zetten en deze resetten (waarbij de opgeslagen elektronen worden vrijgegeven). Het commando schrijft dus niets op de drager.

Seagate : SeaTools SSD GUI (met grafische interface - secure erase is beschikbaar in de sectie Operations - Maintenance - Erase) en SeaTools SSD CLI (zonder grafische interface - het commando 'sanitize' biedt de opties 'block erase' en 'overwrite');

- Lenovo ThinkPad Drive Erase Utility : dit programma reset de cryptografische sleutel van ondersteunde harde schijven (HDD's) (Full Disk Encryption - FDE, zie artikel 3.2.4.2.) en wist de SSD-schijf (Solid State Drive).

109. De website van de fabrikant is de eerste plaats waar u een geschikte tool kunt vinden om gegevens veilig te wissen. Deze tools bieden echter niet altijd de mogelijkheid om geïntegreerde commando's uit te voeren. Of als ze dit wel doen, is de kwaliteit van het resultaat van de uitvoering onzeker.

110. In het licht van de kenmerken van de SSD's en het bovenstaande en om een voldoende beveiligings-/vertrouwelijkheidsniveau te bereiken, raden we dan ook aan om een extra 'opschoning' uit te voeren met behulp van een andere techniek[69].

3.2.2. Anonymisation

111. \\ Anonimisering, waardoor het onmogelijk is om de betrokkenen opnieuw te identificeren, wordt naarmate de toegang tot steeds grotere en online databanken toeneemt, steeds moeilijker.

112. \\ Daarom gaan we er niet van uit dat deze techniek een voldoende vertrouwelijkheids-/beveiligingsniveau biedt. En dit los van de middelen (tijd en mankracht) die nodig zijn voor de uitvoering, wat het voordeel ervan nog verder vermindert in vergelijking met andere technieken.

113. Als anonimisering reeds werd uitgevoerd, moet de geldigheid van de gebruikte methode vóór elke overdracht van een informatiedrager worden onderzocht en moet er, bij voorkeur, een heridentificatietest worden uitgevoerd. Deze laatste wordt idealiter uitgevoerd door personeel dat onafhankelijk is van het personeel dat de anonimisering heeft uitgevoerd (wat des te meer gerechtvaardigd is als de drager grote hoeveelheden gegevens bevat).

114. Ten slotte mogen we niet vergeten dat het wijzigen van gegevens op een drager (bijvoorbeeld waarden in een databank) er niet noodzakelijkerwijs toe leidt dat deze waarden worden verwijderd (de gegevens worden niet gewist).

3.2.3. Demagnetiseren - degaussen (degaussing)

115. Bij demagnetisering wordt een magnetische kracht toegepast die voldoende sterk is om alle gegevens van een bepaalde magnetische drager te wissen. De doeltreffendheid van deze techniek is gelinkt aan de relatieve sterkte van de magnetische kracht van het demagnetiseerapparaat en de magnetische eigenschappen van de gegevensdrager.

[69] In dit geval voor ATA wordt een block erase gevolgd door een overwrite, een cryptographic erase en een secure erase. Bij SCSI voeren we een sanitize-block erase uit na een cryptographic erase. Bij NVM Express tenslotte starten we het commando 'user data erase' op na een cryptographic erase.

116. Hoewel het een belangrijke techniek is om magnetische dragers op te schonen, zult u uit het bovenstaande kunnen afleiden dat demagnetiseren, gezien de aard ervan, niet doeltreffend is op de meeste flashgeheugenapparaten, inclusief SSD's. Dit komt omdat deze gebruikmaken van geïntegreerde schakelingen om gegevens op te slaan in plaats van ze magnetisch op te slaan. Demagnetiseren wordt eveneens niet gebruikt bij gemengde gegevensdragers die minstens bestaan uit een niet-magnetische, niet vluchtige drager.

117. We herinneren hier aan de noodzaak om een correcte inventaris van dragers op te stellen, met vermelding van het soort drager en de bijbehorende opschoningsmethode. Als er namelijk tijdens de demagnetisering geen onderscheid wordt gemaakt tussen SSD's en harde schijven, blijven de gegevens die op de SSD's zijn opgeslagen intact.

118. We mogen niet vergeten dat sommige apparaten beide soorten dragers (elektronisch en magnetisch) kunnen bevatten. Als u demagnetisering voor deze hybride apparaten overweegt, moet u eveneens een opschoningstechniek toepassen die geschikt is voor de elektronische opslagdrager.

119. De ideale inventaris (zie hoofdstuk 2.3.) vermeldt moet de demagnetiseringskracht die nodig is om de drager 'op te schonen', m.a.w. de coërciviteit[31]. Coërciviteit kan immers moeilijk te bepalen zijn op basis van de informatie op het productetiket alleen. Bijgevolg kan het nuttig zijn om op voorhand de fabrikant van het apparaat te raadplegen.

120. Het is belangrijk om systematisch te controleren of het juiste vermogen op de drager wordt toegepast (een te hoog vermogen kan de drager onbruikbaar maken, bij een te laag vermogen bestaat het risico dat de drager niet correct wordt 'opgeschoond'), vooral omdat het benodigde vermogen met de technologie evolueert. De coërciviteit van dragers neemt namelijk toe naarmate de dichtheid/capaciteit stijgt[70]. Nieuwere dragers met een grotere capaciteit vereisen daarom krachtigere degaussers.

121. Afhankelijk van de intensiteit van de degaussing kan de drager onbruikbaar worden gemaakt. In dit geval wordt demagnetisering ook een vernietigingstechniek (zie sectie 3.3.5.). In verband hiermee kan demagnetisering eveneens worden overwogen in geval van een beschadigde drager die niet meer kan worden 'opgeschoond' via een methode waarbij de drager moet werken.

122. Aangezien niet alle degaussers op dezelfde manier werken, moet u ervoor zorgen dat de operators die ervan gebruikmaken, op de hoogte zijn van hun specifieke werkingsmodi. Sommige apparaten vereisen bijvoorbeeld slechts een pass, terwijl andere meerdere passes vereisen. Sommige modellen vereisen dat de informatiedragers uit elkaar worden gehaald en andere niet.

---

[70] Om de magnetische opslagdichtheid te verhogen, moet de oppervlakte die aan elk bit wordt toegewezen, worden verkleind. Dit vereist het gebruik van magnetische materialen met een verhoogde coërciviteit om te voorkomen dat de informatie wordt gewist als gevolg van interacties met nabijgelegen bits. Dit maakt de registratie van bits moeilijker omdat het een hoger magnetisch veld vereist. Dit verklaart ook waarom het met de toename van de capaciteit moeilijker wordt om de betreffende dragers te demagnetiseren (het benodigde vermogen neemt toe).

123. Ter informatie, het NSA publiceert een bijgewerkte lijst van degaussers waarmee u magneetbanden en magnetische harde schijven op een veilige manier 'opschoont'. De in dit document genoemde apparaten[71] worden vermeld met de coërciviteit van het opslagapparaat dat ze veilig kunnen wissen.

3.2.4. Cryptografisch wissen (cryptographic erase - crypto-erase - CE)

124. Dit is de laatste van de 'opschoningstechnieken' waarbij de drager wordt bewaard. Hoewel het een techniek op zich is, wordt ze vaak als aanvulling op andere technieken gebruikt.

125. Het doel van de in dit document vermelde methoden is om de gegevens op een drager definitief ontoegankelijk te maken. De versleuteling[72] van deze gegevens kan op het eerste gezicht eveneens dit doel bereiken door de gegevens onbegrijpelijk te maken voor iedereen die geen toegang heeft tot de decoderingssleutel. Het is deze extra stap, namelijk de definitieve vernietiging van de sleutel die decodering mogelijk maakt, die het verschil vormt tussen encryptie en cryptografisch wissen en waardoor deze techniek een 'opschoningstechniek' wordt.

126. Versleuteling is natuurlijk zeer nuttig in veel andere situaties op het gebied van gegevensbescherming. Het is in het bijzonder een belangrijke maatregel om een verlies aan vertrouwelijkheid tegen te gaan in geval van diefstal, ongeoorloofde toegang of verlies van de drager. Versleuteling wordt in de AVG[73] vermeld als mogelijk middel om de risico's voor de betrokkenen te beperken door in sommige gevallen vrij te stellen van de mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkenen (art.34.3.a van de AVG)[74]. Dit valt echter buiten de analyse die het voorwerp uitmaakt van dit document.

3.2.4.1. Geïntegreerde commando's

127. Zowel de commandogroepen ATA/IDE ('crypto scramble' optie) als SCSI ('cryptographic erase' optie) die in artikel 3.2.1.2. worden besproken, bevatten specifieke commando's die de actie 'cryptografisch wissen' van de gegevens op de

---

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

[72] De versleuteling van een informatiedrager is meestal gebaseerd op een authenticatiesleutel en een encryptiesleutel. De encryptiesleutel is de sleutel waarmee gegevens daadwerkelijk worden versleuteld en ontsleuteld. De authenticatiesleutel is gebaseerd op het wachtwoord of de passphrase van de gebruiker en wordt gebruikt om de encryptiesleutel te decoderen (die op zijn beurt de gegevens ontsleutelt). Met deze aanpak op twee niveaus kan de gebruiker dus zijn wachtwoord wijzigen zonder dat hij al zijn gegevens opnieuw moet versleutelen. De encryptiesleutel blijft namelijk ongewijzigd (deze wordt opnieuw versleuteld met het nieuwe wachtwoord van de gebruiker).

[73] Versleuteling wordt vermeld in art. 6.4.e (rechtmatigheid), art. 32.1.a (beveiliging) en art. 34.3.a (mededeling aan de betrokkene) van de AVG.

[74] Artikel 34.3.a van de AVG: 'De in lid 1 bedoelde mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld: a) de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;'

drager activeren. Ze worden echter niet in alle dragers van alle fabrikanten geïmplementeerd.

128. Als deze techniek wordt gebruikt, beveelt het NIST (guidelines SP.880-88r1) aan om de drager vervolgens te overschrijven, hetzij via de andere geïntegreerde commando's, hetzij met behulp van software van derden (zie artikel 3.2.1.1.). Dit verkleint het potentiële risico dat de drager nog een toegankelijke decoderingssleutel bevat na een ondoeltreffende vernietiging of als er geen vernietiging werd uitgevoerd.

129. NB: we hebben gezien (par. 0) dat er 2 afzonderlijke ATA-commando's met vergelijkbare namen bestaan die verschillen vertonen op het vlak van overschrijfacties (Secure Erase en Enhanced Secure Erase). Als deze worden gebruikt om een drager te versleutelen, zullen ze hetzelfde resultaat opleveren, ongeacht welke u gebruikt.

3.2.4.2. SED's

130. Heel wat informatiedragers bevatten ingebouwde 'zelfversleutelingsmechanismen'. Deze worden over het algemeen aangeduid als 'hardware-based full disk encryption' (FDE) en meer specifiek als 'self-encrypting devices' (SED's[75]), als het harde schijven of Solid State Drives (SSD's) betreft. Zelfversleuteling houdt in dat de drager alle gegevens die op de drager worden geschreven, zal versleutelen voordat ze worden geschreven en zal ontsleutelen op het moment dat ze worden gelezen[76]. De encryptiesleutel is enkel bij de drager bekend, maar kan door een geautoriseerde gebruiker worden gewijzigd. Als de sleutel wordt gewijzigd, worden alle gegevens die eerder met de oorspronkelijke sleutel werden geschreven, onleesbaar. De wijziging van de sleutel kan dus worden gebruikt om de gegevens te 'vernietigen' door ze onherstelbaar (onleesbaar) te maken.

131. De techniek van cryptografisch wissen kan daarom eenvoudig en vooral snel SED's worden uitgevoerd omdat de versleutelingsfase reeds werd uitgevoerd.

[75] Bij wijze van voorbeeld vindt u hier de link naar de gedetailleerde technische handleiding (EN) voor de beveiligingsimplementatie en volledige encryptie van SED-modellen van het merk Seagate:

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

[76] In de praktijk worden de gegevens bij FDE-dragers altijd versleuteld (via de encryptiesleutel) als ze op de drager worden opgeslagen, zelfs als er geen wachtwoord is ingesteld (bijvoorbeeld in geval van een nieuwe schijf of een gebruiker die geen wachtwoord wil instellen).

132. SED's die aan de OPAL[77]-norm van de Trusted Computing Group[78] voldoen, gebruiken het AES[79] (Advanced Encryption Standard)-versleutelingsalgoritme met sleutels van 128 of 256 bits. Voor deze dragers wordt cryptografisch wissen 'PSID Revert' genoemd. Het vereist namelijk, voordat het eigenlijke commando wordt gestart en de sleutels worden gewist, dat er een unieke identifier voor elke drager wordt ingevoerd: de PSID[80] of Physical Security ID.

3.2.4.3. Beveiligingskwetsbaarheden bij SED's

133. \\ Een ander aandachtspunt is de publicatie van een studie die een beveiligingskwetsbaarheid in het ingebouwde 'zelfversleutelingsmechanisme' van SSD's aan het licht brengt en de mogelijkheid biedt om deze versleuteling te omzeilen als u fysiek toegang hebt tot de informatiedrager.

134. Afhankelijk van de risicoanalyse geeft u best de voorkeur aan een softwareversleutelingsoplossing, zoals de open source software VeraCrypt (voor Windows, Mac OSX en Linux) en LUKS (Linux Unified Key Setup), boven een hardware-oplossing.

135. We wijzen erop dat sommige fabrikanten rekening houden met deze mogelijke inbreuken in verband met SSD's en waarschuwingen formuleren (bv. : Samsung).

3.2.4.4. Aandachtspunten

136. Deze techniek (versleuteling gevolgd door cryptografisch wissen) kan op andere dragers worden gebruikt (die geen SED's zijn of geen ingebouwde commando's ondersteunen), door gebruik te maken van versleutelingssoftware van derden en door de sleutels permanent te verwijderen zodra de versleuteling is uitgevoerd. De versleutelingsfase van de drager kan echter een zeer tijdrovend proces zijn (enkele uren, afhankelijk van de capaciteit van de drager, de schrijf-/leessnelheid en het rekenvermogen dat aan de bewerking is toegewezen).

137. 'On-the-fly' versleuteling van SED's daarentegen maakt de techniek van cryptografisch wissen zeer snel en verhindert vrijwel onmiddellijk de toegang tot de gegevens die zich op de drager bevinden.

138. In geval van cryptografisch wissen, moet u er bovendien voor zorgen dat er vóór de 'on-the-fly' versleuteling geen persoonsgegevens werden geschreven omdat deze niet beschermd zullen worden door cryptografisch wissen.

---

[77] Set van specificaties voor zelfversleutelende drives die TCG heeft ontwikkeld om de vertrouwelijkheid van opgeslagen gegevens te beschermen.

[78] TCG is een groep van bedrijven die is opgericht om standaarden en technologieën voor trusted computing te ontwikkelen en te promoten. Deze standaarden en technologieën moeten hardwarefabrikanten in staat stellen om te controleren wat er op hun systemen kan werken en om de uitvoering van niet-gevalideerde (niet-ondertekende) software te weigeren. Leden van TCG zijn onder andere Western Digital, Samsung, Seagate, HP, Toshiba, Lenovo, Dell en Microsoft.

[79] De AES versleutelt niet-gecodeerde tekst, in blokken van 128 bits tegelijk, met behulp van symmetrische sleutels van 128, 192 of 256 bits. Een symmetrische sleutel is een sleutel die zowel wordt gebruikt om een tekst te versleutelen als om dezelfde tekst te ontsleutelen.

[80] De PSID is een unieke identifier die bestaat uit 32 alfanumerieke tekens die meestal op het etiket van de drager wordt afgedrukt.

139. Bij de risicoanalyse die aan de keuze van deze techniek voorafgaat, moet de verantwoordelijke rekening houden met toekomstige technologische ontwikkelingen die de huidige versleutelingsmethoden mogelijk minder veilig maken.

140. De versleuteling, die wordt uitgevoerd om de toegang tot de gegevens op de drager te voorkomen, moet worden uitgevoerd volgens een door de verwerkingsverantwoordelijke gevalideerde procedure.

3.2.4.5. Risico's

141. Zodra de gegevens zijn versleuteld, zijn ze, hoewel ze in een andere vorm werden geregistreerd, nog steeds aanwezig op de drager. Het gebruik van deze techniek houdt dus in dat het versleutelingsalgoritme voldoende robuust moet zijn om ontsleuteling zonder kennis van de sleutel te voorkomen. Ook mag het niet mogelijk zijn om de oorspronkelijke sleutel (dus voordat deze wordt gewijzigd/vernietigd) op een of andere manier te herstellen is, noch op de drager zelf, noch elders (zoals eventuele back-ups). Deze vereisten gelden voor alle technieken die gebruikmaken van versleuteling.

142. Deze procedure moet ervoor zorgen dat:

- Het gebruikte versleutelingsalgoritme wordt herkend en veilig is[81,82] (gebruik geen verouderde algoritmen zoals bijvoorbeeld DES of 3DES ;
- De gebruikte versleutelingssleutels voldoende lang zijn[83,82];
- De gebruikte versleutelingssleutels correct worden beheerd (dat ze niet op de drager staan en in ieder geval niet in niet-gecodeerde tekst);
- Versleuteling op de volledige drager of op een logische onderverdeling ervan wordt toegepast (in tegenstelling tot de versleuteling van afzonderlijke mappen of bestanden).

Opgemerkt moet worden dat de meeste moderne encryptietechnieken aan deze eisen voldoen.

143. Naast de risico's op het vlak van technologische ontwikkelingen, brengt cryptografisch wissen, of preciezer gezegd de versleuteling, ook intrinsieke risico's

---

[81] \\ Bij wijze van voorbeeld beveelt bijlage B1 van de door ANSSI gepubliceerde 'Référentiel général de sécurité' het symmetrische AES-versleutelingsmechanisme aan (links in bijlage C).

[82] ENISA (European Union Agency for Cybersecurity) publiceert ook documenten met betrekking tot aanbevolen algoritmen, sleutellengtes, parameters en encryptieprotocollen op haar website.

[83] \\ Bij wijze van voorbeeld beveelt bijlage B1 van de door ANSSI gepubliceerde 'Référentiel général de sécurité' een minimale grootte voor symmetrische sleutels van 128 bits aan (links in bijlage C).

met zich mee die gepaard gaan met een mogelijk zwak wachtwoord dat de authentificatiesleutel moet beschermen (desgevallend), de aanwezigheid van sleutels in het geheugen, de aanwezigheid van niet-versleutelde gegevens in tijdelijke bestanden of een zwak protocol voor de versleuteling. Bovendien kan het moeilijk zijn om helemaal zeker te zijn dat encryptiesleutels daadwerkelijk permanent ontoegankelijk werden gemaakt[84].

144. Ten slotte merken we op dat, voor de ontoegankelijke gebieden van de drager, hardware-onafhankelijke versleutelingssoftware dezelfde beperkingen kennen als 'opschoningssoftware' van derden (zie artikel 3.2.1.1.).

145. Om deze reden raden wij, net als het NIST, aan om na de actie 'cryptografisch wissen' de drager te wissen/overschrijven (met verificatie). Dit verkleint meer bepaald het potentiële risico dat de drager nog een toegankelijke decoderingssleutel bevat na een ondoeltreffende vernietiging of als er geen vernietiging werd uitgevoerd.

Idealiter

146. Idealiter verschaffen fabrikanten van SED's of van dragers die commando's zoals 'secure erase' aanbieden, alle noodzakelijke informatie over de ingebouwde commando's en bieden ze garanties over het wisresultaat, bij voorkeur via een contract. Bovendien verhindert niets de verwerkingsverantwoordelijke om bij de aankoop van deze dragers schriftelijke garanties in dit verband te vragen.

3.3. De gegevensdrager wordt vernietigd

147. Allereerst merken we op dat er een aantal gevallen zijn waarin de fysieke vernietiging van de informatiedrager de voorkeur krijgt boven de 'opschoning' ervan:

- Als de drager defect is;
- Als de drive defect is;
- Als de apparatuur die nodig is om toegang te krijgen tot de gegevens niet meer beschikbaar is;
- Als het soort drager niet de mogelijkheid tot 'opschoning' biedt, zoals bij WORM-dragers (write once, read many - voorbeeld: niet-overschrijfbare cd-rom);
- Als de controlestap die de 'purge' of 'clear' methodes afsluit geen veilige resultaten oplevert of niet lukt (om bekende of onbekende redenen).

148. Ongeacht de milieubezorgdheid kan het voordeliger zijn om de drager te vernietigen dan om deze 'op te schonen' met het oog op hergebruik.

149. Tot slot merken we op dat chemische vernietiging in dit document niet wordt besproken. Hoewel bepaalde chemische stoffen in staat zijn om gegevensdragers aan

[84] Zie sectie 4.7.3 (Verification of Sanitization Results) van de guidelines SP.880-88r1 van het NIST, waar het specifieke geval van cryptografisch wissen op pag. 21 wordt besproken.

te vallen en te vernietigen, is deze zelden gebruikte techniek gevaarlijk voor de gezondheid en schadelijk voor het milieu.

3.3.1. Segmentatie van technieken

150. A) Sommige vernietigingstechnieken beschadigen de drager slechts gedeeltelijk.

- Hierdoor blijven de gegevens die op de intacte onderdelen zijn opgeslagen, toegankelijk. Dit is het geval voor de vervormingstechnieken die in de volgende sectie 3.3.2. worden besproken.

151. B) Andere technieken, zoals versnipperen, verpletteren of desintegreren, halen de drager uit elkaar (zie sectie 3.3.3.).

- Het is belangrijk om te beseffen dat ook in dit geval de gegevens nog altijd aanwezig zijn op de respectieve drager. Ze zijn eenvoudigweg in kleinere delen opgesplitst. Als we weten dat een harde schijf meerdere terabytes aan gegevens kan bevatten, is het niet meer dan logisch dat een fragment van een harde schijf, niet meer dan een cm^2 groot, nog steeds enkele gigabytes aan gegevens kan bevatten.

- Het beveiligings-/vertrouwelijkheidsniveau van een fragment van de drager houdt verband met de grootte van de verkregen fragmenten. Hoe kleiner de fragmenten, hoe meer middelen en tijd er nodig zijn om de gegevens te herstellen. Dit verband (grootte van de fragmenten - beveiliging/vertrouwelijkheid) staat centraal in DIN 66399, die in sectie 3.3.6. wordt besproken.

152. C) Een derde groep technieken ten slotte maakt de volledige vernietiging van de drager en a fortiori van de gegevens erop mogelijk.

- Het resultaat wordt bereikt door de toestand van de drager te veranderen, d.w.z. van vast naar gasvormig (sublimeren) of vloeibaar (smelten).

3.3.2. Fysieke vervorming

153. De term 'fysieke vervormingstechnieken[85]' dekt een groot aantal verschillende technieken. Deze technieken kunnen worden toegepast met zowel grote industriële apparatuur als met gangbaar gereedschap zoals een hamer, persluchtspijkermachine, boor of pers.

154. Voorbeelden van dergelijke technieken zijn:

- Plooien (folding/bending);
- Snijden (cutting);
- En boren/perforeren/ponsen (drilling / puncturing / punching / piercing).

[85] In het Engels: deformation.

155. Benders gebruiken een metalen wig om een drager (meestal harde schijven) in de lengte te plooien in een hoek van 90 graden. De metalen wig, die met grote kracht wordt ingedrukt, beschadigt de platen, leeskoppen, elektrische motor en elektronica van de harde schijf, zodat deze niet meer toegankelijk is via de interface.

156. Hoewel u bij perforeren misschien onmiddellijk denkt aan een technicus die zijn boormachine gebruikt om gaten in een harde schijf te maken, is dit toch niet de methode die de ITAD-sector (IT Asset Disposition) aanbeveelt. Er bestaan inderdaad machines die specifiek voor deze methode zijn bestemd. Een perforator gebruikt een pin in gehard staal om dragers te doorboren. Als een harde schijf wordt doorboord, worden de platen, leeskoppen, elektrische motor en elektronica van de harde schijf beschadigd, zodat deze niet meer toegankelijk is via de interface.

157. Sommige apparaten bieden een optionele module die eveneens SSD's (Solid State Drives) via perforatie kan vernietigen. Afhankelijk van het model wordt de SSD op verschillende plaatsen met metalen pinnen doorboord of in de vorm van een golf gespleten.

158. De gemeenschappelijke deler van deze technieken is dat ze de drager slechts gedeeltelijk beschadigen en dat de gegevens die zijn opgeslagen op de onderdelen die niet worden vervormd, toegankelijk blijven.

159. Als gevolg hiervan bereiken deze technieken niet het 'destroy' vertrouwelijkheidsniveau. Ook al maken ze het onmogelijk om de gegevens via de interface van de drager te herstellen en kan de drager niet meer worden gebruikt voor verdere opslag. De drager worden niet als 'vernietigd' beschouwd zolang het herstel van de gegevens mogelijk is, ook al vereist dit geavanceerde laboratoriumtechnieken.

160. Bij wijze van bevestiging vermeldt het NSA ('National Security Agency' van de Verenigde Staten) in zijn referentiedocument[86] over dit onderwerp vervormingstechnieken enkel als aanvullende[87] en sterk aanbevolen maatregelen bij een demagnetisering van magnetische harde schijven. Het NSA valideert vervorming op zich niet als 'opschoningsmethode'.

3.3.3. Versnipperen, verpletteren en desintegreren[88]

161. Hoewel deze technieken verschillend zijn, leiden ze alle drie tot een desintegratie van de drager, door deze in kleinere onderdelen om te zetten. De grootte van het afval is afhankelijk van de techniek, de materialen waaruit de drager bestaat en de technische kenmerken van het gebruikte apparaat.

162. Shredders bijvoorbeeld bestaan in alle maten en vormen en kunnen, al naargelang het model, vrijwel alles versnipperen, van banden tot harde schijven of SSD's, van papier tot een bank. De gemiddelde grootte van het afval is afhankelijk van het model. De individuele grootte zal afhangen van de materialen die bij de

---

[86] NSA/CSS Storage Device Sanitization Manual

[87] Ondanks alles toetst het NSA het vermogen van bepaalde apparaten om de platen (platen) van een (magnetische) harde schijf in 30 seconden of minder te vervormen door deze te plooien (bending), te ponsen (punching) of te persen (waffling). Apparaten die aan deze criteria voldoen, worden in het document 'NSA/CSS Evaluated Products List for Hard Disk Drive Destruction Devices' opgesomd.

[88] In het Engels: shredding, crushing and desintegration

samenstelling werden gebruikt. Zo zullen bij een harde schijf de plastic onderdelen van het omhulsel groter zijn dan de onderdelen van de platen.

163. De keuze voor de ene techniek in plaats van de andere is ondergeschikt aan de grootte van het verkregen afval. Daarom zullen we niet verder gaan dan een eenvoudige beschrijving van de technieken zelf.

164. Zoals de ISO/IEC 21964-norm specificeert, 'binnen deze context (vernietiging van de drager) betekent een veilige vernietiging de vernietiging van de gegevensdragers die de persoonsgegevens bevatten op een zodanige manier dat het onmogelijk is om de informatie op deze dragers te herstellen of enkel mogelijk is met aanzienlijke uitgaven (in termen van personeel, materiële middelen en tijd)'.

3.3.3.1. Versnipperen

165. Shredders bestaan uit naast elkaar geplaatste cilinders met messen van gehard staal, die in tegengestelde richting draaien om materialen te snijden, te verscheuren en te extruderen. Voor de materialen waarin we in het bijzonder zijn geïnteresseerd, zijn er shredders die enkel dunne dragers verwerken, zoals optische dragers (cd, dvd, Blu-Ray), geheugendragers (USB-sticks, geheugenkaarten), magnetische banden (audio, video, gegevens), alle soorten magnetische of chipkaarten. Andere shredders verwerken daarenboven smartphones, tablets, harde schijven en mogelijk SSD's. Nog andere apparaten ten slotte zijn bestemd voor de vernietiging van papier.

166. Een papiershredder is een mechanisch apparaat dat wordt gebruikt om papier in stroken of deeltjes te snijden. We merken eveneens op dat een dergelijk apparaat ook kan worden gebruikt om flexibele dragers zoals diskettes te vernietigen, zodra de dragers fysiek uit het omhulsel worden verwijderd. De grootte van de afgescheurde stukken moet klein genoeg zijn dat er een redelijke zekerheid is, in overeenstemming met de vertrouwelijkheid van de gegevens, dat de gegevens niet kunnen worden hersteld. Met het oog op goedkeuring van het NSA moeten papiershredders in staat zijn om papieren documenten tot snippers van maximaal een millimeter bij vijf millimeter te verkleinen[89]. Ook apparaten zoals een desintegrator kunnen papieren documenten vernietigen (zie par.178)

Solid State Drives - SSD's

167. We herinneren er nogmaals aan dat (magnetische) harde schijven en (elektronische) SSD's zeer uiteenlopende technische kenmerken hebben en a priori niet op dezelfde manier kunnen worden 'opgeschoond'/vernietigd.

168. Shredders die niet specifiek aan deze dragers zijn aangepast, zullen afval produceren dat te groot is om gegevens op 'high density' halfgeleiderchips op een veilige manier te vernietigen.

169. De NSA-beveiligingsnormen vereisen dat harde schijven worden gereduceerd tot een uiteindelijke deeltjesgrootte van twee millimeter of worden gedemagnetiseerd en vervolgens fysiek vernietigd (pletmachines of shredders). Deze

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

tweede optie is niet mogelijk voor SSD's. Volgens een door Blancco uitgevoerde studie (dec 2018) hebben een groot aantal organisaties (33 % in de VS en Canada) geen verschillend procedé om deze twee soorten dragers te verwerken.

170. Door de steeds grotere dichtheid van de gegevensopslag wordt de grootte van de chips op SSD's steeds kleiner. Bij het versnipperen tot grotere afmetingen dan deze componenten kan de informatie op de drager dus volledig intact blijven.

171. Om het herstel van de gegevens nog moeilijker te maken, kan het versnipperde materiaal met een niet-gevoelig materiaal van dezelfde soort (versnipperd papier of versnipperde flexibele drager) worden vermengd. Een grotere hoeveelheid afval verhoogt de moeilijkheidsgraad van het herstel. Dit geldt bovendien voor alle technieken en alle restanten van vernietigingsacties.

3.3.3.2. Verpletteren

172. Plet- of breekmachines gebruiken dan weer drukkracht om de drager te verbrijzelen door deze in stukken te breken (voorbeelden: tussen twee knijpers, waarvan er een vast zit - jaw crusher of via stootkracht - impact crusher).

173. De term pletmachine wordt soms gebruikt voor 'apparaten die in staat zijn om de laag van een optische schijf waar zich de gegevens bevinden, tot fijn stof te reduceren. De schijf zelf blijft intact en kan worden gerecycled of opgeruimd. Deze methode kan echter niet bij dvd's worden gebruikt omdat de laag met de informatie in het midden is ingeklemd (bron: KSZ[90]). Dit is echter meer een slijptechniek. We voegen eraan toe dat het probleem hetzelfde is voor Blu-Ray discs.

174. Nog steeds met betrekking tot optische dragers merken we op dat het NSA, net als voor harde schijven[87] en andere soorten dragers[91], een lijst van gevalideerde apparaten[92] voor vernietiging via fragmentatie publiceert. Om in de lijst te worden opgenomen, moeten de apparatuur restanten produceren waarvan de zijde niet groter is dan:

- Voor cd's, een lengte van 5 millimeter;
- Voor dvd's en Blu-Ray, een lengte van 2 millimeter.

3.3.3.3. Desintegreren

175. We gebruiken de term desintegratie/desintegrator als de grootte van de zijde van de verkregen fragmenten kleiner is dan of gelijk is aan twee millimeter. Deze grootte houdt verband met de NSA-voorschriften, die in het document NSA/CSS Storage Device Sanitzation Manual worden vermeld. Als de apparatuur door het NSA is getest en aan de vereisten van de handleiding voldoet, wordt deze in de lijst NSA/CSS Evaluated Products List for Hard Disk Drive Destruction Devices opgenomen.

---

[90] Document van de KSZ (Kruispuntbank van de Sociale Zekerheid): Beleidslijn informatieveiligheid en privacy - Wissen van elektronische informatiedragers(maart 2017) pag. 7

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

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

176. Tegelijkertijd raden we aan om de dragers (zowel HD als SSD's) in batches met andere opslagapparaten te desintegreren.

177. Schijfdesintegratoren maken gebruik van de messenfreestechnologie om de drager continu in stukken te snijden tot de stukken klein genoeg zijn om door een specifieke afvalzeef te gaan. Desintegratie verloopt langzamer dan versnippering, maar de grootte van het afval is kleiner en het bereikte beveiligings-/vertrouwelijkheidsniveau is hoger.

178. Bij papierdesintegratoren (verschillend van papiershredders - zie par. 165) mag, met het oog op NSA-goedkeuring, de grootte van de zijde van de afgescheurde stukken niet groter zijn dan drie millimeter bij vijf millimeter[93].

3.3.3.4. Opmerkingen

179. We merken op dat vertaaltools niet erg nauwkeurig zijn, waardoor u in een en dezelfde zin meerdere verschillende vertalingen van eenzelfde techniek kunt vinden. Websites over de fysieke vernietiging van gegevensdragers (inclusief deze van sommige fabrikanten) verwisselen ook vaak de namen van apparaten en technieken, of gebruiken zelfs namen die geen verband houden met de gebruikte technologie (destroyer, dissambly device, cracker, ...).

180. We hebben bijvoorbeeld gezien dat, voordat het NSA ervan uitgaat dat informatiedragers zoals harde schijven en SSD's adequaat zijn 'opgeschoond', er aan twee voorwaarden moet worden voldaan: de zijde van de restanten mag niet groter zijn dan 2 mm en het gebruikte apparaat moet op de lijst van goedgekeurde apparaten staan (deze lijst vermeldt enkel Amerikaanse bedrijven). Dit is verschillend van DIN 66399.

181. Deze norm specificeert, op basis van de grootte van de restanten, welk beveiligingsniveau er wordt bereikt met eender welke vernietigingsmethode voor zes belangrijke klassen van informatiedragers (bv. papier, optisch, elektronisch of magnetisch). In sectie 3.3.6. komen we hierop terug.

182. De verwerkingsverantwoordelijke moet er rekening mee houden dat als hij een beroep doet op een externe dienstverlener om zijn dragers op te ruimen met behulp van de technieken die in hoofdstuk 3.3. werden besproken, de dienstverlener deze dragers na vernietiging waarschijnlijk zal recyclen of naar een stortplaats zal brengen.

183. Dit betekent dat de gegevens, als de dragers niet op een veilige manier werden vernietigd, mogelijk weer toegankelijk zijn voor derden. De restanten van de dragers kunnen zelfs in verschillende delen van de wereld terechtkomen als ze aan afvalbeheers- of recyclingbedrijven worden verkocht. Een mogelijke oplossing voor dit probleem is verbranding.

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

3.3.4. Verbranding

184. Alhoewel verbranding minder vaak wordt toegepast en een aanzienlijke impact op het milieu heeft, is het een doeltreffende techniek. Als het correct en in geschikte verbrandingsovens[94] wordt uitgevoerd, garandeert het de totale en onomkeerbare vernietiging van gegevens en dragers. Geschikte verbrandingsovens zijn zowel grote afvalverbrandingsinstallaties als kleinere mobiele en compacte verbrandingsinstallaties die gespecialiseerde bedrijven op verzoek naar de locatie van de verwerker kunnen brengen. Sommige mobiele modellen zijn bestemd voor papieropruiming, andere zijn in staat om metaal te smelten.

185. Als onderdeel van de digitale transformatie digitaliseren veel organisaties hun documenten om deze online op te slaan of te archiveren. Hierna moeten ze natuurlijk de originelen opruimen. Als er heel wat papier moet worden opgeruimd, kan verbranding een alternatief zijn voor versnippering.

186. Deze techniek kan ook bij andere soorten dragers worden gebruikt. In de handleiding over de opschoning van dragers vermeldt het NSA magnetische banden, diskettes, optische dragers, elektronische dragers en papier als dragers die via verbranding veilig kunnen worden vernietigd, op voorwaarde dat ze tot as worden herleid. Wat harde schijven betreft, verduidelijkt het NSA dat de coating van de binnenplaten tot as moet worden herleid en/of dat de binnenplaten door de werking van de warmte fysiek moeten worden vervormd.

187. Ingeval verbranding buiten de controle van de verwerkingsverantwoordelijke gebeurt, moet deze laatste ervoor zorgen dat de externe dienstverlener(s) de dragers verwerken op een manier die een volledige traceerbaarheidsketen biedt.

3.3.5. Demagnetiseren - degaussen (degaussing)

188. Demagnetisering, die reeds als een 'opschoningstechniek' werd voorgesteld (waarbij de drager wordt bewaard - zie sectie 3.2.3.), biedt eveneens de mogelijkheid om magnetische dragers, ongeacht het besturingssysteem en de interface, te vernietigen (onbruikbaar te maken), zelfs als ze zijn beschadigd. Voorwaarde is wel dat ze aan een voldoende magnetische kracht worden blootgesteld[95].

189. We benadrukken opnieuw het feit dat demagnetisering niet doeltreffend is bij apparaten met een flashgeheugen zoals SSD's. Deze techniek is eveneens niet geschikt voor papieren en optische dragers.

190. Demagnetisering stelt magnetische dragers bloot aan een sterk magnetisch veld dat ofwel door sterke magneten of door een elektromagnetische lading kan worden gecreëerd.

191. We raden aan dat het demagnetisering wordt gevolgd door een andere vernietigingstechniek. Dit garandeert het hoogste beveiligings-/vertrouwelijkheidsniveau, verdoezelt een storing van de degausser of een

---

[94] Een unit die een bijna totale verbranding van de brandbare bestanddelen van een afvalstof mogelijk maakt.

[95] Voorbeelden van degaussers die in staat zijn om harde schijven en magnetische banden te vernietigen.

onoplettendheid van een technicus en biedt een visuele verificatie dat de drager is vernietigd en kan worden opgeruimd. Onder deze voorwaarden en met behulp van een goedgekeurd apparaat[9671] valideert het NSA deze techniek op 'purge' niveau.

3.3.6. De DIN 66399-norm

192. De DIN 66399-norm van het Deutsches Institut für Normung, 'Büro- und Datentechnik - Vernichten von Datenträgern' genoemd[97], specificeert al naargelang de grootte van het afval ten gevolge van de vernietiging van de drager welk beveiligingsniveau apparaten bereiken die zijn bestemd om gegevensdragers te vernietigen.

193. Deze in Europa zeer populaire norm houdt minder rekening met de gebruikte techniek dan met de resultaten, en dit voor zes grote klassen van informatiedragers.

194. De (betalende[98]) norm, of beter gezegd de reeks normen, bestaat uit drie delen[99]:

- Deel 1: Beginselen en definities (publicatie 10/12);
- Deel 2: Vereisten voor apparatuur voor de vernietiging van gegevensdragers (publicatie 10/12);
- Deel 3: Vernietigingsproces voor gegevensdragers (publicatie 02/13).

195. Hoewel deze norm sinds 2012 door de DIN 66399-norm is vervangen, wordt de classificatie[100] uit de verouderde DIN 32357-norm (1995), die uitsluitend van toepassing was op papier, nog vaak genoemd in de beschrijving van de betreffende apparaten (voornamelijk papiershredders).

196. De DIN 66399-norm definieert beschermingsklassen, categorieën van dragers en beveiligingsniveaus.

Drie beschermingsklassen

197. Deze klassen bepalen in welke mate gegevens moeten worden beschermd, op basis van een evaluatie van het soort gegevens op de drager. De bescherming-/beveiligingsvereiste is onderverdeeld in de categorieën 'normaal', 'hoog' en 'zeer hoog':

---

[96] Een degausser is een fijn afgestelde magneet die in contact komt met andere magnetische dragers en die de magnetische handtekening van opgeslagen gegevens kan vernietigen.

[97] Duits instituut voor normalisatie - 'Office machines - Destruction of data carriers'.

[98] Elk deel kost enkele tientallen euro.

[99] Deel 1: Beginselen en definities, deel 2: Vereisten voor apparatuur voor de vernietiging van gegevensdragers en deel 3: Vernietigingsproces voor gegevensdragers.

[100] De DIN 32757-norm definieert 5 beveiligingsniveaus. In de literatuur is er eveneens sprake van een onofficieel 6e niveau 'Niveau 6 - Highest Security'. Deze beveiligingsniveaus houden verband met de fijnheid waarmee de shredder het materiaal versnippert en geven dus het beveiligingsniveau van de shredders aan.

- Beschermingsklasse 1 - Normale beveiligingsvereiste voor interne gegevens. Het verlies van de gegevens zou een negatief effect op de organisatie hebben of een risico op identiteitsdiefstal voor de betrokkenen met zich meebrengen;

- Beschermingsklasse 2 - Hogere beveiligingsvereisten voor vertrouwelijke gegevens. Het verlies van de gegevens zou een zeer negatief effect op de organisatie hebben of zou een inbreuk op de wettelijke verplichtingen betekenen of een financieel of sociaal risico voor de betrokkenen met zich meebrengen;

- Beschermingsklasse 3 - Zeer hoge beschermingsvereisten voor heel vertrouwelijke en geheime gegevens. Het verlies van de gegevens kan onherstelbare gevolgen voor de organisatie hebben of een risico voor de gezondheid en veiligheid of de individuele vrijheden van de betrokkenen inhouden.

Zes categorieën van gegevensdragers

198. De norm verdeelt de verschillende soorten gegevensdragers in 6 categorieën of klassen:

- Klasse P (papier) - origineel formaat (papier, röntgenfoto's);

- Klasse F (microfilm) - klein formaat (microfilm);

- Klasse O (optisch) - optische gegevensdragers (dc, dvd, Blu-Ray);

- Klasse T (tape) - magnetische gegevensdragers (banden, diskettes, kredietkaarten);

- Klasse H (harde schijf) - magnetische harde schijven;

- Klasse E (elektronisch) - elektronische gegevensdragers (USB-sticks, SSD's, geheugenkaarten, chipkaarten, flashgeheugens van smartphones en tablets, geheugenkaarten voor digitale camera's).

Zeven beveiligingsniveaus

199. De zeven beveiligingsniveaus zijn afgeleid van de drie beschermingsklassen, waarbij elke klasse drie beveiligingsniveaus omvat:

- Beschermingsklasse 1 - beveiligingsniveaus 1, 2 en 3

- Beschermingsklasse 2 - beveiligingsniveaus 3, 4 en 5

- Beschermingsklasse 3 - beveiligingsniveaus 5, 6 en 7

200. Deze beveiligingsniveaus bepalen hoeveel inspanning en middelen er nodig zijn om gegevens van een vernietigde drager te herstellen (hoe hoger het beveiligingsniveau, hoe kleiner het afval moet zijn):

- Beveiligingsniveau 1 - gegevensherstel vereist een eenvoudige inspanning (betreft algemene documenten die onleesbaar moeten worden gemaakt).

Met andere woorden, niveau 1 wordt gekozen voor gewone gegevens, waarvoor weinig of geen bescherming nodig is (bijvoorbeeld brochures en kranten) en waarvan het eventuele herstel vanuit de vernietigde drager geen problemen voor de gegevensbescherming zou opleveren;

- Beveiligingsniveau 2 - gegevensherstel vereist specifieke inspanningen en middelen (betreft interne documenten die onleesbaar moeten worden gemaakt);

- Beveiligingsniveau 3 - gegevensherstel vergt een aanzienlijke inspanning op het gebied van mankracht, tijd en tools (betreft zowel gevoelige/vertrouwelijke gegevens als persoonsgegevens waarvoor hoge beschermingsvereisten gelden);

- Beveiligingsniveau 4 - gegevensherstel vergt uitzonderlijke inspanningen en ongebruikelijke tools (betreft zowel zeer gevoelige/vertrouwelijke gegevens als persoonsgegevens waarvoor hoge beschermingsvereisten gelden);

- Beveiligingsniveau 5 - gegevensherstel is enkel mogelijk met ongebruikelijke tools (betreft vertrouwelijke gegevens die van fundamenteel belang zijn voor een organisatie of de betrokken personen);

- Beveiligingsniveau 6 - gegevensherstel is bij de huidige stand van de techniek onwaarschijnlijk (betreft vertrouwelijke gegevens waarvoor buitengewone beschermingsvereisten gelden);

- Beveiligingsniveau 7 - gegevensherstel is bij de huidige stand van de techniek onmogelijk (betreft strikt vertrouwelijke gegevens waarvoor de hoogste beschermingsvereisten gelden).

Met andere woorden, niveau 7 wordt gekozen voor 'top secret' gegevens (geheime diensten, militaire documenten), waarbij de mogelijkheid om de gegevens van de vernietigde drager te herstellen, absoluut moet worden uitgesloten (volgens de huidige stand van de kennis).

Tabellen

201. We kunnen al deze elementen samenbrengen in een tabel waarin we het vereiste vernietigingsniveau kunnen terugvinden.

	Beschermingsklasse 1		Beschermingsklasse 2		Beschermingsklasse 3		
Materiaal classificatie	Beveiligingsniveau 1	Beveiligingsniveau 2	Beveiligingsniveau 3	Beveiligingsniveau 4	Beveiligingsniveau 5	Beveiligingsniveau 6	Beveiligingsniveau 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. Bij wijze van voorbeeld vindt u hieronder de aanbevolen beveiligingsniveaus voor de dragercategorieën H en P:

H – Magnetische harde schijven	
Beveiligingsniveau	**Conditie / Max. residu grootte**
H-1	Niet werkend
H-2	Beschadigd
H-3	Vervormd
H-4	160 mm²
H-5	30 mm²
H-6	10 mm²
H-7	5 mm²

P – Originele grotte (papier)	
Beveiligingsniveau	**Conditie / Max. residu grootte**
P-1	Snipperformaat 12 mm ou 2000 mm²
P-2	Snipperformaat 6 mm ou 800 mm²
P-3	Snipperformaat 2 mm ou 320 mm²
P-4	160 mm²
P-5	30 mm²
P-6	10 mm²
P-7	5 mm²

203. Opmerking: op niveau H1 kan de schijf om mechanische of elektronische redenen buiten gebruik zijn.

Voorbeelden van interpretatie

204. Veel fabrikanten en dealers nemen referenties zoals 'E-1/H-3' of 'T-1/E-2/H-3' op in de beschrijving van hun vernietigingsapparatuur voor informatiedragers. Dit zijn, volgens de fabrikanten, de beveiligingsniveaus, al naargelang de klasse van dragers van de DIN 66399-norm, die de apparatuur kan bereiken. Hieronder volgen enkele voorbeelden van interpretaties van deze beveiligingsniveaus:

- Een harde schijf uit dragercategorie 'H' (zie bovenstaande tabel) met gevoelige of vertrouwelijke gegevens die beveiligingsniveau 3 (d.w.z. niveau H-3) vereisen, moet worden vervormd om aan de vereisten van de DIN 66399-norm te voldoen.

- Als een vernietigingsapparaat aangeeft dat het niveau P-5 bereikt (zie bovenstaande tabel), betekent dit dat het voor dragers in origineel formaat (bv. papier - dragercategorie 'P') aan beveiligingsniveau 5 voldoet en dus in staat is om de drager in deeltjes van 30 mm² te fragmenteren. Een dergelijk apparaat zal dus aan de vereisten van de DIN-norm voor zeer vertrouwelijke gegevens (bv. medische documenten) voldoen. Zodra het apparaat de gegevens heeft vernietigd, kunnen ze niet meer worden hersteld met behulp van de gebruikelijke technieken.

- Een microfilm die tot dragercategorie 'F' behoort (deze tabel vindt u niet hierboven) en die van zeer vertrouwelijke aard is en waarvoor beveiligingsniveau 5 (d.w.z. F-5) is vereist, moet worden versnipperd tot een deeltjesgrootte van maximaal 1 mm².

Gebruik van de DIN-norm in de praktijk

205. De stappen die u moet volgen om het te bereiken beveiligingsniveau en de maximale grootte van de restanten na de vernietiging van de drager te bepalen om zodoende het juiste vernietigingsapparaat te selecteren:

A. Kies uit de 3 beschermingsklassen de klasse die overeenkomt met het vertrouwelijkheids-/beveiligingsniveau van de gegevens op de te vernietigen drager (intern, vertrouwelijk of zeer vertrouwelijk document).

B. De gekozen beschermingsklasse biedt u vervolgens de keuze uit 3 beveiligingsniveaus (hoe hoger het gekozen beveiligingsniveau, hoe kleiner de restanten zullen zijn).

C. Selecteer vervolgens het soort drager dat moet worden vernietigd (papier, elektronisch, magnetische banden, ...).

D. Verbind nu de gegevensdrager met het beveiligingsniveau. Deze informatie kunt u gebruiken om een geschikt vernietigingsapparaat te kiezen.

DIN et ISO

206. In 2018 heeft de ISO/IEC JTC101 de in 2013 ontwikkelde DIN 66399-norm internationaal gestandaardiseerd. Deze norm met het nummer ISO/IEC 21964 wordt nu wereldwijd door organisaties gebruikt voor de vereisten voor gegevensvernietiging. De materialen waarnaar er in de beveiligingsniveaus wordt verwezen, zijn identiek aan de materialen waarnaar er in de DIN 66399-norm wordt verwezen.

207. De 3 delen van de DIN-norm (zie par. 193) komen overeen met de volgende 3 delen van de ISO-norm:

- 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

Vergelijking DIN - NSA - NIST

208. In het algemeen is de DIN 66399-norm niet zo veeleisend als de richtlijnen en normen van het NIST of het NSA.

209. In tegenstelling tot de DIN-norm beveelt het NSA aan om bij de vernietiging van harde schijven (magnetisch) deze eerst te demagnetiseren. Bovendien moet de vernietiging gebeuren met door het NSA goedgekeurde apparatuur.

210. Bovendien neemt de DIN-norm demagnetisering, net zoals elke techniek waarbij de drager niet wordt gefragmenteerd, niet in aanmerking, terwijl enerzijds het NSA deze techniek integreert en aanraadt om erna een vervormings- of vernietigingstechniek toe te passen en anderzijds het NIST deze op het 'purge' niveau integreert (en indirect op het 'destroy' niveau, gezien de onherstelbare schade die de techniek kan aanrichten).

211. Met betrekking tot de beveiligingsniveaus zelf, vereist het NIST bijvoorbeeld dat papieren dragers tot snippers van niet meer dan 1 mm x 5 mm worden versnipperd, of met behulp van een apparaat dat is uitgerust met een veiligheidsscherm[102] van 2,4

[101] Joint Technical Committee van de International Organization for Standardization (ISO) en van de International Electrotechnical Commission.

[102] De drager wordt continu gesneden tot de resulterende deeltjes klein genoeg zijn om door een zeef van specifieke grootte te gaan.

mm worden verpulverd/gedesintegreerd. Alleen het laatste DIN-beveiligingsniveau (P-7) voldoet aan deze vereiste (maximale grootte van de restanten van 5 mm^2).

212. Er is nog een andere bijzonderheid die verband houdt met elk DIN-beveiligingsniveau en niet voorkomt in de richtlijnen en normen van het NIST en het NSA en die eveneens het niveau van de vereisten verlaagt. Dit is de toegestane afwijking van de aanbevolen deeltjesgrootte voor elk DIN-beveiligingsniveau.
213. Bijvoorbeeld, beveiligingsniveau H5 (zie tabel par. 202) van de DIN-norm bepaalt een maximale deeltjesgrootte van 320 mm^2. De volledige specificaties van dit niveau bepalen echter dat slechts 90 % van de deeltjes kleiner moet zijn dan of gelijk moet zijn aan deze grootte en dat 10 % van de deeltjes zelfs 800 mm^2 groot mag zijn. Dit feit op zich zou ertoe leiden dat H5 niet aanvaardbaar is voor vertrouwelijke gegevens die van fundamenteel belang zijn voor een organisatie of de betrokkene.

214. Deze toegestane afwijking wordt op elk beveiligingsniveau voor elk soort drager gedefinieerd.

215. Samengevat kunnen we stellen dat de DIN 66399-norm gemakkelijk is te lezen en nuttig is voor het bedrijfsleven, maar ongetwijfeld minder geschikt is dan de richtlijnen en normen van het NIST en het NSA voor dragers met zeer vertrouwelijke gegevens die een hoog beveiligingsniveau vereisen.

4. Speciale gevallen

216. De verwerkingsverantwoordelijke is niet altijd in staat om gegevensdragers te wissen of te vernietigen.

217. Dit is het geval als de dragers niet van hem zijn. Voorbeelden hiervan zijn geleasede IT-apparatuur (printers/kopieerapparaten, serverinfrastructuur bij de IT-dienstverlener, cloud computing of videobewakingssysteem met opname).

218. In dit geval moet de verwerkingsverantwoordelijke ervoor zorgen dat het contract voorziet in de mogelijkheid om de gegevens te wissen of de dragers te vernietigen volgens een methode die hij goedkeurt. Bovendien moet hij in staat zijn om de correcte uitvoering en het resultaat te controleren. Als een contractuele aanpassing of een controle moeilijk blijkt, kan de verwerkingsverantwoordelijke eveneens onderhandelen over een terugkoop van de dragers in de apparatuur.

219. We kunnen niet genoeg benadrukken hoe belangrijk het is om alle kwesties inzake gegevensbescherming te bespreken voordat het contract wordt ondertekend. Na ondertekening is dit vaak heel moeilijk.

220. Dit is ook het geval als een apparaat met een informatiedrager (of de drager zelf) moet worden hersteld, vervangen of onderhouden buiten uw controlegebied. U moet het risico beoordelen dat ontstaat als een dienstverlener toegang krijgt tot de gegevens. We herinneren er nog eens aan de AVG zich focust op de gevolgen van een verlies aan vertrouwelijkheid voor de betrokkenen (de personen op wie de gegevens betrekking hebben).

221. Ingeval deze handeling een risico voor de betrokkenen inhoudt, moet deze onder de controle van de verwerkingsverantwoordelijke worden uitgevoerd (bv. herstelling ter plaatse of aankoop van een vervangende drager om de defecte drager te kunnen houden[103]).

[103] We merken op dat sommige leveranciers (waaronder HP, Dell en Lenovo) de mogelijkheid bieden om een extra 'keep your drive' garantie af te sluiten. Dit biedt klanten de mogelijkheid om een defecte drager die moet worden vervangen, te houden.

5. Verificatie

222. De laatste stap in de procedure, voordat er een document wordt afgegeven dat de opschoning of vernietiging bevestigt (zie deel 6 'Registratie'), is de controle van de vernietiging van de gegevens. Deze stap garandeert dat de gegevens correct werden opgeschoond of vernietigd. Deze stap is onmisbaar omdat er heel wat kan mislopen. Denk aan menselijke fouten (bv.: onverwerkte schijf in de stapel verwerkte schijven, gebrek aan opleiding, te grote haast), 'hardwarefouten' (bv.: beschadigd shreddermes of een storing in een van de onderdelen tussen de wissoftware en de gegevens op de schijven) en 'softwarefouten' (gemiste update, kwaliteit van de software).

223. Als de verwerkingsverantwoordelijke een beroep doet op een verwerker voor de opschoning of vernietiging van gegevens moet hij de verificatiemodaliteiten met de verwerker bespreken en deze eventueel contractueel vastleggen.

224. Idealiter zal een onafhankelijke persoon die niet bij de feitelijke vernietiging of opschoning van de gegevensdragers was betrokken, de verificatie uitvoeren. Volgens dezelfde logica moet, ingeval er software wordt gebruikt om gegevens op te schonen, de verificatie worden uitgevoerd door een andere software dan de software die voor de 'opschoning' werd gebruikt.

225. Dit kwaliteitscontroleproces wordt op dezelfde manier gedocumenteerd als de andere stappen van de vernietigings-/reinigingsprocedure. Zo moet de documentatie bijvoorbeeld het aantal te testen monsters vermelden.

226. Samen met deze documentatie moet de verwerkingsverantwoordelijke over een informatiesysteem beschikken dat het mogelijk maakt om, op verzoek, een conformiteitsattest af te leveren (d.w.z. bevestiging dat de gegevens met succes zijn gewist) voor elke afzonderlijke drager.

227. We sluiten dit deel 5 af met wat informatie over de verificatie van de verschillende 'opschoningstechnieken'.

Wissen - overschrijven

228. Afhankelijk van de omvang kan het resultaat van de verificatie minder of meer betrouwbaar zijn. De beste garantie voor een doeltreffende 'opschoning' van de gegevens wordt over het algemeen verkregen door alle toegankelijke gebieden van de drager te lezen. Zo controleert u of de verwachte waarden (binaire getallen 0 of 1) aanwezig zijn, d.w.z. de waarden die bij de instelling van de parameters voor de overschrijfpass werden bepaald.

229. Deze verificatie is uiteraard enkel mogelijk als de drager niet werd vernietigd.

230. Zelfs als de verificatie een tijdrovend proces is, moet het percentage van de te verifiëren oppervlakte van de drager, afhankelijk van de beschikbare tijd, zo groot mogelijk zijn. In ieder geval mag deze niet minder dan 10 % bedragen (wat vaak het standaardpercentage is dat software van derden aanbieden).

231. Software van derden en geïntegreerde commando's bieden verificatiemogelijkheden. Als u echter een manuele verificatie wilt uitvoeren die losstaat van de tool die bij de opschoning werd gebruikt, kunt u een 'disk editor'

gebruiken (vaak gekoppeld aan een 'hex editor'). Dergelijke software wordt bovendien het meest gebruikt voor gegevensherstel en digitale criminalistiek (digital forensics). \\ Bij wijze van voorbeeld noemen we drie van deze softwareprogramma's: Active@Disk-editor en HxD (freeware) en WinHex (bekende commerciële software).

232. In geval van de niveaus 'clear' en 'purge', ongeacht of het gaat om software van derden of om ingebouwd overschrijfcommando, moet de verificatie bevestigen dat de drager de verwachte waarden (zie par. 228) vertoont. Ingeval er meerdere overschrijfpasses werden uitgevoerd, worden de waarden van de laatste pass gezocht.

Cryptografisch wissen

233. In geval van cryptografisch wissen bestaat de meest doeltreffende verificatie erin dat u, vóór het wissen, willekeurige locaties leest. Na het cryptografisch wissen leest u de locaties opnieuw en vergelijkt u de resultaten.

234. Dit betekent dat als u na het cryptografisch wissen een andere techniek (bv. vernietiging) uitvoert, de verificatie vóór deze laatste stap moet gebeuren. Nadat u de extra techniek hebt toegepast, zal er een verificatie via 'rapid sampling' (snelle monstername) worden uitgevoerd.

Versnipperen, verpletteren, desintegreren

235. Ingeval dragers tot stukken werden herleid, wordt de grootte van de restanten visueel of met behulp van een zeef die overeenkomt met de maximaal toelaatbare grootte of een ander meetinstrument (bv. uiterst nauwkeurige digitale schuifmaat) gecontroleerd).

Demagnetiseren

236. De garantie van een correcte demagnetisering is in wezen gebaseerd op de selectie van een doeltreffende degausser, op het juiste gebruik ervan en op de periodieke steekproefsgewijze verificatie van de resultaten om zeker te zijn dat het proces verloopt zoals bedoeld.

6. Registratie

237. Het bewijs van vernietiging is een essentieel onderdeel van de traceerbaarheidsketen. Overeenkomstig de verantwoordingsplicht (accountability) uit de AVG (artikel 5.2) biedt dit bewijs de verwerkingsverantwoordelijke de mogelijkheid om aan te tonen dat hij de beginselen inzake de verwerking van persoonsgegevens naleeft, met inbegrip van de beginselen inzake opslagbeperking en de beginselen inzake integriteit en vertrouwelijkheid (artikel 5.1.e en f - zie bijlage B).

238. Bijgevolg is het belangrijk om informatie over het goede verloop van de opschoning en/of vernietiging en over de techniek (en dus het gekozen vertrouwelijkheids-/beveiligingsniveau) te noteren en te bewaren, ongeacht of de procedure intern of met behulp van een verwerker wordt uitgevoerd. Gewoonlijk zal de persoon die verantwoordelijk is voor de handeling (onder het gezag van de verwerker of de verwerkingsverantwoordelijke) dit bewijs van vernietiging/opschoning afgeven. Een door de verwerkingsverantwoordelijke aangeduide persoon is verantwoordelijk voor de validering.

239. Hoewel verschillende actoren binnen de sector dit bewijs vaak 'vernietigingscertificaat' noemen, geven wij de voorkeur aan de minder officieel klinkende termen 'attest' of 'verklaring'[104].

Verwerking

240. Als er een beroep wordt gedaan op een verwerker om gegevensdragers op te schonen en/of te vernietigen, kan de verwerkingsverantwoordelijke de dragers verzamelen en bewaren op een plaats zonder beveiligde toegang tot de verwerker deze komt ophalen. De tijdelijke opslag van deze dragers sluit de kans op verlies of diefstal niet uit. Het kan dus nuttig zijn om de lijst van opgeslagen dragers te vergelijken met de lijst van dragers die de externe dienstverlener daadwerkelijk heeft meegenomen. Wij herinneren u nogmaals aan de noodzaak om een of meer personen aan te wijzen die verantwoordelijk zijn voor elke fase van de verwerking, met inbegrip van met name de inzameling van de dragers en de opslag ervan.

241. Het eigenlijke opschoningsproces kan plaatsvinden op het terrein van de verwerkingsverantwoordelijke of erbuiten (afhankelijk van de technische mogelijkheden van de verwerker of het verzoek van de verwerkingsverantwoordelijke). Ingeval de verwerking buiten het terrein gebeurt, is een afgevaardigde van de verwerkingsverantwoordelijke idealiter fysiek aanwezig gedurende het volledige vernietigingsproces. Deze persoon kan zich ervan vergewissen dat de dragers daadwerkelijk werden vernietigd. Zo niet bestaat de mogelijkheid dat het door de verwerker afgeleverde 'bewijs van vernietiging' niet strookt met de werkelijkheid en geen bewijsstuk vormt. De verwerkingsverantwoordelijke kan ook een beroep doen op gerechtsdeurwaarders om alle handelingen te controleren en te registreren.

242. Zoals reeds vermeld in par. 58 moet de afgifte van een attest van opschoning/vernietiging door de verwerker deel uitmaken van een contractuele

[104] De Larousse definieert een certificaat als 'een schriftelijk, officieel of naar behoren ondertekend document van een bevoegd persoon dat getuigt van een feit'.

overeenkomst met deze laatste. Ingeval er later gegevens worden gevonden die in het kader van het contract hadden moeten worden verwerkt, kan het attest het bewijs vormen dat de verwerker een fout heeft begaan.

Het attest

243. Het bewijs van opschoning/vernietiging wordt afgeleverd in de vorm van een gedetailleerd attest voor elke verwerkte drager. Het attest, op papier of in digitaal formaat, vormt een cruciaal element in de validering dat de gegevens niet meer kunnen worden versteld vanaf de drager die werd opgeschoond.

244. Algemeen gesproken, vermeldt het attest elk opslagapparaat per serienummer. Bovendien beschrijft het het beoogde vertrouwelijkheids-/beveiligingsniveau (clear, purge, destroy, H-1, P-5 ...), de gebruikte reinigingstechniek (demagnetiseren, versnipperen, cryptografisch wissen ...), de gebruikte tools, de gebruikte controlemethode en het resultaat ervan, alsook andere informatie zoals datum, plaats en betrokken personen.

245. Samengevat zal het attest van vernietiging informatie bevatten over:

- De datum en plaats van de procedure;
- De organisatie, de persoon die de vernietiging uitvoert (identificatie);
- De gegevensdrager en de apparatuur waarin deze drager zich bevindt (serienummer, soort, ...);
- De gebruikte techniek (software- en hardwaretools, vertrouwelijkheids-/beveiligingsniveau, referentienorm, methode, ...);
- De verificatie (methode) en het eindresultaat ervan;
- De bestemming van de drager (hergebruik, opruiming, terugkeer naar de leverancier, ...);
- De validering van het attest (contactgegevens van de persoon die het attest verifieert, aangezien deze persoon niet de persoon is die de vernietiging heeft uitgevoerd).

246. Het attest moet worden bewaard en moet, op verzoek, kunnen worden overgelegd. Hoewel de Kruispuntbank van de Sociale Zekerheid (KSZ) een bewaartermijn van 'minstens 2 jaar[105]' aanbeveelt, vinden wij het verstandig om

[105] https://www.ksz-bcss.fgov.be/sites/default/files/assets/veiligheid_en_privacy/bld_erase_wissen_informatiedragers.pdf:

rekening te houden met de wettelijke verjaringstermijnen[106]. Deze termijnen bedragen over het algemeen 5[107] of 10 jaar[108].

247. Zolang de verjaringstermijn niet is verstreken, kan een persoon of organisatie die schade heeft geleden als gevolg van een ontoereikende opschoning van gegevens of een ontoereikende vernietiging van een gegevensdrager, een rechtsvordering instellen bij de rechterlijke instanties om de verwerkingsverantwoordelijke te laten veroordelen tot vergoeding van de schade of tot andere sancties.

[106] De verjaringstermijnen worden vermeld in de artikelen 2262 bis en volgende van het Burgerlijk Wetboek.

[107] Persoonlijke acties die voortvloeien uit een buitencontractuele gebeurtenis: 5 jaar (art. 2262 bis §1, lid 2 en 3 van het Burgerlijk Wetboek).

[108] Persoonlijke acties die voortvloeien uit de uitvoering van een contract: 10 jaar (art. 2262 bis §1, lid 1 van het Burgerlijk Wetboek).

Bijlage A: Aanbevolen technieken voor de belangrijkste soorten dragers

Magnetische dragers Floppy Disks	**Clear**	⇨ De drager **overschrijven** (wissen) met behulp van een door de organisatie goedgekeurde software en vervolgens valideren (verificatie). Het 'clear' niveau moet resulteren in minstens een schrijfpass met een vaste gegevenswaarde (bv. allemaal nullen). Optioneel: er kunnen eventueel meerdere schrijfpasses of complexere waarden worden gebruikt.
	Purge	⇨ De drager **demagnetiseren** met behulp van een door de organisatie goedgekeurde degausser (raadpleeg eventueel de lijst met NSA-goedgekeurde apparaten).
	Destroy	⇨ De drager **verbranden**: de steun moet tot as worden herleid. ⇨ **Versnipperen - desintegreren** (eventueel verwijzen naar de lijst met NSA-goedgekeurde apparaten). De DIN-norm beveelt afvalafmetingen van max. 2000 mm² voor T2, max. 320 mm² voor T3, max. 160 mm² voor T4, max. 30 mm² voor T5, max. 10 mm² voor T6 en max. 2,5mm² voor T7 aan.
Optische schijven Cd/dvd/Blu-Ray	**Clear**	Niet beschikbaar.
	Purge	Niet beschikbaar.
	Destroy	⇨ **Slijpen** (schuren). Alle informatiehoudende lagen van de drager verwijderen met behulp van een commercieel slijpapparaat voor optische schijven. Deze techniek is niet geschikt voor dvd en Blu-Ray (zie par. 172). ⇨ De drager **verbranden**: de drager moet tot as worden herleid. ⇨ **Versnipperen - desintegreren - verpletteren** Het NSA vermeldt een maximaal afvalformaat van 2 mm voor dvd's en Blu-Ray en 5 mm voor cd's (zie par. 173) (eventueel verwijzen naar de lijst met NSA-goedgekeurde apparaten). De DIN-norm beveelt afvalafmetingen van max. 2000 mm² voor O1, max. 800 mm² voor O2, max. 160 mm² voor O3, max. 30 mm² voor O4, max. 10 mm² voor O5, max. 5 mm² voor O6 en max. 0,2 mm² voor O7 aan.

Magnetische dragers Harde schijven van het type ATA	**Clear**	⇨ De drager **overschrijven** (wissen) met behulp van een door de organisatie goedgekeurde software en vervolgens valideren (verificatie). Het 'clear' niveau moet resulteren in minstens een schrijfpass met een vaste gegevenswaarde (bv. allemaal nullen). Optioneel: er kunnen eventueel meerdere schrijfpasses of complexere waarden worden gebruikt.
	Purge	In volgorde van voorkeur: ⇨ **1. 'Sanitize Device' commando**: indien dat wordt ondersteund, gebruikt u een van de commando's van de 'ATA Sanitize Device' functieset (te verkiezen boven het 'Secure Erase' commando). Een van de volgende opties (of beide) kan beschikbaar zijn: **1.a) Overschrijven** ('overwrite ext' commando). Pas een schrijfpass met een vaste gegevenswaarde toe (bv. allemaal nullen). Een enkele schrijfpass zou genoeg moeten zijn om de drager te 'purgen'. Optioneel: voer in plaats van een schrijfpass drie schrijfpasses uit. Maak hierbij gebruik van de optie 'Invert' zodat de tweede schrijfpass de omgekeerde versie van het gespecificeerde patroon is. **1.b) Cryptografisch wissen**('crypto scramble ext' commando). Optioneel: zodra u de drager met succes cryptografisch hebt gewist, gebruikt u het 'overwrite' commando om een nulpass of een pseudowillekeurig patroon op de drager te schrijven. Als dit commando niet wordt ondersteund, kunt u na de actie 'cryptografisch wissen' de 'Secure Erase' of 'Clear' procedure toepassen. ⇨ **2. 'Secure Erase' commando:** indien dat wordt ondersteund, gebruikt u het 'Secure Erase Unit' commando in de 'enhanced' modus. ⇨ **3. Cryptografisch wissen** via de klasse van het Opal-beveiligingssubsysteem (zie par. 131), als de ingebouwde commando's niet beschikbaar zijn. Optioneel: zodra u de drager met succes cryptografisch hebt gewist, gebruikt u het 'overwrite' commando om een nulpass of een pseudowillekeurig patroon op de drager te schrijven. Als dit commando niet wordt ondersteund, kunt u na de actie 'cryptografisch wissen' de 'Secure Erase' of 'Clear' procedure toepassen. ⇨ **4.** De drager **demagnetiseren** met behulp van een door de organisatie goedgekeurde degausser (raadpleeg eventueel de lijst met NSA-goedgekeurde apparaten). We raden aan om de harde schijf te beschadigen door de interne platen te vervormen voordat u deze weggooit.

	Destroy	⇨ De drager **verbranden**: de drager moet tot as worden herleid. De coating van de binnenplaten moet tot as worden herleid en/of de binnenplaten moeten door de werking van de warmte fysiek worden vervormd. ⇨ **Versnipperen - desintegreren** De NSA vermeldt een maximale afvalgrootte van 2 mm en raadt aan om de dragers, samen met andere opslagapparaten, in batches te vernietigen (raadpleeg eventueel de lijst met NSA-goedgekeurde apparaten). De DIN-norm raadt aan dat de drager bij niveau H1 mechanisch/ elektronisch onbruikbaar wordt gemaakt, bij niveau H2 wordt beschadigd en bij niveau H3 wordt vervormd. Bovendien beveelt de norm afvalafmetingen van max. 2000 mm² voor niveau H4, max. 320 mm² voor H5, max. 10 mm² voor H6 en max. 5 mm^2 voor H7 aan.

Magnetische dragers SCSI Drives	**Clear**	⇨ De drager **overschrijven** (wissen) met behulp van een door de organisatie goedgekeurde software en vervolgens valideren (verificatie).
	Purge	⇨ **'Sanitize' commando** (zie 'Sanitize Device' commando voor ATA Hard Drives) ⇨ De drager **demagnetiseren** met behulp van een door de organisatie goedgekeurde degausser (raadpleeg eventueel de lijst met NSA-goedgekeurde apparaten). We raden aan om de harde schijf te beschadigen door de interne platen te vervormen voordat u deze weggooit.
	Destroy	⇨ De drager **verbranden**: de drager moet tot as worden herleid. De coating van de binnenplaten moet tot as worden herleid en/of de binnenplaten moeten door de werking van de warmte fysiek worden vervormd. ⇨ **Versnipperen - desintegreren** De NSA vermeldt een maximale afvalgrootte van 2 mm en raadt aan om de dragers, samen met andere opslagapparaten, in batches te vernietigen (raadpleeg eventueel de lijst met NSA-goedgekeurde apparaten). De DIN-norm raadt aan dat de drager bij niveau H1 mechanisch/ elektronisch onbruikbaar wordt gemaakt, bij niveau H2 wordt beschadigd en bij niveau H3 wordt vervormd. Bovendien beveelt de norm afvalafmetingen van max. 2000 mm² voor niveau H4, max. 320 mm² voor H5, max. 10 mm² voor H6 en max. 5 mm² voor H7 aan.
Papier	**Clear**	Niet beschikbaar.
	Purge	Niet beschikbaar.
		⇨ De drager **verbranden**: de drager moet tot as worden herleid. ⇨ **Versnipperen - desintegreren** Het NIST raadt aan dat de shredder afvalafmetingen van max. 5 mm² produceert en dat u voor desintegratoren een zeef van 2,4 mm gebruikt (raadpleeg eventueel de lijst met NSA-goedgekeurde desintegratoren en NSA-goedgekeurde shredders). De DIN-norm beveelt een maximale strookbreedte van 12 mm voor P1 en 6 mm voor P2 aan. Bovendien beveelt de norm afvalafmetingen max. 320 mm² voor P3, max. 160 mm² voor P4, max. 30 mm² voor P5, max. 10 mm² voor P6 en max. 5 mm² voor P7 aan.

Flashdragers - USB Removable Drives - Memory Cards - Solid State Drives	**Clear**	⇨ De drager **overschrijven** (wissen) met behulp van een door de organisatie goedgekeurde software en vervolgens valideren (verificatie). Voor Solid State Drives van het type ATA & SCSI, USB Removable Media en Memory Cards: ⇨ De drager **overschrijven** (wissen) met behulp van een door de organisatie goedgekeurde software en vervolgens valideren (verificatie). Het 'clear' niveau moet resulteren in minstens een schrijfpass met een vaste gegevenswaarde (bv. allemaal nullen). Optioneel: er kunnen eventueel meerdere schrijfpasses of complexere waarden worden gebruikt. Voor Solid State Drives van het type ATA (alleen): ⇨ **'Secure Erase' commando:** indien dat wordt ondersteund, gebruikt u het 'Secure Erase Unit' commando in de 'enhanced' modus.
	Purge	A) Solid State Drives van het type ATA ⇨ **1. 'Sanitize Device' commando**: indien dat wordt ondersteund, gebruikt u een van de commando's van de 'ATA Sanitize Device' functieset (te verkiezen boven het 'Secure Erase' commando. Een van de volgende opties (of beide) kan beschikbaar zijn: **1.a) 'Block erase' commando** Optioneel: nadat het commando met succes is toegepast, schrijft u allemaal binaire 1'en in het door de gebruiker adresseerbare gebied van de drager. Voer vervolgens een tweede 'block erase' uit. **1.b) Cryptografisch wissen**('crypto scramble ext' commando). Optioneel: zodra u de drager met succes cryptografisch hebt gewist, voert u het 'block erase' commando uit. Als dit commando niet wordt ondersteund, kunt u na de actie 'cryptografisch wissen' de 'Secure Erase' of 'Clear' procedure toepassen. ⇨ **2. Cryptografisch wissen** via de klasse van het Opal-beveiligingssubsysteem (zie par. 131), als de ingebouwde commando's niet beschikbaar zijn. Optioneel: zodra u de drager met succes cryptografisch hebt gewist, voert u het 'block erase' commando uit. Als dit commando niet wordt ondersteund, kunt u na de actie 'cryptografisch wissen' de 'Secure Erase' of 'Clear' procedure toepassen. B) Solid State Drives van het type SCSI ⇨ **1. 'Sanitize' commando**: indien dat wordt ondersteund, gebruikt u een van de commando's van de 'SCSI Sanitize' functieset. Een van de volgende opties (of beide) kan beschikbaar zijn: **1.a) 'Block erase' commando**

		1.b) Cryptografisch wissen('cryptographic erase' commando). Optioneel: zodra u de drager met succes cryptografisch hebt gewist, voert u het 'block erase' commando uit. Als dit commando niet wordt ondersteund, kunt u na de actie 'cryptografisch wissen' de 'Secure Erase' of 'Clear' procedure toepassen. ⇨ **2. Cryptografisch wissen** via de klasse van het Opal-beveiligingssubsysteem (zie par. 131), als de ingebouwde commando's niet beschikbaar zijn. Optioneel: zodra u de drager met succes cryptografisch hebt gewist, voert u het 'block erase' commando uit. Als dit commando niet wordt ondersteund, kunt u na de actie 'cryptografisch wissen' de 'Secure Erase' of 'Clear' procedure toepassen. C) Verwijderbare USB-dragers en Memory Cards - Niet beschikbaar De meeste van deze dragers ondersteunen geen ingebouwde commando's of, indien ze dit wel doen, worden de interfaces niet op een gestandaardiseerde manier ondersteund.
	Destroy	⇨ De drager **verbranden**: de drager moet tot as worden herleid. ⇨ **Versnipperen - desintegreren** De NSA vermeldt een maximale afvalgrootte van 2 mm en raadt aan om de dragers, samen met andere opslagapparaten, in batches te vernietigen (raadpleeg eventueel de lijst met NSA-goedgekeurde apparaten). De DIN-norm beveelt afvalafmetingen van max. 160 mm² voor E3, max. 30 mm² voor E4, max. 10 mm² voor E5, max. 1 mm² voor E6 en max. 0,5 mm² voor E7 aan.

Bijlage B: Uittreksels uit de AVG

Artikel 5: **Beginselen inzake verwerking van persoonsgegevens**

1. Persoonsgegevens moeten:

   a) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is ('rechtmatigheid, behoorlijkheid en transparantie');

   b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd ('doelbinding');

   c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ('minimale gegevensverwerking');

   d) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren ('juistheid'); 4/5/2016 L 119/35 Publicatieblad van de Europese Unie NL.

   e) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen ('opslagbeperking');

   f) door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging ('integriteit en vertrouwelijkheid').;

2. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen ('verantwoordingsplicht').

Artikel 32: **Beveiliging van de verwerking**

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

a) de pseudonimisering en versleuteling van persoonsgegevens;

b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

2. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

3. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat dat de in lid 1 van dit artikel bedoelde vereisten worden nageleefd.

4. De verwerkingsverantwoordelijke en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van de verwerkingsverantwoordelijke verwerkt, tenzij hij daartoe Unierechtelijk of lidstaatrechtelijk is gehouden.

Artikel 33: **Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit**

1. Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.

2. De verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.

3. In de in lid 1 bedoelde melding wordt ten minste het volgende omschreven of meegedeeld:

a) de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;

b) de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;

c) de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;

d) de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

4. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.

5. De verwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren.

Artikel 34: **Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene**

1. Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.

2. De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in artikel 33, lid 3, onder b), c) en d), bedoelde gegevens en maatregelen.

3. De in lid 1 bedoelde mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:

a) de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;

b) de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het in lid 1 bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;

c) de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

4. Indien de verwerkingsverantwoordelijke de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de toezichthoudende autoriteit, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, de verwerkingsverantwoordelijke daartoe verplichten of besluiten dat aan een van de in lid 3 bedoelde voorwaarden is voldaan.

Bijlage C: Referenties

Belangrijkste referenties:

- « 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

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

Andere referenties:

- 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 » van het « 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 » van de IRS)
- https://www.killdisk.com/blog-gutmann-method.htm
- https://www.ksz-bcss.fgov.be/sites/default/files/assets/gegevensbescherming/bld_data_data_veiligheid.pdf
- https://www.ksz-bcss.fgov.be/sites/default/files/assets/gegevensbescherming/bld_erase_wissen_informatiedragers.pdf
('Beleidslijn informatieveiligheid & privacy inzake het wissen van elektronische informatiedragers van de Sociale Zekerheid')
- 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
  en de bijlagen 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