Lopen bedrijven door

HET NIEUWE WERKEN meer

risico op inbreuk op gegevens?

Fellowes **'Houd het vertrouwelijk'-enquête 2022**. Een rapport over **papiervernietiging** in een hybride werkwereld

Voorwoord

> “Veel organisaties die begin 2020 op een model voor werken op afstand overschakelden, merkten dat er niet genoeg tijd was om geschikte risico-evaluaties uit te voeren voordat ze dergelijke drastische veranderingen in hun werkwijzen aanbrachten.”

“Iedereen was er vooral op gericht zijn diensten doorgang te kunnen laten vinden in plaats van eerst stil te staan bij de risico’s van de veranderingen die nodig waren. Medewerkers hadden ook geen tijd om zich aan de nieuwe manier van werken aan te passen en uit verschillende onderzoeken blijkt dat er slechte gewoonten rond gegevensbeveiliging zijn ontstaan bij het thuiswerken tijdens de pandemie.

Als we nu in 2022 terugkijken, is de manier waarop we werken snel geëvolueerd, en is hybride werken enorm populair geworden als onderdeel van de terugkeer naar kantoor na de pandemie. Maar hebben bedrijven actie ondernomen en hun processen aangepast, of lopen bedrijven door de nieuwe manier van werken meer risico op inbreuk op gegevens?

Het antwoord op die vraag is: ja. De helft van onze deelnemers aan het onderzoek denkt dat hybride werken de hoeveelheid gevoelige informatie die verloren gaat of in strijd is met de regels onder de AVG, kan hebben vergroot. Papieren documenten waren niet per se het eerste waar bedrijven zich zorgen over zouden maken als ze aan hun beveiligingsbeleid dachten. Door de snelle overgang naar hybride werken nemen we elke week echter wel duizenden documenten mee op reis tussen thuis en werk. Dit roept belangrijke vragen op over vertrouwelijke papieren en hoe we die kunnen beschermen, in een wereld waarin veel medewerkers niet meer alleen op een kantoorlocatie werken.

Om voort te bouwen op de 40 jaar ervaring met papierversnipperaars van Fellowes, wilden we erachter komen hoe mensen documenten beveiligen en versnipperen in deze uitgebreide hybride werkwereld, en ook op welke manier organisaties, 4 jaar na de invoering van de AVG (Algemene Verordening Gegevensbescherming), de regels onder deze verordening naleven. Onze papierversnipperaars hebben we altijd ontwikkeld zodat ze aan elke werkplekbehoefte kunnen voldoen. We zetten ons in voor de bescherming van bedrijven en personen in elke werkruimte, door te helpen voorkomen dat papieren documenten in verkeerde handen vallen.

Ons onderzoek werd in samenwerking met B2B International gehouden onder 605 gebruikers van papierversnipperaars in Frankrijk, Duitsland en het VK, werkzaam in de financiële dienstverlening, de openbare sector en de gezondheidszorg.

In dit rapport nemen we een diepe duik in trends en gedragingen rond gegevensbeveiliging in deze steeds veranderende werkomgeving. We hopen dat we bedrijven door deze fase van verandering heen kunnen loodsen. Want het veilig vernietigen van gevoelige papieren, waar je ook werkt, is van vitaal belang om de veiligheidsrisico’s in te dammen waarmee elke organisatie te maken krijgt.”

Steven Hickey

Ontwikkelingstijdlijn van de papiervernietiger

1982
Commerciële papiervernietigers

Fellowes sluit een licentieovereenkomst met een Duitse firma voor de fabricage van commerciële papiervernietigers.

1990
De eerste persoonlijke

De nieuwste uitvinding, de persoonlijke papier-vernietiger, wordt gepresenteerd

2005
SafeSense™

Introductie van Fellowes SafeSense™-shreddertechnologie maakt papiervernietigers veiliger voor in huis

2008
100% Jam Proof papiervernietigers

Introductie van een serie 100 procent ‘jam proof’ papiervernietigers van Fellowes om het vastlopen van papiervernietigers te elimineren

2014
Automax™ Autofeed papiervernietigers

Fellowes introduceert AutoMax™ autofeed papiervernietigers om de productiviteit van de papiervernietiger op kantoor te verbeteren

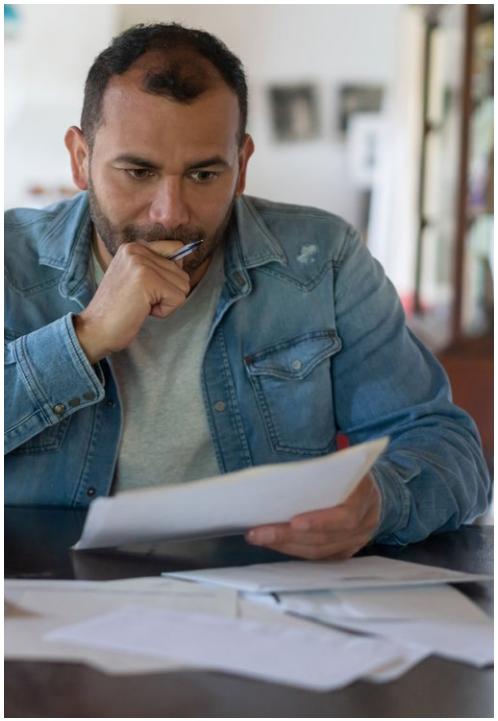
2020
LX -Serie

Introductie van de meest geavanceerde micro-cut papiervernietigers van Fellowes, die in elke werkruimte kunnen worden geïntegreerd

AVG en gegevensbescherming in het hybride werken

Uit ons onderzoek blijkt dat **8 van de 10** respondenten geheel of gedeeltelijk op afstand werken. Hybride werken – een combinatie van werken op locatie en werken op afstand – heeft misschien meer flexibiliteit en variatie in de keuze van werkplek gebracht, maar het vormt ook de voortdurende uitdaging om ervoor te zorgen dat mensen weten hoe ze vertrouwelijk moeten werken en goede gegevensbeschermingsbeginselen toepassen, op alle locaties.

Of je personeel nu op kantoor, thuis, in gedeelde werkruimten of ergens anders werkt, je moet rekening houden met hun veiligheidsrisico's. Dit begint met ervoor te zorgen dat je kijkt naar enkele van de gebieden die nieuwe risico's voor je organisatie kunnen veroorzaken. Je moet bijvoorbeeld een strikt beleid voeren rond het gebruik door medewerkers van hun eigen computers, tablets en smartphones voor werkdoeleinden, omdat je als bedrijf minder controle hebt over hoe die apparaten geconfigureerd en gebruikt worden. Een ander punt van zorg is het gebruik van openbare en thuis-wifi, en zwakke en herhaaldelijk gebruikte wachtwoorden. Beide gebieden zijn een veel voorkomend zwak punt voor cyberaanvallen en er moeten duidelijke instructies met de medewerkers gedeeld worden om ervoor te zorgen dat zij en het bedrijf beschermd zijn.



Het verbaast ons niet dat papieren documenten één van de meest onderschatte risico's voor bedrijven vormen. Nu alles tegenwoordig digitaal is, vergeet men vaak het element van papieren gegevens in het beveiligingsbeleid op te nemen. Het is echter belangrijk te benadrukken dat de meerderheid van de bedrijven (68%) die aan ons onderzoek hebben meegedaan, heeft aangegeven dat ze dagelijks omgaan met een grote hoeveelheid gevoelige gedrukte informatie. **70%** van alle respondenten heeft ofwel gedrukte werkdocumenten mee naar huis genomen,

Weet je nog niet alles van de AVG? Wij helpen je...

De Algemene Verordening Gegevensbescherming is in mei 2018 ingevoerd en is een uitgebreide reeks gegevensbeschermingsvoorschriften voor de omgang met persoonsgegevens van Europese burgers. Elke organisatie die met deze persoonsgegevens omgaat mag ze alleen verzamelen onder strikte voorwaarden, voor legitieme doeleinden en moet ze beschermen tegen misbruik.

Persoonsgegevens moeten worden verwerkt op een manier die een passende beveiliging van de gegevens garandeert, en moeten worden beschermd tegen ongeautoriseerde of onwettige verwerking en onopzettelijk verlies, vernietiging of schade, met behulp van passende technische en organisatorische maatregelen.

Wat zijn persoonsgegevens?

Persoonsgegevens zijn gegevens die betrekking hebben op een levende persoon die aan de hand van die gegevens geïdentificeerd kan worden. Het kan gaan om namen, adressen, BSN-nummers, gegevens van sociale media, bewakingscamerabeelden of foto's. Persoonsgegevens kunnen in digitale of papieren vorm voorkomen.

Wat zijn de gevolgen van het niet naleven van de AVG?

Een inbreuk in verband met persoonsgegevens kan boetes opleveren van **4% van de wereldwijde omzet of € 20 miljoen**, maar kan ook schade toebrengen aan de reputatie van het bedrijf.

Zes beginselen van gegevensbescherming

In elke strategie voor gegevensbescherming moeten de volgende beginselen terugkomen:

- **Persoonsgegevens moeten wettig, eerlijk en op een transparante manier verwerkt worden;**
- **Persoonsgegevens moeten verzameld worden voor specifieke, expliciete en legitieme doeleinden, en mogen dientengevolge niet verwerkt worden op een manier die tegen die doeleinden ingaat;**
- **Persoonsgegevens moeten adequaat en ter zake dienend zijn, en beperkt blijven tot wat nodig is;**
- **Persoonsgegevens moeten nauwkeurig en actueel zijn; onjuistheden in de persoonsgegevens moeten worden verwerkt, gewist en gecorrigeerd;**
- **Persoonsgegevens mogen niet langer bewaard worden dan nodig is;**
- **Persoonsgegevens moeten veilig worden verwerkt**

Meer informatie vind je op General Data Protection Regulation - Fellowes®

werkdocumenten thuis afgedrukt of beide, en iets minder dan de helft van deze groep heeft deze documenten vervolgens in een prullenbak of recyclebak gedaan zonder ze te versnipperen. Verder heeft **46%** van alle respondenten wel eens gezien dat mensen vertrouwelijke werkdocumenten onbeheerd achterlieten. Hierover moeten bedrijven zich grote zorgen maken. Ook al lijkt er in Europese bedrijven een strikt beleid te bestaan voor het versnipperen van gevoelige informatie, toch worden die richtlijnen buiten het kantoor vaak niet gevolgd. Of het nu in een bedrijfskantoor is of op een thuiswerkplek, gevoelige papieren gegevens moeten worden opgeborgen als ze niet worden gebruikt en veilig versnipperd als ze niet meer nodig zijn voor het doel waarvoor ze werden verkregen.

Uit ons onderzoek blijkt ook dat zelfs na 4 jaar, slechts **60%** over het algemeen met de AVG vertrouwd is en slechts **1 op de 4** bedrijven thuiswerken of telewerken in het algemeen in het beleid heeft opgenomen. Regelgevers zoals het Information Commissioner's Office (ICO) maakten een uitzondering voor de druk die de pandemie op bedrijven legde. Maar nu de meeste beperkingen in heel Europa opgeheven zijn, zal de ICO minder mild zijn. Het is daarom van essentieel belang om nu te handelen als je met je bedrijf hybride wilt blijven werken. Je moet ervoor zorgen dat de beleidsregels worden herzien en bijgewerkt, zodat de nieuwe manier van werken erin terugkomt en mogelijke risico's op inbreuk op gegevens erin zijn opgenomen.

Als die beleidslijnen eenmaal zijn bijgewerkt, is het belangrijk dat er een sterk uitvoerings- en communicatieplan ligt. Het onderzoek wees op een duidelijke kloof binnen organisaties. Terwijl de meerderheid (83%) van de respondenten in de wat hogere functies op de hoogte leek van de AVG en zich actief aan de gegevensbeschermingsregels en voorschriften van de bedrijven zou houden, was slechts **57%** van de respondenten in de wat lagere functies bekend met de AVG en zou zich dus niet aan de richtlijnen houden, ongeacht de werkplek.

Communicatie en controle over wat er met gevoelige documenten en gegevens gebeurt, lijkt vaak gemakkelijker als je met het hele team op kantoor samenwerkt. Maar een feit is dat hybride werken een trend is die blijft en waar bedrijven ter ondersteuning van hun personeel niet meer omheen kunnen. Tegelijk is het absoluut noodzakelijk dat processen en voorschriften aan deze veranderingen worden aangepast. De gevolgen van het zoekraken van gevoelig papierwerk zijn verstrekkend. Daarom is het van vitaal belang dat alle collega's, op elk niveau, over deze regelgeving worden voorgelicht. Er hoeft namelijk maar één keer een situatie te zijn waarin gegevens verkeerd terechtkomen om een inbreuk te veroorzaken. In het volgende gedeelte geven we suggesties over hoe die veranderingen in het hele bedrijf kunnen worden doorgevoerd.

BLIJF AVG PROOF

Wat kunnen bedrijven doen om hun personeel te helpen aan het privacy- en gegevensbeleid te voldoen?

Bijwerken van het beleid

Denk goed na over je Bring Your Own Device (BYOD)-beleid (beleid bij gebruik van eigen apparatuur), als medewerkers hun eigen apparaten gebruiken bij het thuiswerken.

Benadruk dat openbare en thuis wifinetwerken een bedreiging kunnen vormen en instrueer medewerkers wat ze moeten doen om ze veilig te gebruiken.

Herzie je beleid rond het afdrukken, bewaren en weggooien van papieren documenten en pas het aan. Voeg tevens een rubriek toe rond het bewaren en weggooien van documenten in het thuiskantoor.

Herzie je beleid voor wachtwoordbeveiliging. Het National Cyber Security Centre (NCSC) adviseert momenteel het gebruik van wachtwoordzinnen van drie woorden in plaats van wachtwoorden. Bovendien zou je kunnen overwegen multifactor authenticatie te gaan gebruiken.

In je beleid moet staan dat voordat je een oude computer of harde schijf weggooit, verkoopt of weggeeft, alle gegevens volledig van de harde schijf gewist moeten worden.

Training

Ga er niet van uit dat iedereen de AVG kent en begrijpt. Licht alle medewerkers voor over de vereisten onder de AVG, het omgaan met persoonsgegevens en de zes beginselen van gegevensbescherming. Er moet training gegeven worden aan alle nieuwe medewerkers en als onderdeel van regelmatige opfrissessies over gegevensbeveiliging.

Geef je medewerkers een checklist van gebieden die een risico kunnen vormen voor een inbreuk op gegevens; je kunt ze ook een Data Security Health check(gezondheidscheck voor gegevensbeveiliging) laten doen.

Zorg ervoor dat in de training wordt ingegaan op gevoelige papieren documenten en hoe daarmee om te gaan. Welke documenten en dossiers moeten voor bepaalde tijd bewaard worden en welke moeten meteen vernietigd worden als ze niet meer nodig zijn.

Werk met een trainingsmodule rond gegevensbeveiliging in het thuiskantoor waarin de nieuwe toevoegingen aan je beleid naar voren komen.

Overweeg te gaan werken met een online trainingsportaal, zodat je de status van ieders training kunt bijhouden en een vaste deadline kunt stellen.

Apparatuur

Om problemen met BYOD te vermijden, adviseren we het bedrijf te investeren in laptops in plaats van desktops: zo kan de apparatuur gemakkelijk meegenomen worden tussen thuis en het bedrijfskantoor.

Investeer in superieure anti-virusprogramma's en firewallsystemen.

Zorg ervoor dat je personeel toegang heeft tot een papiervernietiger in het hoofdkantoor. Bovendien moeten thuiswerkende medewerkers voorzien zijn van een kleine papiervernietiger of een papierversnipperaar voor thuisgebruik.

Kies voor zeer vertrouwelijke of persoonlijke gegevens zoals adressen, facturen en balansen voor een micro-cut vernietiger (P-5). De kleinere deeltjesgrootte ervan levert je een superieure beveiliging op, waardoor gegevens onmogelijk te lezen of te herstellen zijn.

Zorg voor een productieve en veilige werkplek voor je medewerkers door bij het zoeken naar een papiervernietiger rekening te houden met vastloopreventie en veiligheidsvoorzieningen.

Communicatie

Communicatie is heel belangrijk op alle niveaus van het bedrijf. Voorkom hiaten in de kennis op de wat lagere functieniveaus.

Gegevensbeveiliging moet aan de orde komen op de eerstvolgende vergadering van de vestiging en ook in kleinere groepen tijdens de maandelijkse teamvergaderingen en in één-op-één momenten.

Hang overal in het bedrijf posters op ter herinnering, maar vermeld de bijwerking van het beleid ook in je nieuwsbrief en zet het op je intranet.

Deel beste werkwijzen en eventuele dreigingen van phishing of cyberaanvallen binnen het bedrijf, zodat iedereen erop kan letten.

Maak gegevensbeveiliging onderdeel van driemaandelijkse bedrijfsbeoordelingen.

Wat kun je als medewerker doen om inbreuk op gegevens te voorkomen?

Zorg dat je inzicht hebt in welke gegevens gevoelig zijn en beschermd moeten worden

Documenten die persoonlijke gegevens bevatten en bedrijfsgegevens moeten veilig vernietigd worden volgens de wettelijke voorschriften inzake het bewaren van gegevens.

Zorg dat je je ervan bewust bent dat elk land een eigen vastgestelde periode heeft waarbinnen contracten, zakelijke overeenkomsten en soortgelijke documenten bewaard moeten worden. Als aan deze bewaarvoorschriften voldaan is, is vernietiging van documenten de beste manier om opslagruimte vrij te maken en vertrouwelijkheid te beschermen.

Ontvangstbewijzen, stortingsstrookjes en bankafschriften kunnen meestal vernietigd worden als ze met de rekeningen verwerkt zijn.

Personeelsdossiers moeten regelmatig gecontroleerd worden, en als ze hun wettelijke vervaldatum bereikt hebben, worden vernietigd. De AVG schrijft voor dat HR-afdelingen moeten aantonen waarom ze gegevens over voormalige en huidige medewerkers bewaren, en moeten verantwoorden waarom ze gegevens langer bewaren dan de vereiste bewaartermijn.

Sla papieren gegevens veilig op of gooi ze veilig weg

Denk goed na voor je iets afdrukt. Vraag jezelf af: Heb ik hier echt een papieren exemplaar van nodig? Wie zou dat document per ongeluk in handen kunnen krijgen?

Vernietig documenten gaandeweg tijdens je werk. Als dat niet mogelijk is, versnipper dan al het gevoelige papierwerk voordat je het recycleert of weggooit, liefst zonder het risico te hoeven nemen het van huis naar kantoor te vervoeren, of vice versa.

Laat thuis of op kantoor nooit gevoelige papieren gegevens onbeheerd rondslingeren. Ruim je bureau 's avonds altijd op en berg als beschermd gemarkeerde papieren en alle verwijderbare computermedia op voor je je werkplek verlaat.

Bekijk regelmatig de gegevens die je bewaart en anonimiseer waar mogelijk persoonsgegevens zodra ze niet meer nodig zijn.

Blijf op de hoogte van training en beleid

Zorg dat je op de hoogte bent van de beschikbare trainingsmodules en dat je die kunt volgen. Overweeg ook om elk kwartaal een herinnering in je agenda te zetten om opfrissessies bij te wonen.

Spoor collega's en teamleden aan om training te volgen, en herinner elkaar aan de regels en richtlijnen als je merkt dat iemand niet volgens het beleid handelt (bv. gevoelige documenten laat rondslingeren, persoonlijke apparaten gebruikt enz.).

Verdiep je in de zes beginselen van gegevensbescherming.

Bespreek eventuele vragen die je hebt met je manager of functionaris voor gegevensbescherming.

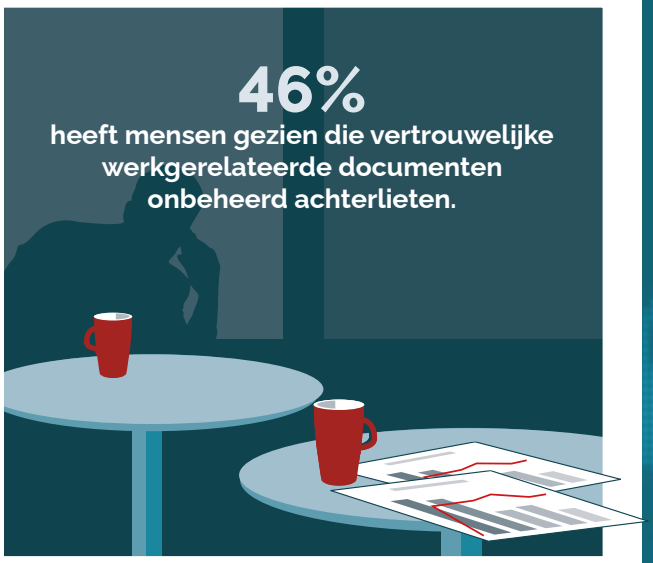
Belangrijkste bevindingen van ons onderzoek

8 van de 10
respondenten zijn overgegaan tot thuiswerken.

70% van alle respondenten
heeft ofwel gedrukte werkdocumenten mee naar huis genomen, documenten thuis afgedrukt, of beide.

47%
van hen versnippert geen werkdocumenten na ze gebruikt te hebben >>> Leidt tot veiligheidsrisico's tijdens het transport!

46%
heeft mensen gezien die vertrouwelijke werkgerelateerde documenten onbeheerd achterlieten.



Er is een groot gebrek aan bewustzijn over de AVG in junior of niet-leidinggevende functies

Maar 57%
zegt bekend te zijn met de AVG

Na 4 jaar

Slechts 60%
van alle respondenten zegt op de hoogte te zijn van de AVG

Vier van de tien (41%)
zeggen nog steeds geen formele update van het gegevensbeveiligingsbeleid voor thuiswerken te hebben vernomen.

Richtlijnen voor betere papiervernietiging:

Veilig versnipperen is essentieel om vertrouwelijk papierwerk uit de verkeerde handen te houden en de blootstelling van de organisatie aan gegevensinbreuken te verminderen. In een tijdperk waarin meer mensen dan ooit hybride werken, pendelend tussen thuis en kantoor, zijn het naleven van het AVG-beleid en de risico's die dit met zich meebrengt voor de gegevensbeveiliging meer dan duidelijk.

Het vernietigen van vertrouwelijk papierwerk met een papiervernietiger zou deel moeten uitmaken van onze dagelijkse routine, waar we ook werken.

- Ga er niet van uit dat iedereen het AVG-beleid begrijpt. Geef voorlichting aan alle werknemers over de vereisten van de AVG-wetgeving, de behandeling van persoonlijke gegevens en de zes principes van gegevensbescherming. Deze training moet worden gegeven aan alle nieuwe medewerkers, telkens wanneer de wetgeving wordt bijgewerkt, en als onderdeel van regelmatige opfrissessies over gegevensbeveiliging.
- Berg vertrouwelijke documenten op als ze niet gebruikt worden, en laat ze nooit onbeheerd rondslingeren op je thuiswerkplek of kantoor.
- Versnipper al het gevoelige papierwerk voordat u het recyclet of weggooit, bij voorkeur zonder het risico te hoeven nemen om het te vervoeren van huis naar kantoor, of omgekeerd.
- Geef alle medewerkers op kantoor en thuis gemakkelijk toegang tot een veilige papiervernietiger.

Vind de juiste papiervernietiger voor uw werkomgeving.
Kijk op www.Fellowes.com of klik hier

‘Houd het vertrouwelijk’-enquête 2022
Methodologie

Het onderzoek is in april 2022 uitgevoerd door B2B International. Er zijn 605 gebruikers van papiervernietigers geënquêteerd, met een gelijke verdeling over het VK, Frankrijk en Duitsland. De aandacht ging vooral uit naar gebruikers van papiervernietigers op verschillende hoge managementniveaus van kleine tot middelgrote bedrijven uit de volgende sectoren – financiële dienstverlening (206) , de publieke sector (206) en de gezondheidszorg (193).
Voor het vergelijken van werkgewoonten rond gegevensbeveiliging in een hybride werkwereld, was het belangrijk een gelijke verdeling te hebben over mensen die afwisselend thuis en op kantoor werken, meestal op een bedrijfskantoor werken, alleen op een bedrijfskantoor werken, meestal thuis werken of alleen thuis werken.

Voor meer informatie over de methodologieverdeling kun je contact opnemen met jdettler-bates@fellowes.com.

Fellowes

www.fellowes.com