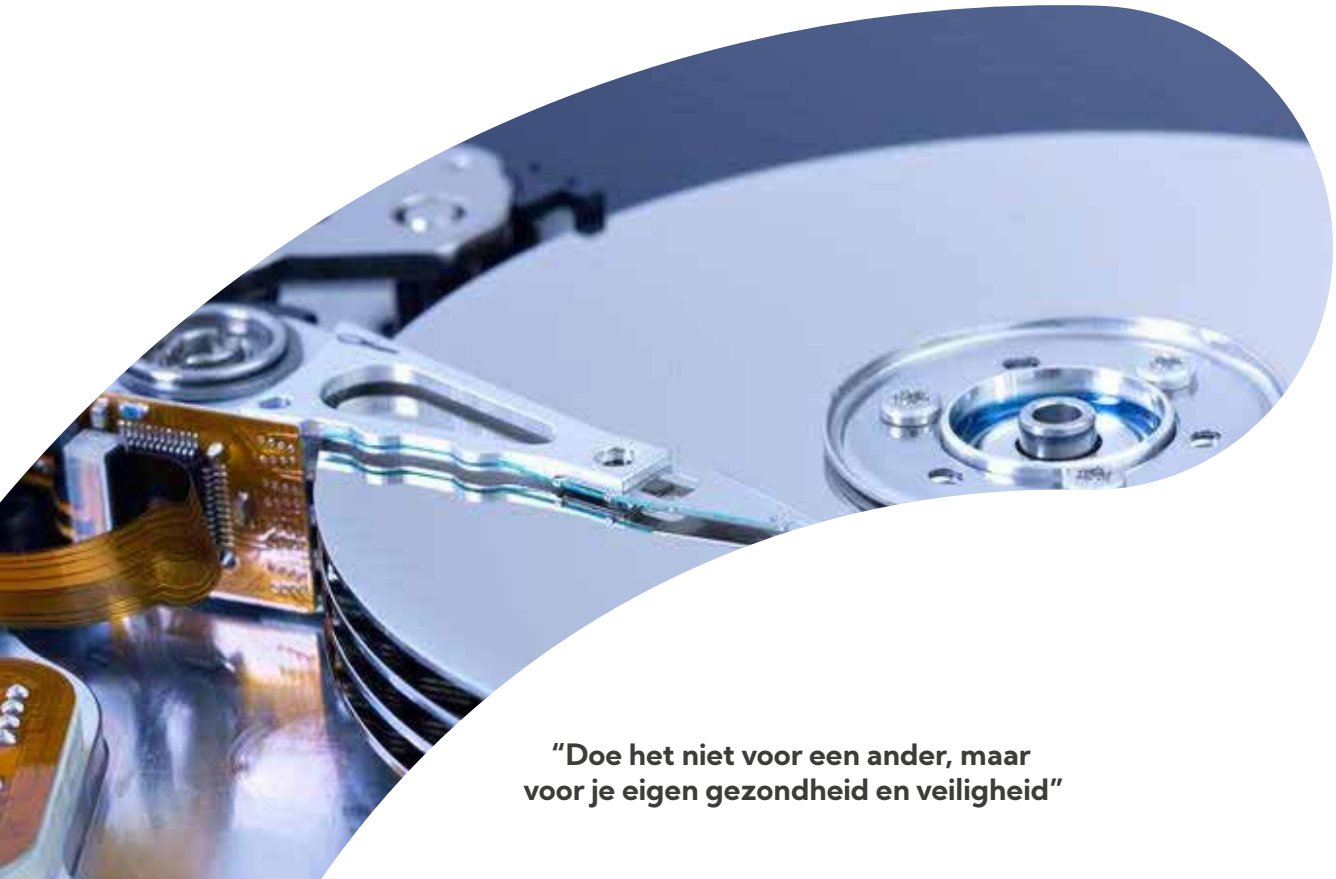
(De) weg van jouw data

Hoe kun je jouw data veilig en volledig verwerken?



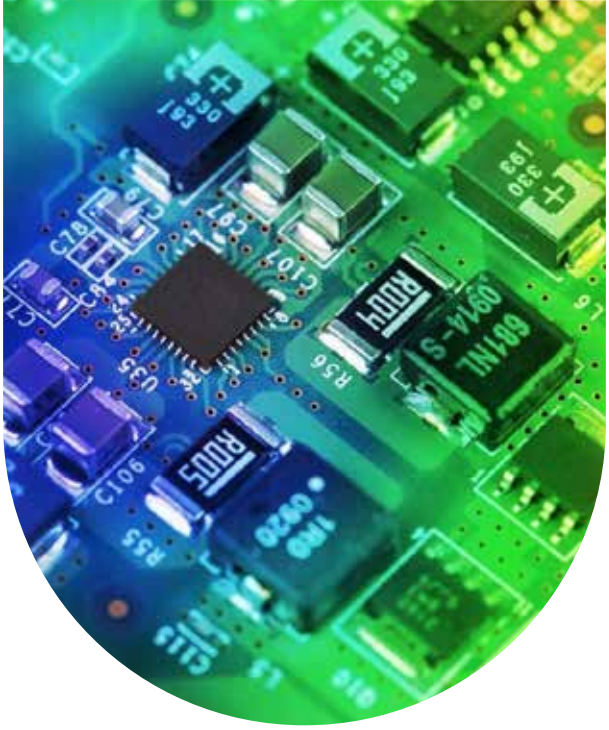
“Doe het niet voor een ander, maar voor je eigen gezondheid en veiligheid”

Inhoudsopgave

Inleiding

We hebben, verzamelen en bewaren steeds meer informatie. Denk aan smartphones, bankpasjes, usb-sticks, laptops, harde schijven, dvd's, id-kaarten, servers en sd-kaarten. Maar denk ook aan zogenaamde datadragers in bijvoorbeeld printers, 'slimme televisies' en zelfs koelkasten.

Al die datadragers bieden eindeloos veel mogelijkheden, maar informatie kan daar ook 'tot in de eindigheid' op blijven staan. Het kan natuurlijk gebeuren dat je gegevens wilt vernietigen. Bijvoorbeeld omdat je nieuwe systemen aanschaft, omdat gegevens verouderd zijn, of omdat wetgeving dit voorschrijft (denk aan de AVG-richtlijnen).



Het belang van datavernietiging

Het is dan belangrijk om (verouderde) data veilig en volledig te vernietigen. Daar is een reden voor. Als jouw gegevens ten eerste in verkeerde handen vallen, kan dat schadelijk zijn voor jou en jouw organisatie. Want de informatie op die oude harde schijf kan voor jou wel verouderd zijn, voor een ander hoeft dat niet zo te zijn. Je voorkomt met datavernietiging dus (on)bedoelde datalekken en misbruik van informatie.

Bovendien is er de afgelopen jaren meer aandacht gekomen voor privacybescherming en datalekken. Door nieuwe wetgeving (vooral de AVG uit 2018) moeten persoonsgegevens beter beschermd worden, en dat betekent dat data ook zorgvuldig moet worden vernietigd. Houd je je niet aan die regelgeving? Dan kan dat leiden tot forse geldboetes of strafrechtelijke processen, nog los van enorme reputatieschade en nadelige gevolgen voor de betrokkenen.

Data vernietigen of verwijderen

Bedenk daarbij dat data verwijderen zeker niet hetzelfde is als data vernietigen. Wanneer je zelf bestanden verwijdert van jouw computer of telefoon, zijn ze met bepaalde software alsnog terug te halen. Wil je ervoor zorgen dat jouw gegevens echt weg zijn en voorkomen dat persoonsgegevens of bedrijfsdata in de verkeerde handen vallen? Dan is professionele datavernietiging nodig.

Hetzelfde geldt voor cloudopslag. Heb je de gegevens van jouw datadrager vernietigd? Dan bestaat de kans dat er nog een kopie van de gegevens ergens in de cloud staat en dat de gegevens dus niet volledig vernietigd zijn.

Datavernietiging in Nederland

Uit de bevindingen van datavernietiging in Nederland, blijkt dat ruim 70% van de ondervraagde bedrijven gebruik maakt van datavernietiging. Het gaat daarbij vooral om harde schijven (92%), usb-sticks (38%) en telefoons (19%). In de meeste gevallen gaat het om het vernietigen van commerciële gegevens (61%) en financiële gegevens (55%), en in mindere mate gaat het om data van derden of klanten. Daarnaast geeft 30% van de bedrijven aan nog geen gebruik te maken van datavernietiging, terwijl het belangrijk is om een goed beleid te hebben voor gegevensvernietiging, i.v.m. gevolgschade, boetes en aansprakelijkheid (AVG).

Wat zijn de mogelijkheden en waar moet je op letten als je als organisatie jouw (verouderde) data veilig en volledig wilt verwijderen? In deze whitepaper lees je daar meer over. In het volgende hoofdstuk gaan we uitgebreider in op het vernietigen van data, en daarna volgt een overzicht van aandachtspunten voor professionele datavernietiging.

Data vernietigen

Gegevens zijn waardevol en moeten ook zo behandeld worden. Waar je geld niet zomaar op straat gooit maar juist veilig opbergt in een kluis of bij de bank, moet dat met (afgedankte) data en datadragers ook. Maar welke mogelijkheden heb je om jouw data volledig te vernietigen als je het niet meer nodig hebt? Daarvoor worden verschillende methodes gebruikt, die allemaal hun voors en tegens hebben.

Verwerkingsmethodes

Er zijn globaal 4 manieren om elektronica en de informatie daarop te verwerken: de gegevens verwijderen, versleutelen, overschrijven of vernietigen, waarvoor verschillende technieken worden gebruikt. Hierbij geldt – zoals in het vorige hoofdstuk al bleek – dat verwijderen iets anders is dan vernietigen. Niet alle methodes garanderen dus de vernietiging van data.

Verwijderen

De eerste methode om gegevens van een datadrager te verwijderen is op de 'delete-knop' drukken. Dit is op geen enkele manier aan te raden, omdat de gegevens weliswaar weg lijken te zijn, maar dat dus absoluut niet zijn. Het enige wat namelijk gebeurt, is dat de verwijzing naar de informatie verwijderd wordt. Met herstelsoftware is het dan mogelijk om de informatie alsnog terug te krijgen.

Eigenlijk verdient het (op het oog) verwijderen van gegevens dus geen plaats in deze lijst, omdat de gegevens op geen enkele manier verwerkt worden of zijn. Het staat hier dus meer als waarschuwing dan als realistische optie.

Versleutelen

Een tweede methode is het versleutelen van gegevens. Daarmee vernietig je geen gegevens, maar je bouwt wel een 'barrière' in: het moet eerst ontsleuteld worden voordat je het weer kunt gebruiken. Gegevens die (per ongeluk) op straat eindigen, kunnen dan niet zomaar gebruikt worden. Ook als er in een ander vernietigingsproces iets misgaat, kan versleuteling de kans op misbruik verkleinen.

Het voordeel is dat iedereen data kan versleutelen, en eigenlijk zou iedereen daarom een versleutelingsmethode moeten gebruiken. De keerzijde is wel dat je data dus niet weg zijn en dat de gegevens na ontsleuteling alsnog bruikbaar worden. Het biedt dus eerder 'extra waarborg' dan 'volledige veiligheid'.

Gegevens versleutelen kan met gratis versleutelingssoftware, zoals WinRAR, 7-zip en AESCrypt. Maar ook het beveiligen van bestanden in Office-programma's zoals Word, PowerPoint en Excel is een vorm van versleuteling.

Overschrijven

Je kunt je data ook overschrijven (wipen). Digitale gegevens zijn feitelijk niet meer dan een verzameling enen en nullen, die een computer kan lezen en vertalen naar voor ons bruikbare informatie. Bij het overschrijven worden die enen en nullen vervangen door willekeurige enen en nullen, waardoor de gegevens worden versnipperd en niet meer te lezen zijn. Ook dit is op zichzelf geen vorm van veilige gegevensvernietiging, want er blijven nog steeds (kleine) stukjes data bestaan. Het kan wel onderdeel zijn van een breder vernietigingsbeleid.

Er zijn verschillende regels of standaarden voor het overschrijven van data, en afhankelijk van de gevoeligheid van informatie kun je dus meer of minder 'uitgebreid' versnipperen. Wil je echt alle gegevens verwijderen, dan dient de data meerdere keren overschreven te worden. Bij een hoge standaard voor dataverwijdering is het soms wel zes of zeven keer. Dat is een tijdrovende klus waarvoor je software kunt gebruiken, maar daarmee kun je niet alle data van harde schijven verwijderen. Vaak heeft een harde schijf namelijk beveiligde delen waar de software niet bij kan. De methode van overschrijven is dus maar deels betrouwbaar.

Een programma dat veel gebruikt wordt voor het overschrijven van data is Blancco. Maar er is ook andere software, zoals MiniTool Partition Wizard of Disk Wipe, Maar ook bij het resetten van de Windows-pc kun je ervoor kiezen om jouw gegevens direct te overschrijven.

Demagnetiseren

Hier maken we langzaam de stap naar het vernietigen van data. Sommige gegevensdragers (zoals harde schijven, tapes en bankpasjes) hebben een magnetisch veld. De volgorde van die kleine magnetische stukjes kunnen enorm veel binaire informatie (enen en nullen) opslaan. Maar dan moeten die stukjes wel in een specifieke volgorde worden bewaard. Als je de gegevensdrager langs een sterk magnetisch veld haalt, gaat de magnetische binding weg en kun je de magnetische stukjes niet meer ordenen. De schijf werkt dan in principe niet meer en het is onmogelijk om de gegevens op te halen.

Er is wel een voorbehoud: demagnetiseren (degaussing) werkt alleen bij magnetische schijven. Solid State-Drives (SSD) moeten op een andere manier vernietigd worden. Bovendien heb je hier krachtige magneten nodig en kun je niet meteen zien of het demagnetiseren heeft gewerkt. Daarom moet de harde schijf weer getest worden, en dat maakt de methode omslachtig.

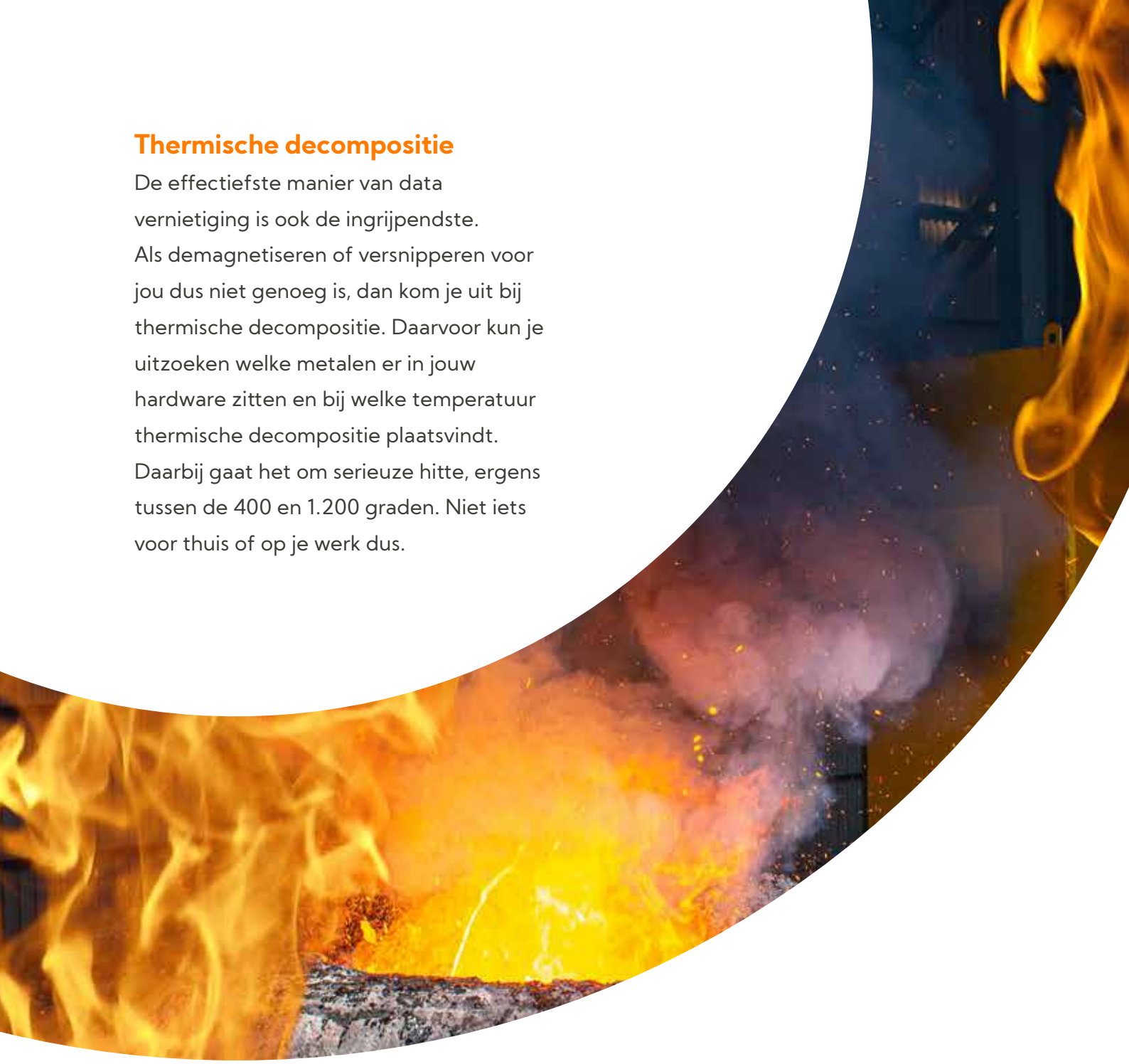
Ook bij kassa's in winkels heb je vaak magnetische velden om de beveiliging van producten te demagnetiseren. Vaak zie je daar een sticker staan met de mededeling dat je jouw telefoon of bankpas niet op de toonbank moet leggen. De reden is dat daardoor mogelijk de informatie op jouw pas of telefoon onleesbaar wordt.

Mechanische vernietiging

Demagnetiseren kan dus een goede optie zijn, maar het werkt niet bij Solid State-drive (SSD). De enige optie in dit geval is het mechanisch vernietigen van de gegevensdrager. En als je ook bij magnetische en optische media zeker wilt zijn dat je gegevens écht weg zijn, is vernietiging de enige garantie. Daarbij zijn er speciale procedures en specificaties die tot op de millimeter nauwkeurig aangeven hoe klein de stukjes en hoe groot de snijhoeken moeten zijn. Dat vernietigen kan vervolgens op verschillende manieren plaatsvinden, zoals verbranden of -in de meeste gevallen- versnipperen: Maar ook hierbij geldt: mechanische vernietiging maakt het een stuk lastiger om informatie te achterhalen, maar het is niet onmogelijk. De informatie is er immers nog steeds. Vergelijk het met het versnipperen van papier: het wordt op het oog onbruikbaar, maar als je maar voldoende tijd en geduld hebt, kun je er best nog wat van maken.

Thermische decompositie

De effectiefste manier van data vernietiging is ook de ingrijpendste. Als demagnetiseren of versnipperen voor jou dus niet genoeg is, dan kom je uit bij thermische decompositie. Daarvoor kun je uitzoeken welke metalen er in jouw hardware zitten en bij welke temperatuur thermische decompositie plaatsvindt. Daarbij gaat het om serieuze hitte, ergens tussen de 400 en 1.200 graden. Niet iets voor thuis of op je werk dus.



Dus één van de methoden om jouw data volledig te vernietigen, is met behulp van thermische decompositie.
Door te verhitten tot een ontledingstemperatuur, worden chemische bindingen afgebroken. Zo weet je zeker dat er van jouw data en datadrager niets overblijft.

Normen, eisen en certificaten

Als je jouw data en datadragers veilig en volledig wilt verwijderen, dan is het belangrijk om hiervoor een professionele organisatie in te schakelen. Zo weet je dat jouw gegevens vertrouwelijk worden ingezameld, vervoerd en vernietigd. Daarbij kun je gebruikmaken van verschillende eisen, normen en certificaten, waarvan we de belangrijkste hier bespreken.

DIN 66399 Norm

Materiaal Classificatie

Originele grootte Papier, film, drukplaten	**P-1** Strokenbreedte max. 12 mm	**P-2** Strokenbreedte max. 6 mm	**P-3** Snipperformaat max. 320 mm²	**P-4** Snipperformaat max. 160 mm²	**P-5** Snipperformaat max. 30 mm²	**P-6** Snipperformaat max. 10 mm²	**P-7** Snipperformaat max. 5 mm²
Verkleind Microfilm	**F-1** Snipperformaat max. 160 mm²	**F-2** Snipperformaat max. 30 mm²	**F-3** Snipperformaat max. 10 mm²	**F-4** Snipperformaat max. 2,5 mm²	**F-5** Snipperformaat max. 1 mm²	**F-6** Snipperformaat max. 0,5 mm²	**F-7** Snipperformaat max. 0,2 mm²
Optisch CD, DVD, Blu-Ray	**O-1** Snipperformaat max. 2000 mm²	**O-2** Snipperformaat max. 800 mm²	**O-3** Snipperformaat max. 160 mm²	**O-4** Snipperformaat max. 30 mm²	**O-5** Snipperformaat max. 10 mm²	**O-6** Snipperformaat max. 5 mm²	**O-7** Snipperformaat max. 0,2 mm²
Magnetisch Tapes, credit cards	**T-1** Mechanisch niet herkend	**T-2** Snipperformaat max. 2000 mm²	**T-3** Snipperformaat max. 320 mm²	**T-4** Snipperformaat max. 160 mm²	**T-5** Snipperformaat max. 30 mm²	**T-6** Snipperformaat max. 10 mm²	**T-7** Snipperformaat max. 2,5 mm²
Harde Schijven SATA, IDE, SCSI, SAS	**H-1** Mechanisch/ elektronisch niet herkend	**H-2** Beschadigd	**H-3** Vervormd	**H-4** In stukken, vervormd Snipperformaat max. 2000 mm²	**H-5** In stukken, vervormd Snipperformaat max. 320 mm²	**H-6** In stukken, vervormd Snipperformaat max. 10 mm²	**H-7** In stukken, vervormd Snipperformaat max. 5 mm²
Elektronisch USB Sticks, SSD's, memorycards	**E-1** Mechanisch/ elektronisch niet herkend	**E-2** In stukken	**E-3** Snipperformaat max. 160 mm²	**E-4** Snipperformaat max. 30 mm²	**E-5** Snipperformaat max. 10 mm²	**E-6** Snipperformaat max. 1 mm²	**E-7** Snipperformaat max. 0,5 mm²

DIN 66399

De DIN 66399 is opgesteld door het Deutsches Institut für Normung en beschrijft de vereisten om verschillende soorten datadragers te vernietigen. De norm bestaat uit zes categorieën datadragers, en elke datadrager kan vervolgens vernietigd worden in zeven veiligheidsniveaus. Die zeven veiligheidsniveaus vallen dan weer onder drie beschermingsklassen.

WEEELABEX certificering / CENELEC Confirmity

Er is ook een CENELEC Confirmity. CENELEC (voluit Comité Européan de Normalisation Electro technique) is een initiatief van Europese inzamelsystemen. Het legt het minimale kwaliteitsniveau vast voor inzameling, opslag, transport, recycling en hergebruik van e-waste. Deze certificering is verplicht voor bedrijven die werken met digitale datavernietiging. Veel bedrijven voldoen niet aan deze standaarden, want je moet aan veel zaken voldoen om dit certificaat te krijgen.

6 materiaalclassificaties

Er zijn zes materiaalclassificaties. In combinatie met de beveiligingsklasse en het veiligheidsniveau ontstaat vervolgens een tabel met normen, waarin de maximaal materiaaldeeloppervlakte staat. De gegevens kunnen op de volgende datadragers staan:

P. Origineel formaat, zoals papier
F. Verkleind, zoals microfilms en folies
O. Optische datadragers, zoals cd's en dvd's
T. Magnetische datadragers, zoals diskettes en id-kaarten
H. Harde schijven (HDD)
E. Elektronische datadragers, zoals usb-sticks, chipkaarten en geheugenkaarten

7 veiligheidsniveaus

Vervolgens kun je kiezen uit zeven veiligheidsniveaus. Hoe hoger het niveau is, hoe kleiner de fractie:

Niveau 1. Algemene documenten
Niveau 2. Interne documenten
Niveau 3. Gevoelige, vertrouwelijke en persoonsgegevens
Niveau 4. Zeer gevoelige, vertrouwelijke en persoonsgegevens
Niveau 5. Geheime gegevens
Niveau 6. Hoogst geheime gegevens
Niveau 7. Strikt geheime gegevens

De gangbare vernietingsmethodes halen veiligheidsklasse 4 of 5. Dit betekent dat met de juiste kennis en apparatuur nog data uitleesbaar is. De bestaande methodes vormen dus een risico voor de privacy van jou(w organisatie).

3 beschermingsklassen

Tot slot zijn er drie beschermingsklassen te onderscheiden:

Klasse 1. Normale bescherming van gegevens. Deze gegevens zijn voor veel mensen toegankelijk en publicatie heeft weinig impact. Wel moeten persoonlijke gegevens ook hierbij worden beschermd. Hieronder vallen veiligheidsniveaus 1, 2 en 3.

Klasse 2. Hoge bescherming van vertrouwelijke gegevens. Bij deze gegevens kan een beperkt aantal mensen komen, en verspreiding ervan kan schadelijk of strafbaar zijn. Hieronder vallen veiligheidsniveaus 3, 4 en 5.

Klasse 3. Zeer hoge beveiliging voor vertrouwelijke en geheime gegevens. Hier kunnen weinig mensen bij, en publicatie kan ernstige gevolgen hebben. Hier gaat het vaak ook om geheimhoudingsplichten op grond van wetten en contracten. Hieronder vallen veiligheidsniveaus 5, 6 en 7.

10 aandachtspunten voor jouw datavernietiging

Steeds meer organisaties worden geconfronteerd met datavernietiging, mede door de strengere privacywetgeving, aansprakelijkheid en imago schade. Dat betekent dat je als organisatie gevoelige bedrijfs- en persoonsgegevens op harde schijven, usb-sticks of andere hardware goed en volledig
moet verwerken. Je wilt immers niet dat die gegevens in verkeerde handen vallen.
Voor het vernietigen van data zijn verschillende methodes, zoals versleutelen, overschrijven, demagnetiseren, mechanisch vernietigen of thermische decompositie. Niet al deze methodes zijn echter even effectief en betrouwbaar, omdat er mogelijk 'stukjes data' achterblijven die mogelijk uitleesbaar zijn.

Om te voldoen aan de wettelijke normen van data vernietigen en te garanderen dat jouw data veilig en volledig vernietigd worden, kun je de onderstaande tips gebruiken.

1 Weet wat er van jou wordt verwacht.

Allereerst is het belangrijk om je te verdiepen in de wet- en regelgeving waar je aan moet voldoen. Dat betekent onder andere dat je weet welke informatie op jouw datadragers staan, hoe lang je die gegevens mag bewaren, hoe je die moet (laten) vernietigen en welk 'bewijsmateriaal' je daar vervolgens van moet hebben. Dit is voor elk bedrijf anders, maar de AVG-wetgeving biedt een hoop inzichten.

2 Houd zicht op (oude) datadragers.

Zorg dat je weet welke datadragers in jouw organisatie gebruikt worden, en laat oude laptops, telefoons, harde schrijven en usb-sticks niet rondslingeren. Als je een duidelijk overzicht hebt van wie welke apparaten heeft en waar die zich bevinden, voorkom je dat datadragers 'zoekraken' en dat informatie (on)bewust op straat belandt.

3 Stel vernietiging niet uit.

Heb je afgedankte hardware liggen? Zorg dan dat ze in een kluis of afgesloten ruimte liggen, totdat je het definitief verwijderd. Je hoeft natuurlijk niet voor elke usb-stick een vernietigingsbedrijf te laten komen, maar weet wel dat je verantwoordelijk bent voor de datadrager zolang je geen bewijs van vernietiging hebt.

4 Kies een soort datavernietiging.

Als je weet welke data jij bewaart en op welke datadragers, dan kun je kijken aan welk veiligheidsniveau je moet (of wilt) voldoen. Daar kun je vervolgens een passende vernietigingsmethode bij zoeken. In het algemeen geldt hier: je kunt beter te hoog dan te laag inzetten.

5 Denk aan het milieu.

Niet alleen de productie van hardware, maar ook het vernietigen daarvan is schadelijk voor het milieu. Bovendien bevat hardware vaak zeldzame metalen. Hoe meer we daarvan kunnen hergebruiken, hoe minder we hoeven te delven. Kijk bij data- en hardwarevernietiging dus goed of metalen en kunststoffen worden gescheiden en hergebruikt kunnen worden en of er geen schadelijke stoffen in de lucht, (ZZS), op het land of in het water terechtkomen. Dat kan bijvoorbeeld door te controleren of de datavernietiger handelt in lijn met het Schone Lucht Akkoord (SLA).

6 Check de certificering.

Er zijn veel kopers van gebruikte hardware en datavernietigers op de markt. Helaas gaan zij niet allemaal even goed met jouw apparaten en gegevens om. Controleer daarom goed hoe veilig en volledig een bedrijf data vernietigt en hoe betrouwbaar het dus is. Dat kan bijvoorbeeld door te kijken naar de certificering, CENELEC of de gehanteerde DIN 66399-norm.

7 Zorg voor een bewijs van gegevensvernietiging.

Een goede administratie kan tot slot de redding zijn als het gaat om aansprakelijkheid. Kun jij aantonen dat jouw data inderdaad veilig en volledig vernietigd zijn?
Dan verklein je de kans dat jij aansprakelijk wordt gehouden bij een privacy-issue. Als je met een professionele partij zaken doet, ontvang je een gecertificeerde verklaring met informatie over de datavernietiging. Zo'n certificaat heeft een uniek serienummer.

8 Vraag om foto- of videobewijs en logboeken.

Een andere manier om bewijs te krijgen van de vernietiging van jouw data is met foto's of video-opnames. Overigens vind je op veel websites van datavernietigers ook beeldmateriaal van het vernietigingsproces. Zo kun je een goed beeld vormen van hoe dat gaat. Vraag ook inzage in logboeken. Daarbij kun je specifiek kijken naar veilig transport, het volgen van het proces, de opslag van hardware en de behandeling (vernietigingsmethode).

9 Vergeet 'opslag elders' niet.

Naast de opslag op jouw eigen gegevensdragers, is de kans groot dat je ook gegevens 'in de cloud' hebt staan. Houd er bij het zoeken naar een cloudserviceprovider rekening mee dat ook die voldoet aan jouw normen voor gegevensvernietiging. Je kunt prima vragen naar het beleid en de normen voor verwijdering, overschrijving en gegevensvernietiging die zij gebruiken, inclusief in welk rechtsgebied jouw gegevens worden gehost.

10 Ga voor zekerheid.

Met gevoelige informatie kun je het beste de veilige route kiezen.
Ga dus voor zekerheid, bijvoorbeeld met de volgende stappen:

1. **Versleutel allereerst de data op de gegevensdrager (dat kan zelf)**
2. **Overschrijf vervolgens de gegevens (ook dit kan je zelf doen)**
3. **Bewaar de gegevensdrager op een veilige en afgesloten plaats**
4. **Laat de gegevensdrager gecertificeerd vernietigen volgens een zo hoog mogelijke standaard.**

Zo weet je zeker dat de gegevens niet te achterhalen zijn en dat alle informatie veilig en volledig wordt vernietigd.

Hulp bij datavernietiging?

Heb jij te maken met (gevoelige) data die je veilig en volledig wilt laten vernietigen? Dan helpen bovenstaande tips je hopelijk bij het maken van een goed beleid. Heb je nog vragen of wil je meer weten over hoe je jouw elektronisch afval milieuvriendelijk, veilig en volledig kunt verwerken, volgens het hoogste veiligheidsniveau? Neem dan vrijblijvend contact met ons op.

Datavernietiging volgens Wee do it

Wee do it zet de nieuwe norm voor datavernietiging. Dankzij de innovatieve verwerkingsmethode garanderen we milieuvriendelijke en volledige datavernietiging.

Wee do it in de media

- Weedoit Animatie Video
- SamenSnellerDuurzaam Bedrijven
- SamenSnellerDuurzaam Particulieren

Contact

Heb je vragen of wil je nog meer weten, neem dan geheel vrijblijvend contact met ons op.

info@weedoit.nl
085 – 0134710
www.weedoit.nl

WEEELABEX CONFORMITY & VERIFICATION

CENELEC EUROPEAN COMMITTEE FOR ELECTROTECHNICAL STANDARDIZATION

niwo gecertificeerd

100% data weg garantie

Jouw e-waste zorgvuldig ingezameld & verwerkt

Elektronisch afval bevat schadelijke, Zeer Zorgwekkende Stoffen (ZZS-stoffen), zoals zware metalen, halogenen en vlamvertragers.
Bovendien bevat elektronica vaak (bedrijfs)gevoelige data.

Daarom is het belangrijk dat we elektronica apart, volgens speciale procedures en in lijn met nationale en internationale wetgeving inzamelen, sorteren, demonteren en verwerken.

Wee do it verzorgt de inzameling, verwerking en vernietiging volledig en secuur, in 3 stappen. Zo ben je volledig ontzorgd en garanderen we dat de giftige stoffen niet in het milieu terechtkomen en jouw gevoelige data niet op straat eindigen.

1 Jouw e-waste veilig ingezameld

Wee do it verzamelt elektronisch afval voor producenten en gebruikers. Dankzij de VIHB-registratie zijn we bevoegd elektronisch afval in te zamelen en te vervoeren. Zo garanderen we dat jouw elektronisch afval veilig en zorgvuldig wordt ingezameld.

Waar de meeste datavernietigers elektronica ter plaatse vernietigen, brengen wij jouw data gratis naar onze eigen locatie voor een veilige verwerking. Zo voorkomen we dat Zeer Zorgwekkende Stoffen in de leefomgeving terechtkomen. Dankzij ons eigen vervoer met Track & Trace is jouw data bovendien volledig volgbaar en jouw veiligheid gegarandeerd.

2 Verwerking van jouw e-waste

Na(ast) inzameling zorgt Wee do it ook voor de verwerking van e-waste. Na de inzameling sorteren en demonteren we het elektronisch afval. Dat gebeurt in eigen beheer in sociale werkvoorzieningen (WEEELABEX/CENELEC gecertificeerd) binnen Nederland, volgens strenge normen en richtlijnen.

Zo helpen we niet alleen het milieu, maar ook mensen met een afstand tot de arbeidsmarkt.

3 Verwerking en recycling van jouw e-waste

Na het sorteren en demonteren vernietigen we het elektronisch afval volledig, duurzaam, veilig en niet-vervuilend. Dat gebeurt via thermische decompositie en is in lijn met de emissie-eisen (ZZS) en het Schone Lucht Akkoord (SLA). We verleggen bovendien de grenzen van de bestaande veiligheidsnormering en behalen als enige bedrijf in Europa beschermingsklasse 3 met een veiligheidsniveau "7+". We vernietigen de data voor de volle 100% door het opheffen van het magnetisme, volledige demontage en thermische decompositie.

Vernietigingscertificaat

(Waarom) werken met Wee do it: 5 redenen

De datavernietiging vindt plaats in eigen beheer.
Na het inzamelen en vernietigen van jouw elektronica en data ontvang je van ons een digitaal Wee did IT-vernietigingscertificaat.

Dat is het bewijs dat de aangeboden data volledig en op milieuvriendelijke wijze zijn vernietigd.

1 Jouw data volledig verwerkt

dankzij de nieuwste, unieke technieken voldoen we aan de hoogste veiligheidsklasse (“7+”) en worden de data voor de volle 100% vernietigd. Zo weet je zeker dat al jouw (gevoelige) informatie verwijderd is. Als bewijs ontvang je na vernietiging het Wee did IT-certificaat.

2 Schoon vernietigingsproces

wij verwerken elektronisch afval via thermische decompositie milieuvriendelijk en deskundig, in lijn met de emissie-eisen en het Schone Lucht Akkoord (SLA).
Na vernietiging brengen we de grondstoffen terug in de cirkel.
Zo blijven er geen reststoffen over en eindigen giftige stoffen (ZZS-stoffen) niet in de natuur en in ons voedsel.

3 Volledig ontzorgd, veilig en volgbaar

we ontzorgen je van a-tot-z. We halen jouw elektronisch afval gratis bij je op, en met een Track & Trace kun je de route naar ons eigen sorteer- en demonteercentrum volgen. Tot slot zorgen wij ook voor volledige verwerking zonder dat je hiernaar hoeft om te kijken.

4 We werken volgens de strengste richtlijnen en normen en zijn onafhankelijk

gecertificeerd. Daarmee garanderen we dat onze diensten voldoen aan de hoogste (veiligheids)eisen.
Zo werken we in lijn met de AVG-richtlijnen, hebben we een VIHB-registratie en zijn we WEEELABEX/CENELEC gecertificeerd.

5 We doen het maatschappelijk verantwoord

omdat we alleen samen kunnen werken aan een betere wereld voor mens, dier en milieu.

Contact
info@weedoit.nl
085 – 0134710
www.weedoit.nl