ISACA
Vertrouwen in en waarde uit informatiesystemen
Netherlands Chapter

DATABESCHERMING

Gestandaardiseerd en gecontroleerd vernietigen

Volgens het College Bescherming Persoonsgegevens (CBP) vinden ruim 62.000 datalekken jaarlijks plaats. Misbruik van data en identiteitsfraude kan ernstige gevolgen hebben voor de betrokkenen. Met de aanscherping van de WBP neemt Nederland alvast een voorschot op de Europese verordening die in 2018 in alle lidstaten zal zijn ingevoerd.

comfort-ia

Introductie

Partner Comfort Information Architekts

Penningmeester en vicevoorzitter Nederlands Genootschap Functionarissen voor de gegevensbescherming (NGFG)

Medeoprichter van CEDPO

Oud president European Association for Data Media Security (EA DMS)

Trainer bij IIR en Security Academy

Nationaal en internationaal spreker op congressen

INHOUD

02-05-2016

- Meldplicht datalekken
- Risico’s
- De DIN 66399 als wereldwijde standaard
- Technieken voor het vernietigen van data

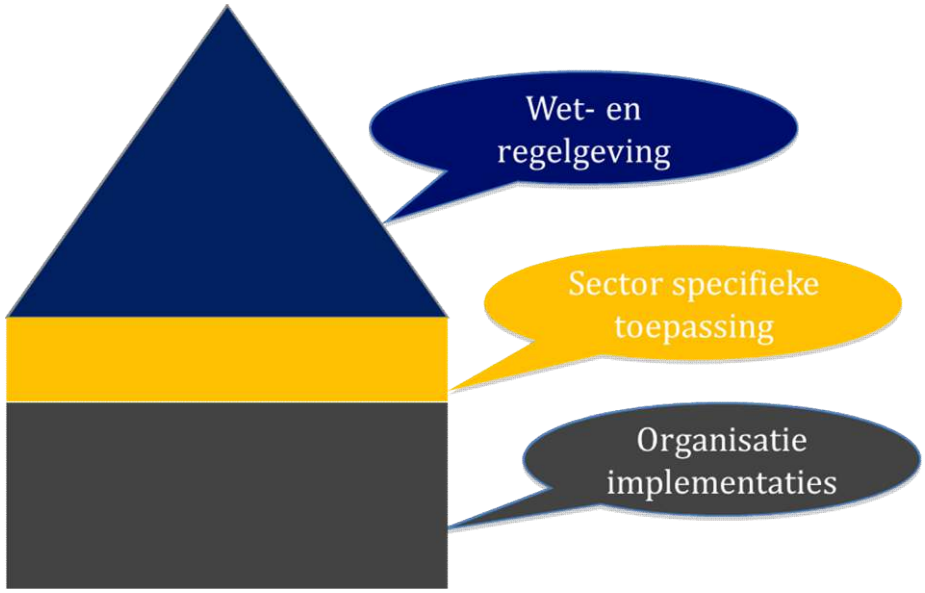
comfort-ia

Incidenten die leiden tot een datalek

- Een aanval op het netwerk
- De diefstal van een Laptop
- Het verlies van een USB stick
- Het openbreken van een kluis
- Het verlies van een mobiele telefoon
- Een gestolen patiënten dossier
- Onjuiste adressering van email of post
- Het inzien van persoonsgegevens door onbevoegde
- Een open papiercontainer in een gebouw met persoonsgegevens
- Het sorteren van papier bij inzamelaar
- Onbevoegde die bij archiefvernietiger persoonsgegevens inzien
- Archiefopslag waar onbevoegden persoonsgegevens inzien
- Datacenter waar een lek in de beveiliging ontstaat
- Tekortschietende beveiliging van persoonsgegevens

Voorbeeld van een datalek

Huis van de privacy



- Doelbinding
- Rechtmatigheid van verwerking
- Verwerking van bijzondere gegevens
- Rechten van betrokkenen op inzage, verzet e.d.

Definities

Persoonsgegeven

- Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijk persoon

Betrokkene

- Degene op wie een persoonsgegeven betrekking heeft

Verantwoordelijke

- Is een entiteit dat, alleen of tezamen met anderen het doel van en de middelen voor de verwerking van persoonsgegevens bepaald

Verwerking

- Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het *verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens*;

Bewerker

- Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen

Zijn er gevoelige gegevens gelekt

1. Aard van persoonsgegevens

- Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp
- Gegevens over de financiële of economische situatie van de betrokkene
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene
- Gebruikersnamen, wachtwoorden en andere inloggegevens
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude
- Beroepsgeheim

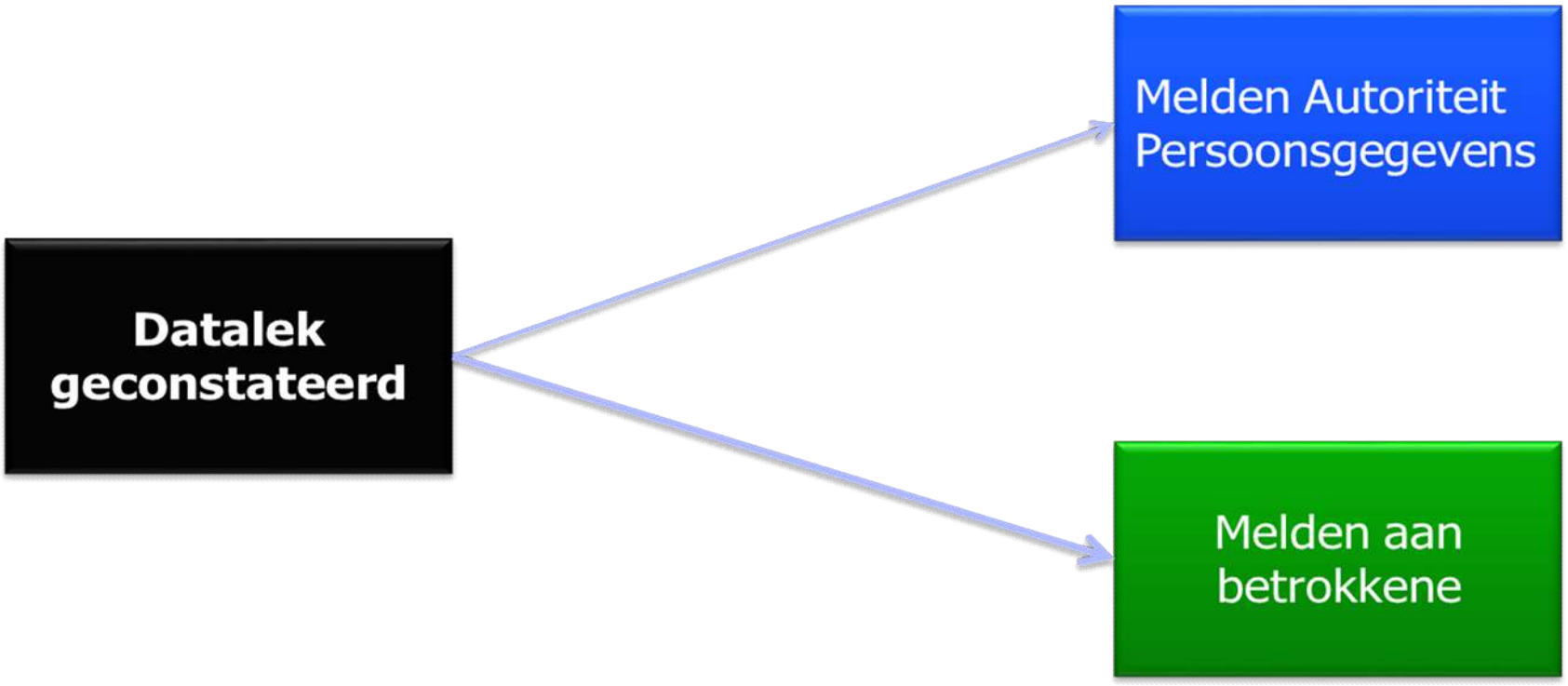
2. Zijn er veel gegevens gelekt

- Weinig of veel gegevens van de betrokkene
- De omvang van groep (aantal betrokkene)

3. Aard van verwerking

- Positie kwetsbare groepen

Datalek geconstateerd en wat nu…



Beveiligingseisen

Passende technische en organisatorische maatregelen

- Tegen verlies van persoonsgegevens
- Tegen onrechtmatige verwerking van persoonsgegevens
- Tegen ongeoorloofde verwerking van persoonsgegevens
- Tegen geoorloofde verstrekking, verspreiding toegang tot of wijziging

Stand van de techniek

- Voorhanden zijnde techniek die qua investering in relatie staat tot het doel

Risico inventarisatie

- Noodzakelijk voor het opstellen van eisen voor de bescherming van persoonsgegevens

Positie van bewerker

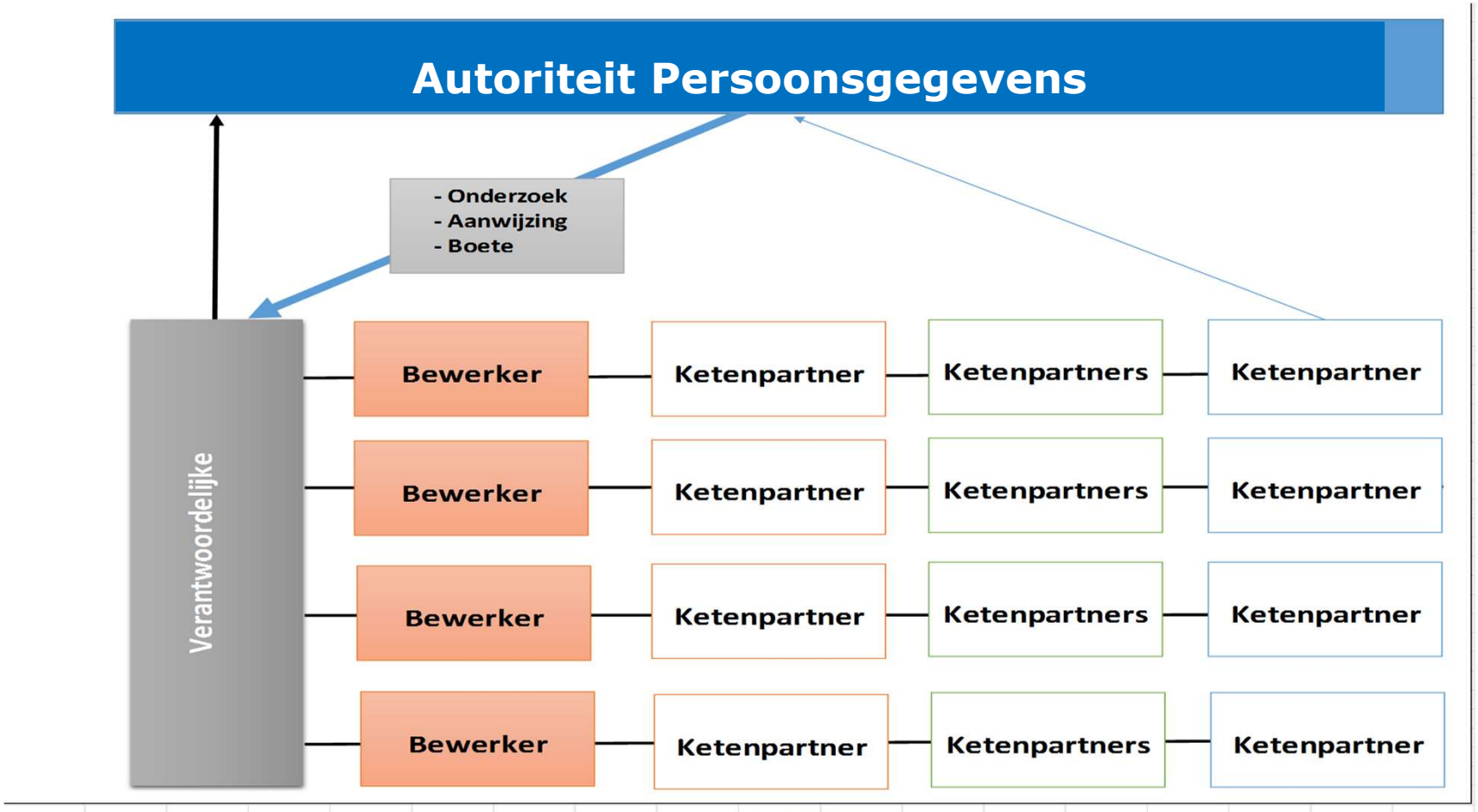
Meer verantwoordelijkheden voor de bewerker op het gebied van

- Communicatie
- Systeemwijzingen
- Beveiligingseisen
- Melden van incidenten (72 uur)
- Risico inventarisatie
- Positie van sub-contractors
- audits

Bewerkersovereenkomst

- Rechten en plichten over en weer
- Gemeenschappelijke zorgplicht tussen verantwoordelijke-bewerker
- Afspraken omtrent verantwoordelijkheden
- Hoe om te gaan met toerekenbare tekortkomingen

Melden en rol van partijen



Bestuurlijke boete van AP

Niet melden van een datalek

- Ernstige verwijdbare nalatigheid
- Verwijtbaarheid van overtreder
- Houdt rekening met omstandigheden
- Boete verhoging (5jaar) of verlaging
- 50% verhoging bij recidive

Wel melden van een datalek

- Eerst bindende aanwijzing van AP
- Afhankelijk van overtreding boete
- Hoor een wederhoor met AP
- Afhankelijk van uitkomst komt boet
- Boete verhoging of verlaging

advies

- Zet een procedure op indien er een datalek ontstaat
- Werk aan bewustwording bij de medewerkers die persoonsgegevens verwerken en beveiligen
- Loop alle bewerkersovereenkomsten na en ga in gesprek met de bewerkers
- Publiceer een heldere en duidelijke privacyverklaring voor alle stakeholders
- Breng de inkoopproces op orde t.a.v. de privacy
- Start met het uitvoeren van PIA’s voor bewerkingen met een hoog risico
- Pas *privacy-by-design* toe in de ontwerp, inkoop en beleidsprocessen
- Ga op zoek naar een FG indien deze na 1 juli 2018 verplicht is

Functionaris voor de Gegevensbescherming (DPO)

Taken	Privacy Officer	Functionaris voor de Gegevensbescherming
Houdt onafhankelijk toezicht op naleving WBP	Neen	Ja
Een openbaar register bijhouden van alle bewerkingen	Neen	Ja
Actief intern onderzoek verrichten	Neen	Ja
Doet aanbevelingen aan verantwoordelijke	Ja	Ja
Klachten bemiddeling en vastlegging (interne en externe klanten)	Ja	Ja
Vraagbaak over de toepassing WBP	?	Ja
Privacy audits	Ja	Ja
Heeft controlebevoegdheden	?	Ja
Rapporteert over bevingen aan de verantwoordelijke	Neen	Ja
Kan aanwijzingen ontvangen van verantwoordelijke	Ja	Neen
Werkt aan een grotere interne Wbp bewustwording	?	Ja
Slagvaardige afwikkeling van geschillen beperkt imago schade	Ja	Ja
FG treed als intermediair op tussen CBP en verantwoordelijke	Neen	Ja
De AP houd afstand vanwege een interen toezichhouder	Neen	Ja

Algemene Verordening Gegevensbescherming

- Is in april 2016 aangenomen door het Europese parlement
- 2 jaar overgangsperiode
- 1 juli 2018 wordt deze van kracht in alle 26 EU landen
- Hij vervangt de huidige Wbp
- Meer harmonisatie tussen EU lidstaten
- Steviger handhaving met boetes tot 20 miljoen of 4% van de w.w. omzet
- Bewerker krijgt zelfstandige verplichtingen en bevoegdheden
- Rechten van betrokken (vergeetrecht)
- Aantoonbare compliance (accountability, privacy by design)
- Documentatieplicht voor verwerkingen
- Data Protection Impact Assessment wordt verplicht voor risicovolle bewerkingen
- Verplichte FG voor overheid, gezondheid, verzekeraars, banken en grote organisaties

Risico’s

comfort-ia

comfort-ia

Schade door datalekken

Schade door datalekken in 2013 met 15% gestegen

mei 7, 2014 Nieuws

Datalekken zorgen voor steeds meer schaden. Een datalek heeft bedrijven in 2013 gemiddeld 2,5 miljoen euro schade opgeleverd. Dit is een stijging van 15% ten opzichte van 2012.

Dit blijkt uit het jaarlijkse Cost of Data Breach-onderzoek dat door Ponemon Institute in opdracht van IBM is uitgevoerd. De schade van een gemiddeld datalek bedroeg 104 dollar per uitgelekt gegeven, een stijging van 9% van opzichte van 2012. Dit betekent dus ook dat de omvang van een gemiddeld datalek is toegenomen.

Cybercrime kost NL 8,8 miljard euro per jaar

Cybercrime kost de Nederlandse economie jaarlijks zo'n 8,8 miljard euro, ofwel ongeveer 1,5 procent van het bruto nationaal product.

In een rapport dat maandag 14 juni 2015 verscheen schrijven zij dat de wereldwijde kosten van cybercrime jaarlijks zeker 325 miljard euro bedragen. Dat is tussen de 0,5 en 0,8 procent van de wereldeconomie en tussen de 15 en 20 procent van de waarde die wordt gecreëerd door het internet.

40% van datadiefstallen met fysieke media

Office-documenten favoriete doelwit aanvallers

vrijdag 25 september 2015, 12:39 door **Redactie**, 0 **reacties**

Microsoft Office-documenten zijn het favoriete doelwit van aanvallers die bij bedrijven en organisaties weten in te breken of daar al werken, zo blijkt uit onderzoek (**pdf**) van Intel Security onder meer dan 500 IT-professionals die met tenminste één grote data-inbraak te maken kregen.

De inbraken worden zowel door externe aanvallers als het eigen personeel uitgevoerd. 57% van de aanvallen was het werk van externe aanvallers. De resterende 43% kwam op naam van het eigen personeel. In de helft van deze gevallen was er sprake van opzet, terwijl bij de andere helft van de interne incidenten het onbedoeld was. Bij zowel de interne als externe aanvallers zijn Office-documenten het favoriete doelwit, gevolgd door txt- en csv-bestanden.

In de meeste gevallen bevatten de gestolen bestanden informatie over klanten en werknemers. Een kwart van de data werd gestolen via "tunnelprotocollen" zoals FTP en SCP, terwijl 40% van de datadiefstallen via gestolen fysieke media plaatsvond. In dit laatste geval krijgen organisaties dan ook

Belgische minister Tommelein

privacy is juist veiligheid
vrijdag 25 maart 2016, 11:52

In discussies over privacy zijn er sommige mensen die stellen dat ze niets te verbergen hebben of dat wie niets te verbergen heeft, ook niets hoeft te vrezen, maar dit zijn dooddoeners. Privacy is juist veiligheid, zo stelt **Bart Tommelein**, de Belgische staatssecretaris voor Privacy.

Ook wie niets te verbergen heeft, heeft iets te verbergen, aldus Tommelein. Daarin waarschuwt hij dat wie zijn privacy afstaat, niet alleen zijn vrijheid opgeeft, maar ook zijn veiligheid. Volgens Tommelein is privacy een basisrecht, maar geen absoluut recht. Het is dan ook een kwestie van afwegen.

Autoriteit persoonsgegevens

Gemeenten onzorgvuldig bij uitwerking privacyregels sociaal domein

Persbericht/19 april 2016

Categorie: Sociaal domein

Nederlandse gemeenten weten onvoldoende welke persoonsgegevens van hun burgers zij in het sociaal domein mogen verwerken en welke regels daarvoor gelden. Bovendien informeren gemeenten hun burgers niet goed over het gebruik van hun persoonsgegevens. Dat constateert de Autoriteit Persoonsgegevens na onderzoek bij 41 gemeenten.

AUTORITEIT
PERSOONSGEGEVENS

comfort-ia

80% van alle fraude intern!

Houd de fraudeur!

Fraude? Bij ons niet hoor! Maar wist u dat ruim de helft van alle organisaties de afgelopen jaren te maken heeft gehad met fraude en dat 80 procent van alle fraude wordt gepleegd door managers en het eigen personeel? Maatregelen tegen interne maar ook externe fraude worden vaak pas genomen als er iets mis is gegaan. Met de Schriftelijke cursus Anti-fraude professionaal krijgt u alle instrumenten aangereikt om fraude(risico's) in uw organisatie te identificeren, te analyseren en te minimaliseren. De auteurs hebben zich mede gebaseerd op de eisen die de Association of Certified Fraud Examiners (ACFE) - de grootste fraudebestrijdingorganisatie ter wereld - stelt aan de titel Certified Fraud Examiner (CFE). De auteurs staan borg voor een hoog kwaliteitsniveau van de lessen en bieden een breder en diepgaander inzicht in fraudemanagement dan de Amerikaanse certificering u biedt.

Grondstoffenhandelaren en de risico's

za 12 jun 2010, 05:30 | lees voor

Kassa voor vuilnismannen

door Bart Mos

AMSTERDAM - Twee vuilnismannen van vuilverwerkingbedrijf Van Gansewinkel dachten snel rijk te kunnen worden door gebruikte statiegeldbonnetjes en spaarzegels van supermarkten opnieuw in te leveren bij de kassa.

De twee zouden de betrokken supermarkten voor vele tienduizenden euro's hebben opgelicht. Minder slim was dat de twee tegen de lamp liepen en onlangs op staande voet werden ontslagen. Ook deed het bedrijf aangifte tegen de medewerkers. Het politieonderzoek loopt nog.

De betrokkenen vuilnisophalers werkten in de regio Rotterdam voor een divisie van Van Gansewinkel die gespecialiseerd is in het ophalen en vernietigen van vertrouwelijke documenten. Deze divisie verwerkt ook gevoelige papieren voor justitie en enkele andere ministeries.

Naïviteit neemt af

Naïef over fraude

Identiteitsfraude veroorzaakt gigantische schade

Nederlanders zijn zich onvoldoende bewust van het risico dat zij lopen om slachtoffer te worden van identiteitsfraude. Vooral persoonlijke documenten worden vaak bij de normale vuilnis gegooid en kunnen daardoor in verkeerde handen vallen. Dat blijkt uit onderzoek in opdracht van het bedrijf Fellowes.

Uit het onderzoek blijkt dat 68 procent van de Nederlanders niet op de hoogte is van de maatregelen die zij kunnen nemen om identiteitsfraude te voorkomen. Zo gooien negen op de tien ondervraagden gevoelige documenten zoals rekeningen, correspondentie van banken, papieren met pincodes en logincodes weg. Johan Hereijgers, sales- en marketing-manager van Fellowes Benelux, vindt de onwetendheid van veel Nederlanders gevaarlijk. "Mensen die slachtoffer worden van identiteitsfraude lopen gemiddeld vijftigduizend euro schade op, bijvoorbeeld doordat hun creditcard gebruikt wordt door criminelen. Het is echt gevaarlijk om documenten met bijvoorbeeld je handtekening of burgerservicenummer bij je gewone vuilnis te gooien. Zulke documenten kun je beter definitief vernietigen."

Ook de politie neemt het probleem serieus. "We hebben een meldpunt identiteitsfraude ingesteld en we zorgen dat onze experts van de vreemdelingenpolitie hun specifieke kennis over identiteitsfraude delen met de andere collega's", laat een woordvoerder van de Raad voor Hoofdcommissarissen weten. Fellowes organiseert deze week daarom met andere partijen zoals Thuiswinkel.org en de politie de identiteitsfraude preventieweek. Met folders en een website willen ze bewustwording bij de burger creëren.

1100

Voor het onderzoek zijn in totaal 1100 Nederlanders ondervraagd. Ruim drie op de vijf Nederlanders weten niet hoe fraudeurs persoonlijke gegevens kunnen misbruiken.

WOUT MAAS
wout.maas@metronieuws.nl

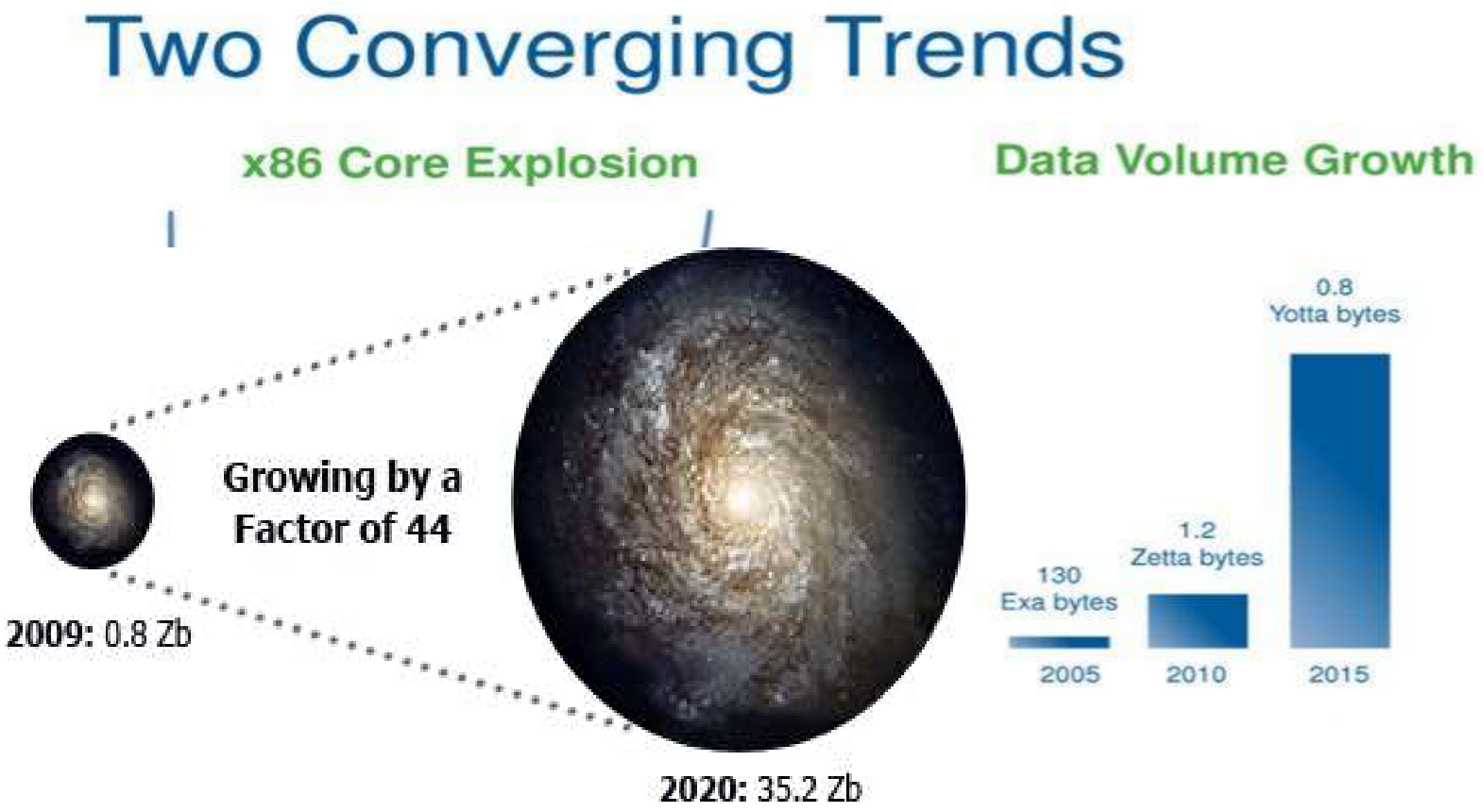
comfort-ia

Dit vraagt naar beleid

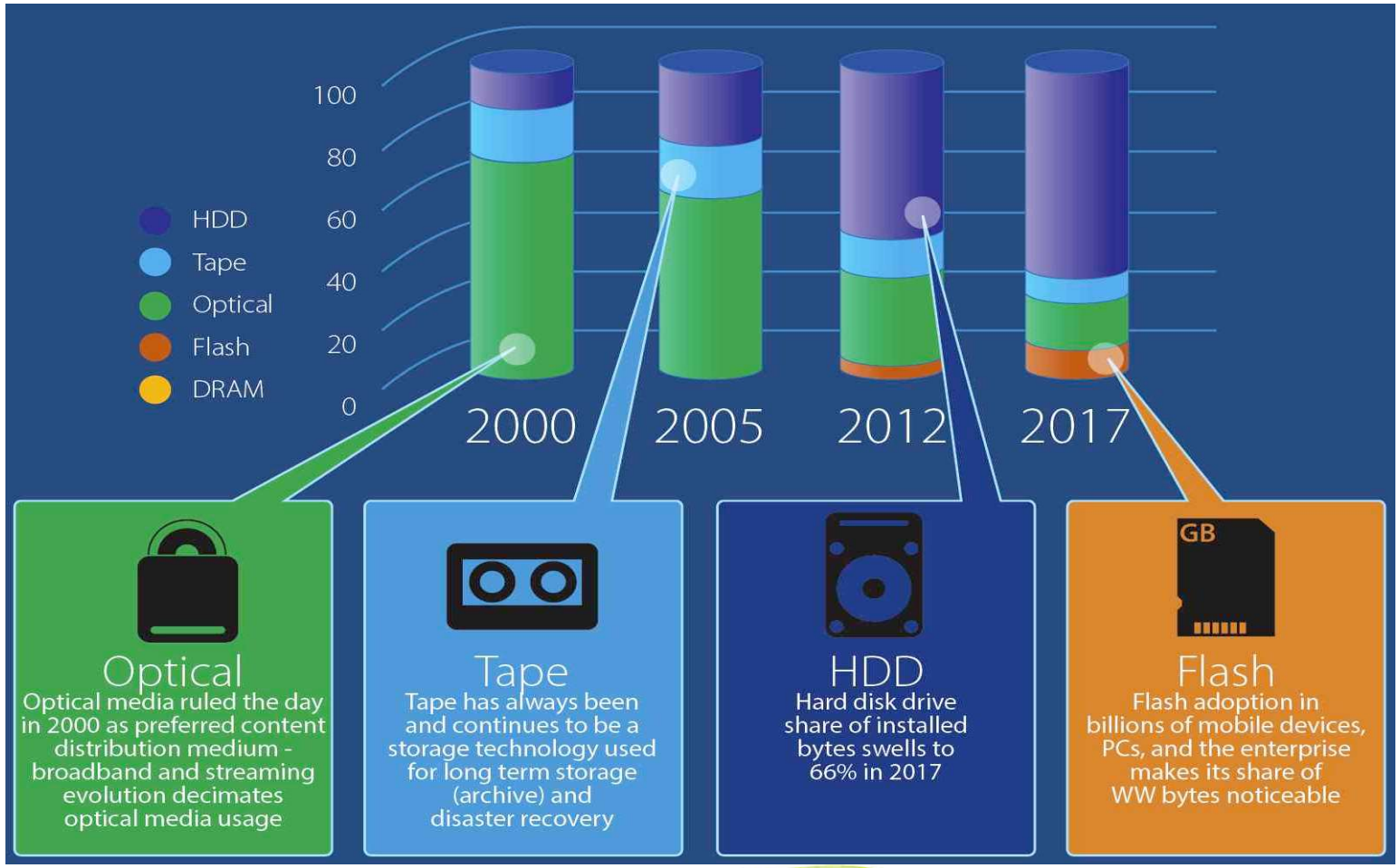
Technologische ontwikkelingen mediadragers

comfort-ia

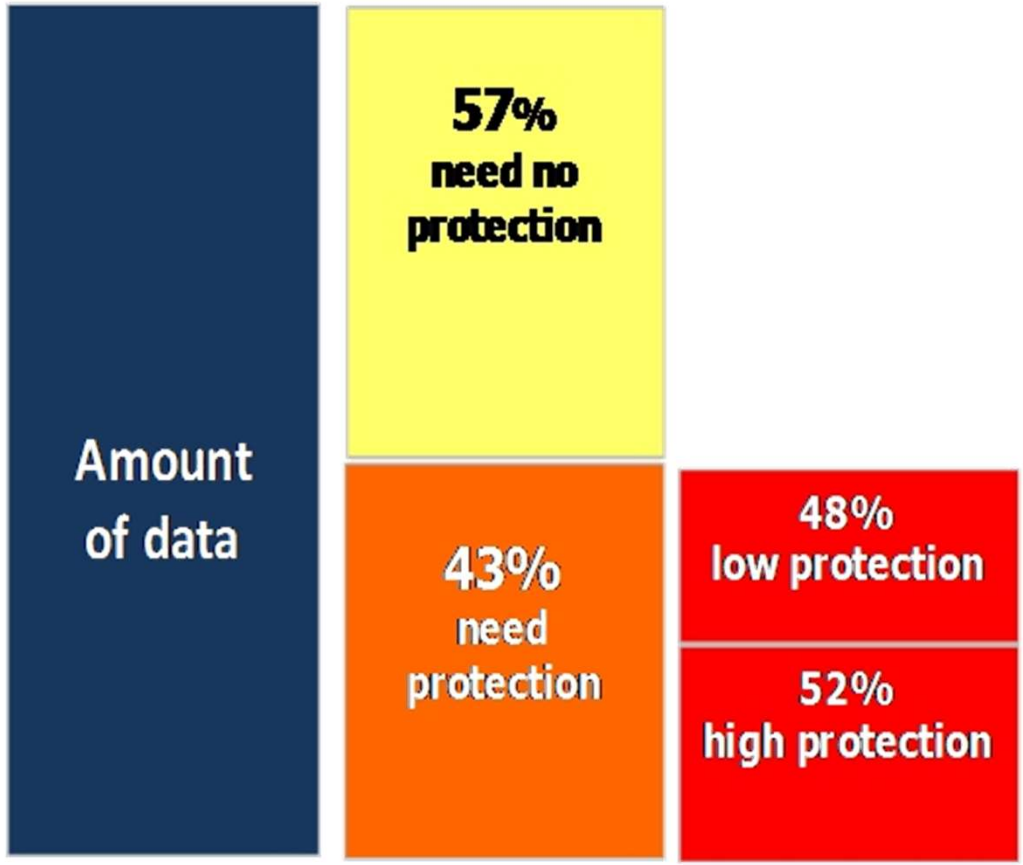
Verwachte groei van data



Groei van type datadragers



Informatiebeveiliging



DIN

Standaard in de bescherming van datadragers

comfort-ia

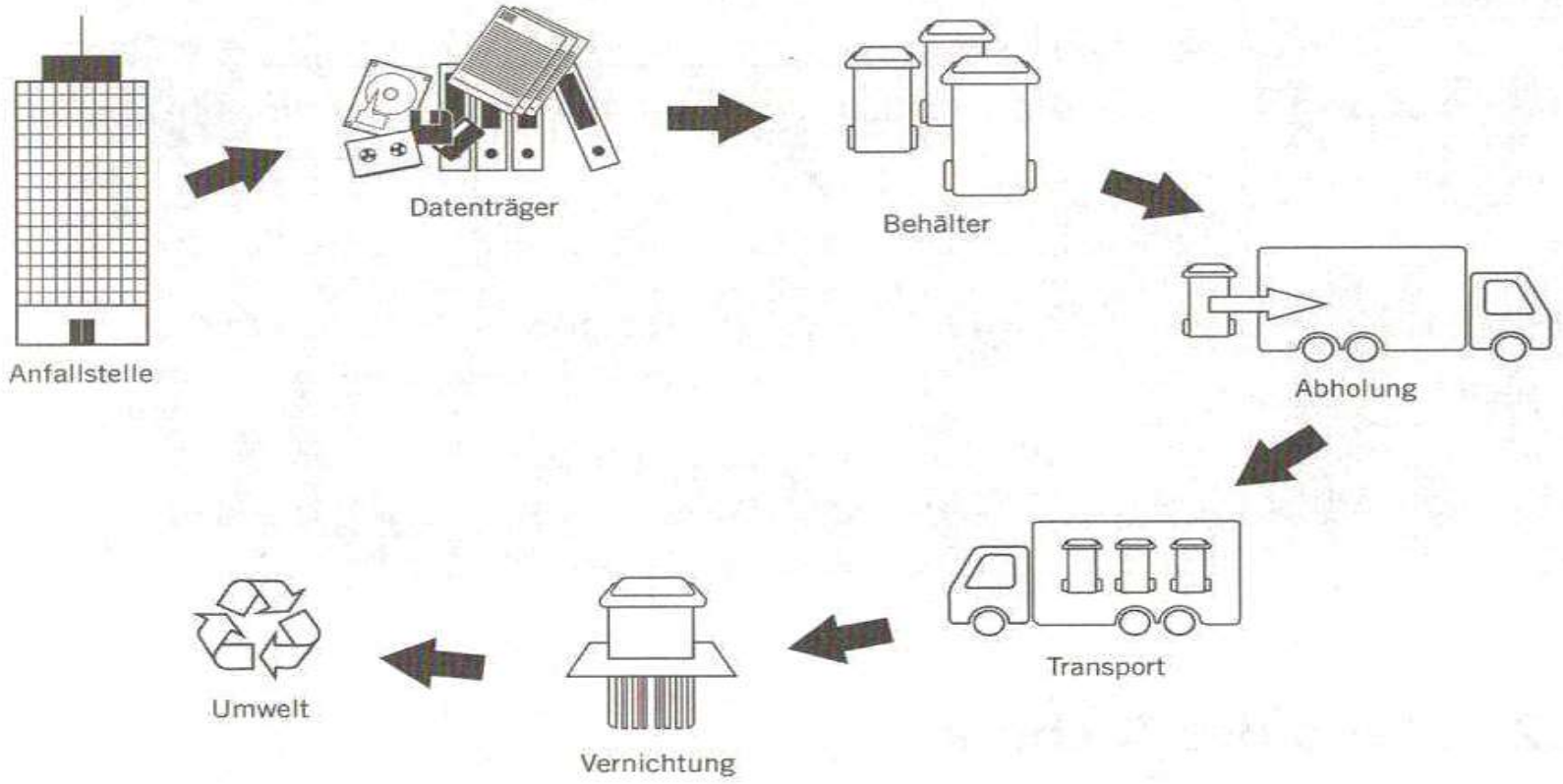
Doelstelling

- Het Duitse instituut voor industriële normeringen ontwierp in 1985 haar eerste vernietigingstandaard, de DIN 32575
- In oktober 2012 ontwierp zij samen met de Duitse industrie een nieuwe norm naar de “laatste stand van de techniek”
- Op termijn wordt dit wederom een Europese standaard
- Het is nadrukkelijk een security standaard voor fysieke datadragers
- Er zijn 6 verschillende categorieën van datadragers
- Het beschermen van de informatie kent 3 niveaus
- Het beveiligen van de datadragers kent 7 categorieën
- Per datadrager is een maximaal toelaatbare afwijking bepaald met een maximale begrenzing naar boven

Keuze bepaling naar beveiligingsniveau

- De “verantwoordelijke” stelt een onderzoek in naar het beschermingsniveau en de veiligheidsklassen
- Hierbij komen de volgende vragen aan de orde:
  - Op welk type datadrager(s) is de informatie vastgelegd?
  - Welke informatie dient beschermd te worden en in welk veiligheidsniveau wordt deze ingedeeld?
  - In welke beveiligingsklasse dienen de datadrager vernietigd te worden
  - Dient de vernietiging direct door de verantwoordelijke op locatie plaats te vinden of door een dienstverlener?
  - Dient de vernietiging op locatie door dienstverlener plaats te vinden, of kan deze extern door dienstverlener uitgevoerd te worden?
  - Welke technisch-, organisatorische- en security maatregelen zijn er getroffen bij overdracht, laden, transport, lossen, sortering, lossen, vernietigingsklasse, afwijkingen, persen, tijdsduur, audits, calamiteiten en kwaliteit/informatie aangaande certificaat?

Het proces van recyclingbedrijven



Het interne proces

1
- Interne inzameling van oude datadragers
- Inzameling in brandvrije containers

2
- Centrale opslag in het gebouw
- Beveiligde ruimte die voor alleen bevoegde toegankelijk is

3
- Vernietiging op locatie volgens vooraf gedefinieerde veiligheidsklasse
- Met eigen apparatuur of door een dienstverlener die onder toezicht de vernietiging uitvoert
- Afvoer van grondstoffen voor opwerking naar nieuwe materialen in EU

In 3 stappen het juiste security niveau

Stap 1

- Bepaal het type informatiedrager dat beveiligd dient te worden door vernietiging

Stap 2

- Bepaal aan de hand van een risico analyse het juiste beschermingsniveau

Stap 3

- Bepaal op basis van het beveiligingsniveau de veiligheidsklasse (mate van verkleining)

Beschermingsniveau

Niveau 1

Algemene informatie

- Beperkte bescherming wenselijk
- Interne informatie, niet geclassificeerd
- Datalekken hebben een beperkte schade
- Niet geschikt voor persoonsgegevens

Niveau 2

Geclassificeerd informatie

- Hoge bescherming gewenst
- Beperkte groep is bekend met de informatie
- Datalekken veroorzaken grote schade
- Geschikt voor persoonsgegevens van beperkte omvang en volume

Niveau 3

Hoog geclassificeerde informatie

- Allerhoogste bescherming gewenst
- Enkele personen zijn bekend met de informatie
- Datalekken veroorzaken een hoge bedreiging voor de organisatie/samenleving
- Geschikt voor omvangrijke persoonsgegevens en grote volume

Veiligheidsklasse

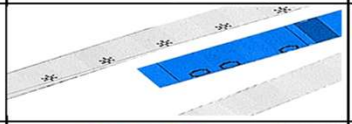
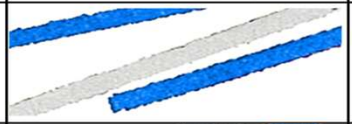
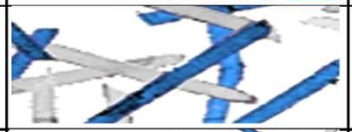
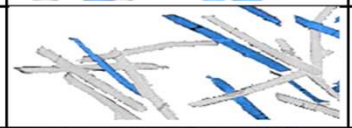
Veiligheidsklasse (mate van verkleining)

Niet veilig ← → Veilig

Veiligheidsniveau	Security klasse 1	Security klasse 2	Security klasse 3	Security klasse 4	Security klasse 5	Security klasse 6	Security klasse 7
1	o[1]	o[1]	o				
2			o	o	o		
3				o	o	o	o

o[1] Niet geschikt voor persoonsgegevens.

Veiligheidsklasse voor papier

Klasse	Toepassing	Snippergrootte	Omschrijving
P - 1 was DIN 1	Wordt geadviseerd voor algemene informatie die onleesbaar gemaakt dient te worden.		Max. snippergrootte **2.000 mm²** of strookbreedte van **≤ 12,0 mm** *(voorbeeld: 11,8 mm stroken)* 10% afwijking tot max. 3.800 mm
P - 2 was DIN 2	Wordt aanbevolen voor interne informatie die onleesbaar gemaakt dient te worden.		Max. snippergrootte is **800 mm²** of strookbreedte van **≤ 6,0 mm** *(voorbeeld: 5,8 en 3,8 stroken)* 10% afwijking tot max. 2.000 mm
P - 3 was DIN 3	Wordt aanbevolen voor algemeen vertrouwelijke informatie die onlees-baar dient te worden.		Max. snippergrootte is **320 mm²** of strookbreedte van **≤ 2,0 mm** *(voorbeeld: 4 x 48 mm snippers)* 10% afwijking tot max. 800 mm
P - 4 **NIEUW**	Wordt sterk aanbevolen voor vertrouwelijke informatie die onleesbaar dient te worden.		Max. snippergrootte is **160 mm²** max. strookbreedte **≤ 6,0 mm** *(voorbeeld: 3,8 x 36 mm snippers)* 10% afwijking tot max. 480 mm
P - 5 was DIN 4	Wordt sterk aanbevolen voor strikt vertrouwelijke informatie die onleesbaar dient te worden.		Max. snippergrootte is **30 mm²** max. strookbreedte **≤ 2,0 mm** *(voorbeeld: 1,9 x 15 mm snippers)* 10% afwijking tot max. 90 mm
P - 6 was DIN 5	Wordt toegepast voor zéér strikt vertrouwelijke informatie die onleesbaar gemaakt dient te worden.		Max. snippergrootte is **10 mm²** max. strookbreedte **≤ 1,0 mm** *(voorbeeld: 0,8 x 12 mm snippers)* 10% afwijking tot max. 30 mm
P - 7 **NIEUW**	Wordt toegepast voor extreem vertrouwelijke informatie die onleesbaar gemaakt dient te worden.		Max. snippergrootte is **5,0 mm²** max. strookbreedte **≤ 1,0 mm** *(voorbeeld: 0,8 x 4,5 mm snippers)* Geen afwijking is toegestaan

Veiligheidsklasse voor 3,5” HDD's

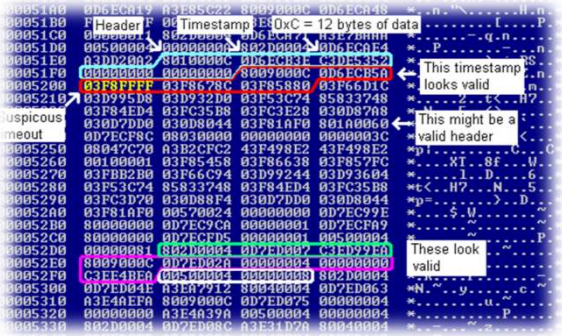
Klasse	Toepassing	Snippergrootte	Omschrijving en toloratie
H - 1	Wordt geadviseerd om algemene informatie zonder classificatie te beschermen.		Mechanische /electrisch onklaar maken
H - 2	Wordt aanbevolen voor interne informatie zonder classificatie te beschermen.		**Datadrager beschadingen**
H - 3	Wordt aanbevolen voor interne informatie zonder classificatie te beschermen.		**Datadrager vervormen**
H - 4	Wordt aanbevolen voor interne informatie zonder classificatie te beschermen.		**Max. snippergrootte is 2.000 mm²** 10% afwijking tot max. 3.800 mm²
H - 5	Wordt sterk aanbevolen om vertrouwelijke geclassificeerde informatie te beschermen.		**Max. snippergrootte is 320 mm²** 10% afwijking tot max. 800 mm²
H - 6	Wordt toegepast voor zéér strikt vertrouwelijke geclassificeerde informatie te beschermen.		**Max. snippergrootte is 10 mm²** 10% afwijking tot max. 30 mm²
H - 7	Wordt toegepast om extreem vertrouwelijke geclassificeerde informatie te beschermen.		**Max. snippergrootte is 5,0 mm²** 10% afwijking tot max. 15 mm²

Toelaatbare afwijking en apparatuur eisen

- Slechts 10% van het vernietigde materiaal mag de maximaal toelaatbare materiaaloppervlakte overschrijden
- De afwijking is per datadrager en per klasse gemaximeerd
- De afwijking wordt door de verantwoordelijke vastgesteld aan de hand van een representatieve steekproef
- Bij off-site vernietiging dient de apparatuur aan bepaalde eisen te voldoen en regelmatig gecontroleerd te worden:
  - Komt de doorvoercapaciteit overeen met de opgave van de fabrikant;
  - Bepaal een procedure voor het vaststellen van vernietigingsklasse;
  - Minimale testhoeveelheid is 10 kg en analyse d.m.v. een zeeftabel

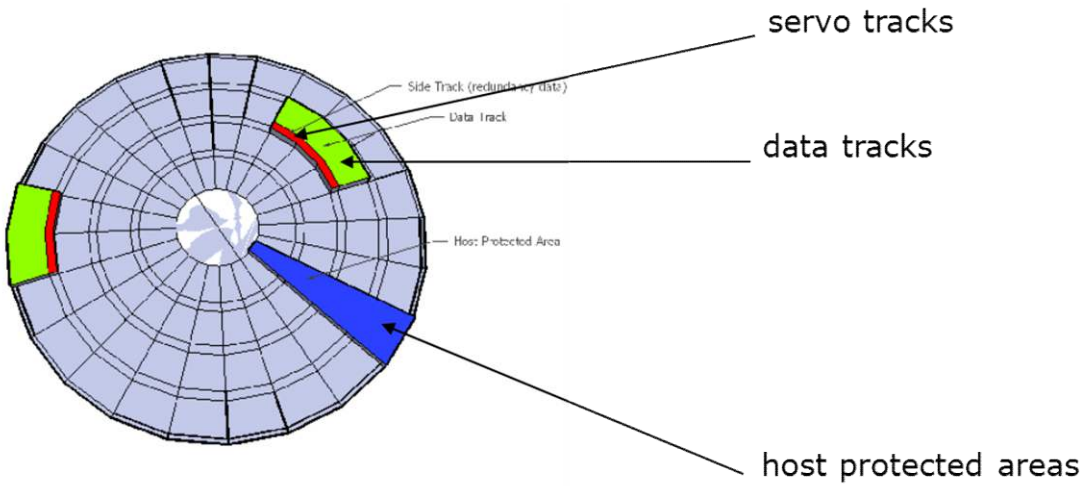
- **Door slijtage, beschadiging en wijziging van zeef en apparatuur kan de mate van verkleining sterk afwijken. Derhalve is regelmatige controle wenselijk**

Techniek van datavernietiging HDD’s



comfort-ia

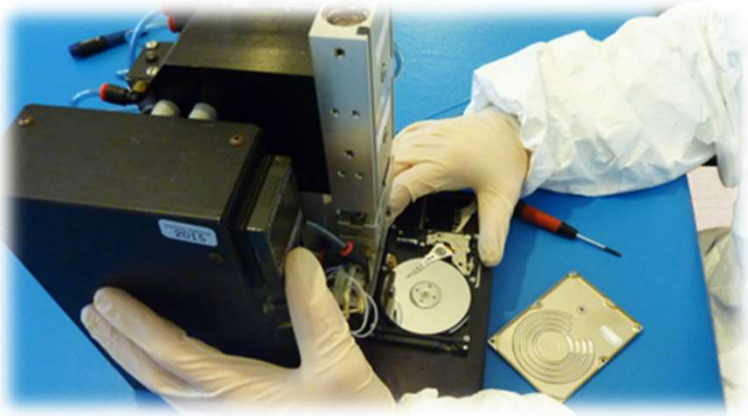
Opslag van data op een HDD



- Servo track is een spoor waarmee de locatie van de data wordt vastgelegd
- Data track is het spoor waar de data is gepositioneerd
- Host protected area is een gebied waar de besturing plaatsvindt
- In alle gebieden bevindt zich de opgeslagen magnetische data

Verschillende technieken om data te verwijderen

- Er worden verschillende technieken toegepast om data te verwijderen, te overschrijven of te vernietigen
- Elke techniek heeft voor en nadelen
- In het navolgende overzicht worden de verschillende aspecten toegelicht zodat gekozen kan worden voor de juiste techniek/beveiliging



Data verwijderen van HDD’s

De 4 technieken voor data verwijdering

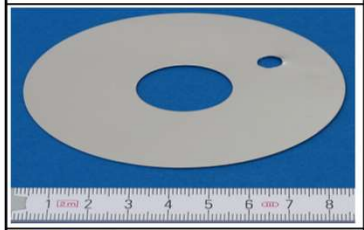
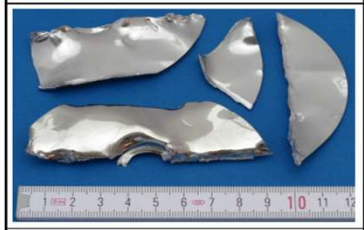
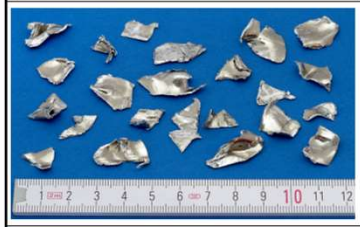
Data verwijderingsmethoden voor HDD's

Critera / Methode		Software	Verbranden	Verbuigen	Magn. Straling (Degauser)	Fysieke Vernietiging
TECHNOLOGIE	Verwijdering van data op "main track"	JA	JA	NEEN	GEDEELTELIJK	JA
	Verwijdering van data op "servo track"	NEEN	JA	NEEN	GEDEELTELIJK	JA
	Verwijderd data in "host protected area"	NEEN	JA	NEEN	GEDEELTELIJK	JA
	Ook toepasbaar voor "flash" data dragers	JA	JA	NEEN	NEEN	JA
	Proceskennis van uitvoerder	BIJZONDER LAAG	LAAG	LAAG	LAAG	LAAG
BEVEILIGING	Mate van veiligheid	BEPERKT	HOOG	ERG LANG	MATIG	HOOG
	Verschillende veiligheidsniveaus	NEEN	NEEN	NEEN	NEEN	JA, DIN 66399
	Controleerbaarheid van vernietigingsproces	NEEN	NEEN	NEEN	NEEN	JA
	Aanwezigheid van transparant controleerbare standaard	NEEN	NEEN	NEEN	NEEN	JA, DIN 66399
MILIEU	Locatie waar het proces plaatsvindt	ON-SITE / OFF-SITE	Altijd OFF-SITE	ON-SITE	ON-SITE	ON-SITE / OFF-SITE
	Materiaal recyclebaar	JA	NEEN	JA	JA	JA
	Milieuvriendelijk	JA	ERG BELASTEND	JA	JA	JA
BUDGET	Hergebruik van harde schijf	JA	NEEN	NEEN	NEEN	NEEN
	Tijdsduur	LANG	RELATIEF LANG	SNEL	SNEL	WORDT BEPAALD DOOR VEILIGHEIDSKLASSE
	Kosten	HOOG	LAAG	LAAG	LAAG	LAAG

EADMS© European Association for Data Media Security

www.EADMS.org

16-2-2011

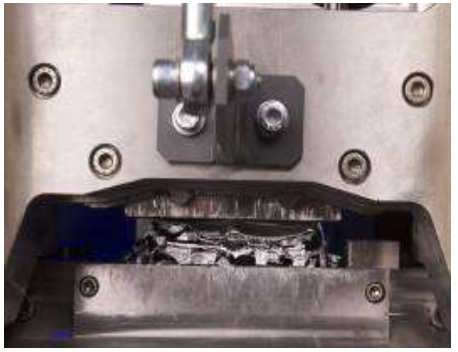
Afbeelding	Omschrijving standaard	Inspanning, kosten, tijdsduur aangaande data recovering	Toepassingsgebied	VIR-BI
	**DMS 2008 klasse A** - De harde schijf wordt door beschadiging onklaar gemaakt	- Zéér geringe inspanning - Zéér geringe kosten - Zéér gemakkelijk en snel uit te voeren	- Geschikt voor privé personen om informatie op basisniveau te beveiligen	- Niet adviseerbaar
	**DMS 2008 klasse B** - De harde schijf wordt vernietigd in stroken van 30 mm	- Geringe inspanning - Geringe kosten - Gemakkelijk en snel uit te voeren	- Geschikt voor commerciële organisaties die weinig tot geen vertrouwelijke bedrijfs-, en persoonsinformatie digitaal opslaan op harde schijf	- Dep. VERTROUWELIJK
	**DMS 2008 klasse C** - De harde schijf wordt vernietigd in deeltjes van 300 mm2	- Hoge inspanning - Hoge kosten - Hoge technische inspanning - Kost veel tijd	- Geschikt voor commerciële en overheidsorganisaties met vertrouwelijke informatie over organisatie en persoons-informatie	- Stg. CONFIDENTIEEL
	**DMS 2008 klasse D** - De harde schijf wordt vernietigd in deeltjes van 30 mm2	- Zéér hoge inspanning - Extreem hoge kosten - Uitsluitend met hoogwaardige apparatuur - Enorm tijdsintensief	- Geschikt voor overheids-organisaties met zéér vertrouwelijke nformatie	- Stg. GEHEIM
	**DMS 2008 klasse E** - De harde schijf wordt vernietigd in deeltjes van 10 mm2	- Extreem hoge inspanning - Extreem hoge kosten - Uitsluitend met technische zéér hoogwaardige apparatuur mogelijk - Extreem tijdsintensief	- Geschikt voor overheidsorganisaties met strikt vertrouwelijke informatie	- Stg. ZEER GEHEIM


DATADRAGERS
IS GEEN AFVALPROBLEEM...
HET IS EEN SECUTRITY
ONDERWERP!

Harde schijven vernietigen

- Nederlands product met internationale reputatie
- Werkt op 230V, is mobiel en kan overal zijn werk doen
- Kan in alle security veiligheidsklasse vernietigen
- Kan een foto/barcode “proof” produceren
- HDD’s – back-up tapes – mobiele telefoons – USB sticks
- Ook beschikbaar als dienstverlening op locatie

- **Referenties**
  - Justitie
  - NATO
  - Defensie
  - Inlichtingendiensten
  - Banken



maxx E-GUARD

comfort-ia

Advies op maat

- Voor advies over het beveiligen van fysieke dragers
- Privacy consultant op het gebied van meldplicht datalekken, DPIA, AVG
- Privacy QuickScan, trainingen en lezingen

Organisatie	**Comfort-Information Architekts**
Contactpersoon	Paul M.H. Korremans
Telefoon	+31 (0)182 64 06 90
Fax	+31 (0)182 64 06 95
Mail	info@comfort-ia.nl