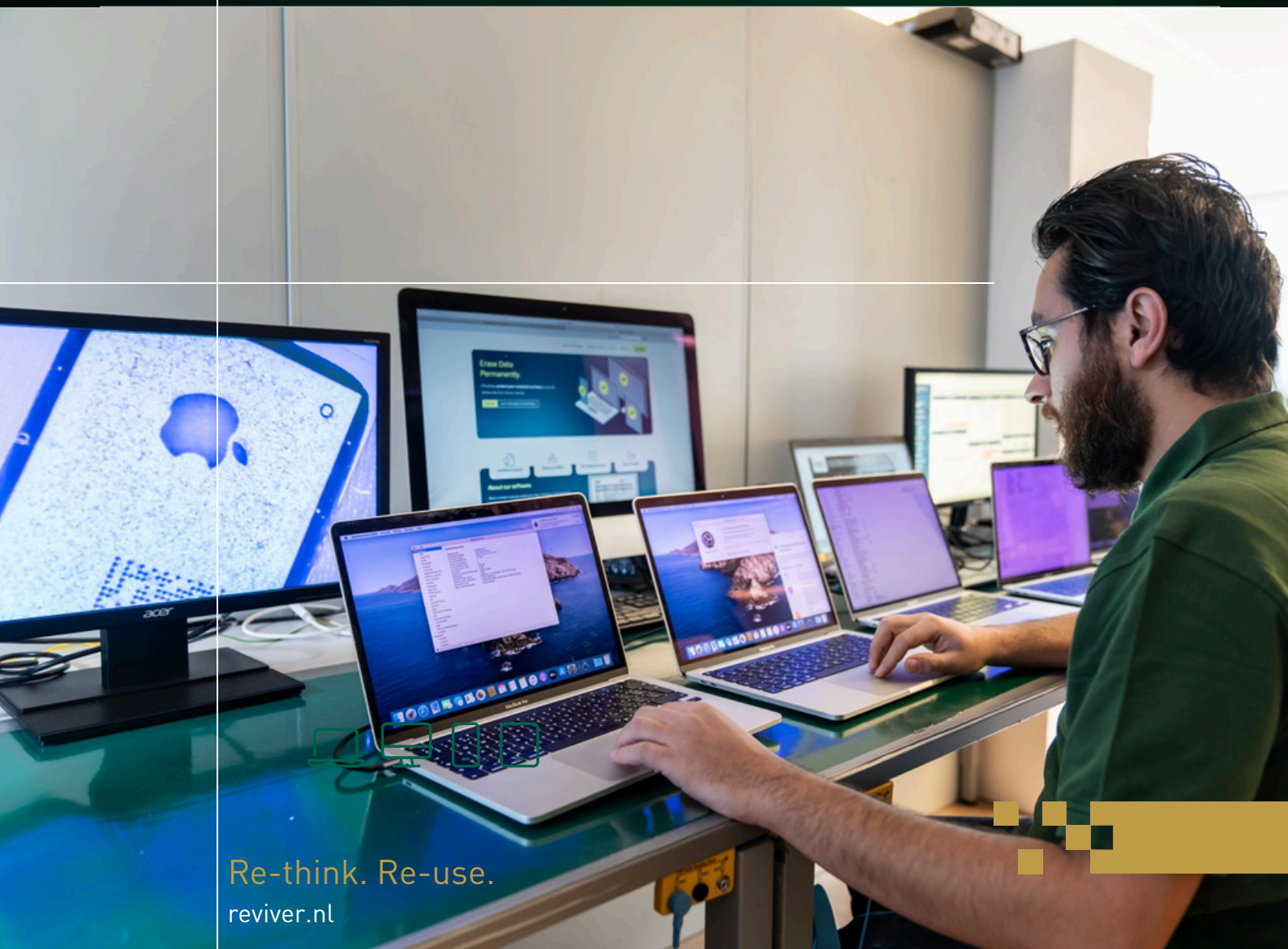
reviver
RE-THINK. RE-USE.
by SW Global

Veilige dataverwijdering van jouw ICT-hardware

Whitepaper



Re-think. Re-use.
reviver.nl

Voor wie is dit document?

Deze whitepaper is bedoeld voor organisaties en bedrijven die:

- Afgeschreven ICT-hardware verantwoord willen afvoeren
- Datalekken willen voorkomen
- Voorbereid willen zijn op audits en AVG-verplichtingen
- Zekerheid zoeken zonder onnodige complexiteit

Je data is óf weg, óf niet

Oude laptops, servers en telefoons verdwijnen dagelijks uit organisaties. Vaak met de gedachte: dit is geregeld. Maar in de praktijk blijkt dat dataverwijdering één van de meest onderschatte risico's binnen IT en facilitaire processen is.

Bestanden verwijderen of apparaten resetten voelt veilig, maar is dat technisch gezien niet. En zolang data niet aantoonbaar is verwijderd, blijft de verantwoordelijkheid bestaan. Ook onder de AVG. Ook bij afgeschreven hardware.

Deze whitepaper helpt je om grip te krijgen op dataverwijdering. Vanuit overzicht, controle en praktische stappen.

Hoofdstuk 1

Waarom afgeschreven hardware een risico blijft

Stilstand betekent geen veiligheid

Actieve systemen worden gemonitord, geüpdatet en beheerd. Afgeschreven hardware niet. Daardoor valt deze vaak buiten processen, verantwoordelijkheden en controles. Juist dat maakt stilstaande hardware risicovol.

Wat er vaak nog op oude apparaten staat

Afgeschreven apparaten bevatten vaak meer dan alleen oude bestanden:

· gebruikersaccounts
· netwerkconfiguraties
· VPN- en systeemtoegang
· lokale back-ups
· persoonsgegevens

Voor kwaadwillenden is dit waardevolle informatie.

De AVG maakt geen onderscheid

Volgens de AVG blijft een organisatie verantwoordelijk voor persoonsgegevens zolang deze niet aantoonbaar zijn verwijderd. Het maakt daarbij niet uit of het apparaat actief wordt gebruikt of al jaren in een kast ligt. Uitstel voelt onschuldig, maar is dat zelden.

Hoofdstuk 2

Veelgemaakte misverstanden over dataverwijdering

Misverstand 1: bestanden verwijderen is voldoende
Technisch onjuist. Data blijft aanwezig totdat deze actief wordt overschreven of vernietigd.

Misverstand 2: resetten van een apparaat wist alles
Een reset maakt data vaak alleen onzichtbaar, niet onherstelbaar.

Misverstand 3: een certificaat betekent automatisch zekerheid
Een certificaat zegt alleen iets als duidelijk is wat eraan voorafging.

Misverstand 4: dataverwijdering is een IT-detail
De impact raakt ook reputatie, compliance en aansprakelijkheid. Het is een organisatievraagstuk.

Hoofdstuk 3

Wat auditors écht verwachten

Audits zijn veranderd. Waar vroeger intentie voldoende was, draait het nu om aantoonbaarheid. Auditors willen inzicht in:

· welke hardware is verwerkt
· welke datadragers zijn gewist
· welke methode is toegepast
· wanneer en door wie
· hoe controle is uitgevoerd

Losse documenten of aannames zijn onvoldoende. Samenhang, herhaalbaarheid en controle zijn doorslaggevend. Wie dit vooraf goed regelt, voorkomt stress op het moment dat het erop aankomt.

Hoofdstuk 4

Certificering versus controle

Een certificaat is het eindpunt, niet het bewijs

Een certificaat heeft alleen waarde als het onderdeel is van een transparant proces. Zonder context is het vooral administratief.

Onafhankelijke toetsing vergroot vertrouwen

Interne controles zijn belangrijk, maar onafhankelijke controle maakt het verschil. Het voorkomt schijnzekerheid en versterkt vertrouwen richting auditors, klanten en toezichthouders. Daarom werkt Reviver met onafhankelijke toetsing via Certus.

Hoofdstuk 5

Zo ziet veilige dataverwijdering er in de praktijk uit

Bij Reviver bestaat dataverwijdering uit vaste, logische stappen:

1. Inventarisatie
Welke apparaten zijn er en welke datadragers bevatten ze?

2. Keuze methode
Softwarematig wissen waar mogelijk.
Fysieke vernietiging waar nodig.

3. Uitvoering
Gecertificeerde dataverwijdering volgens erkende normen.

4. Controle
Logging, verificatie en onafhankelijke toetsing.

5. Vastlegging
Wiscertificaat en rapportage per batch. Zo wordt dataverwijdering geen losse actie, maar een structureel proces.

Waarom eenvoud juist zekerheid oplevert
Complexiteit leidt vaak tot uitstel. En uitstel leidt tot risico. Door dataverwijdering eenvoudig en herhaalbaar te maken, ontstaat juist meer controle. Bijvoorbeeld door centrale inzameling via een vaste locatie of een structurele oplossing zoals een Reviverbox. Wat overzichtelijk is, wordt opgevolgd. Wat vastligt, wordt niet vergeten.

Hoofdstuk 6

Praktische checklist

Veilige dataverwijdering in 12 stappen

Gebruik deze checklist om te beoordelen of dataverwijdering binnen jouw organisatie goed is ingericht.

Inventarisatie

□ We hebben inzicht in alle afgeschreven ICT-hardware
□ We weten welke apparaten datadragers bevatten
□ Er is duidelijk eigenaarschap per hardwarestroom

Proces

□ Dataverwijdering gebeurt volgens vaste stappen
□ Er is een duidelijke keuze tussen softwarematig wissen en fysieke vernietiging
□ Dataverwijdering is geen losse actie, maar onderdeel van een proces

Uitvoering

□ Data wordt actief overschreven of fysiek vernietigd
□ Er wordt gewerkt volgens erkende normen
□ Alleen wat écht niet herbruikbaar is, wordt vernietigd

Controle en bewijs

□ Elke batch wordt gelogd
□ Er is onafhankelijke controle uitgevoerd
□ We ontvangen een wis-certificaat per batch
□ Rapportages zijn terug te vinden voor audits

Organisatie

□ IT en management zijn op één lijn
□ Dataverwijdering is belegd in beleid
□ Er is geen afhankelijkheid van individuele medewerkers

Tot slot

Zekerheid begint bij overzicht

Veilige dataverwijdering draait niet om angst, maar om controle. Wie overzicht heeft, vaste stappen hanteert en werkt met aantoonbare processen, voorkomt risico's zonder extra gedoe.

Reviver helpt organisaties om dataverwijdering structureel en transparant te regelen. Veilig voor data. Slim voor hergebruik. Rustgevend voor audits.

Je data is óf weg, óf niet. En dat verschil wil je zeker weten.

Think twice, it's no waste.
www.reviver.nl