



Rexel

papiervernietiging

Waarom een veiligheidsbeleid voor papier belangrijk is voor naleving van de AVG.

Disclaimer

Niets in deze uitgave mag worden beschouwd als juridisch advies.

Organisaties dienen een raadsman te raadplegen met betrekking tot naleving van de algemene verordening gegevensbescherming of enige andere toepasselijke wetten of voorschriften.

Over dit document

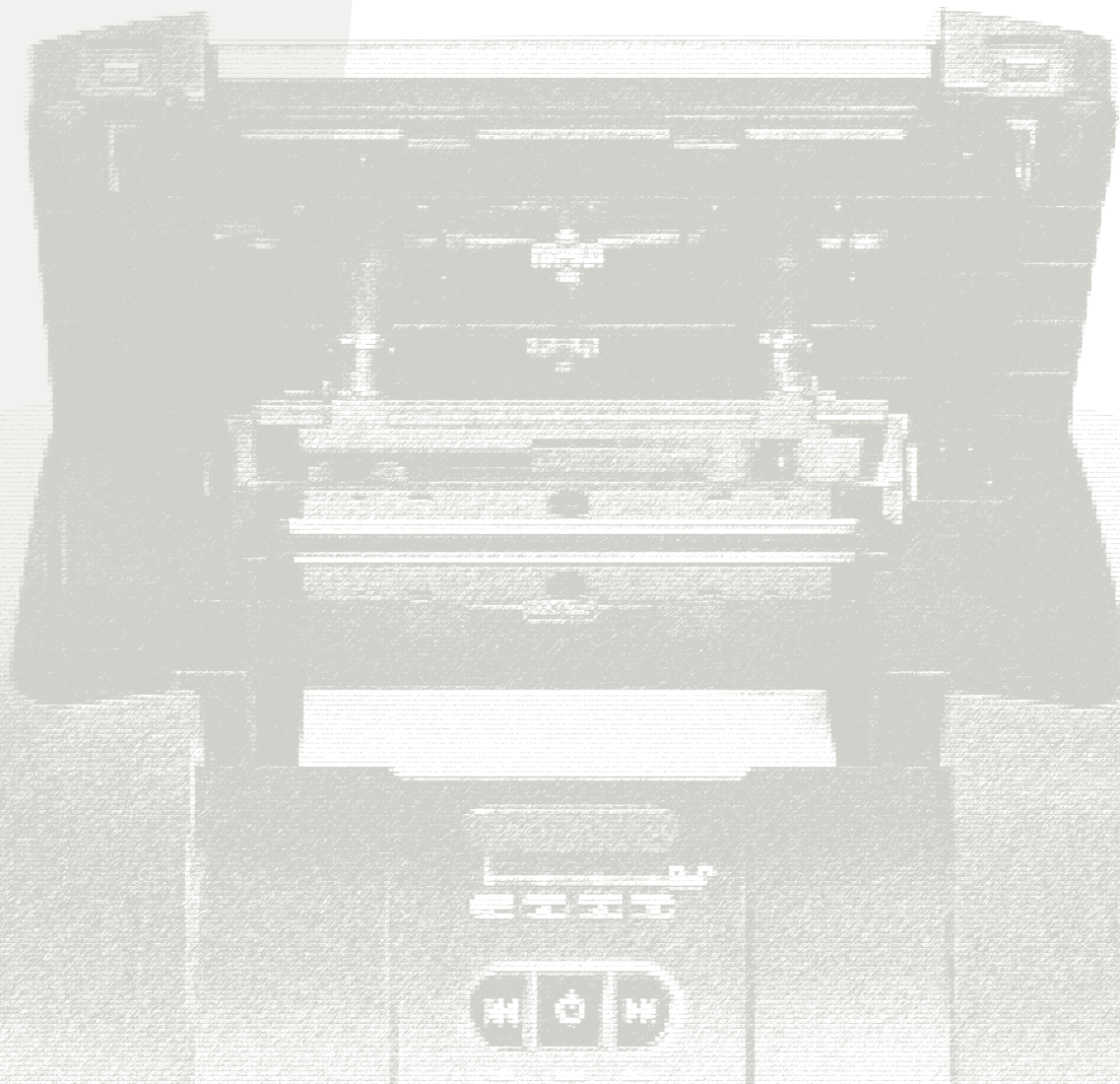
Dit whitepaper geeft u
**een overzicht van de doelstellingen
van de AVG** en de problemen die dit
kan opleveren voor organisaties.

Het doel van dit whitepaper is u een inleiding te geven over de algemene verordening gegevensbescherming (AVG) van de EU en over de manier waarop deze van invloed is op verschillende bedrijfsactiviteiten, zodat u een kader kunt scheppen voor een veiligheidsbeleid voor papier voor uw eigen bedrijf, voordat de verordening in werking treedt in mei 2018.

Waar gaat de AVG eigenlijk over? Deze verordening verplicht organisaties om goede veiligheidspraktijken toe te passen op zowel elektronische gegevens als gegevens op papier en om, in geval van een gegevenslek, de (mogelijk) betrokken personen hiervan op de hoogte te stellen.

De AVG is wereldwijd van toepassing op alle organisaties die persoonlijk identificeerbare gegevens over mensen in de EU beheren of verwerken, ongeacht de geografische voetafdruk van deze organisaties. De voorschriften van de AVG gelden zowel voor persoonsgegevens in elektronische vorm als op papier en dit betekent dat alle organisaties zich moeten houden aan de AVG-voorschriften als ze persoonlijk identificeerbare gegevens verwerken die afkomstig zijn uit de EU.

Hoewel veel organisaties prioriteit geven aan de beveiliging van elektronische gegevens, blijft de beveiliging van gegevens op papier vaak achter. Zo geeft bijna twee derde van de kantoren toe vertrouwelijke informatie niet te vernietigen¹. Hierdoor lopen organisaties het risico niet te voldoen aan de AVG en de betreffende personen lopen het risico van fraude en identiteitsdiefstal. Met dit in het achterhoofd stimuleert Rexel - een toonaangevend merk op het gebied van papierversnieters - organisaties om hun beveiligingsbeleid en -praktijken voor zowel gegevens op papier als elektronische gegevens onder de loep te nemen.



Een overzicht

De AVG wil het privacyrecht van individuele personen in Europa beschermen, ongeacht het feit of ze EU-burgers zijn of niet. Dit privacyrecht omvat, maar is niet beperkt tot:

Transparantie

Het recht om duidelijke informatie te krijgen over hoe organisaties persoonsgegevens verwerken.

Toestemming

Het recht om te controleren hoe organisaties persoonsgegevens gebruiken.

Veiligheid

Het recht op informatie over de manier waarop organisaties persoonsgegevens adequaat beveiligen.

Verzamelen en beperking van de doeleinden

Het recht om te verwachten dat organisaties het verzamelen en gebruiken van informatie tot een minimum beperken.

Kennisgeving van gegevenslekken

Het recht om te worden geïnformeerd in geval van een gegevenslek.

De AVG maakt deel uit van het plan van de Europese Commissie om de regels voor gegevensbescherming te moderniseren en harmoniseren.

Hoewel het hoofddoel van de AVG bestaat uit het vergroten van het privacyrecht voor elektronische gegevens, wordt niet voorbij gegaan aan het privacyrecht voor gegevens op papier.

De nadruk ligt op het aanpakken van de steeds grotere uitdagingen op het gebied van gegevensbescherming en privacy, blootstelling aan veiligheidslekken, hacken en andere onwettelijke manieren van informatieverwerking.



Wat is er veranderd?

De volgende punten **verwijzen naar de specifieke gebieden binnen de AVG die nieuw zijn** voor individuele personen of die een uitbreiding zijn van bestaande rechten volgens de Wet bescherming persoonsgegevens:

Overdraagbaarheid van gegevens en het recht om te worden vergeten

- Individuele personen hebben nu het recht om hun persoonsgegevens van de ene naar de andere organisatie over te dragen.
- Persoonsgegevens moeten in een gestructureerd, door machines leesbaar formaat worden verstrekt.
- Een persoon kan een verzoek indienen voor het vernietigen of verwijderen van persoonsgegevens.

Kennisgeving van gegevenslekken

- Elk gegevenslek moet worden gemeld aan de toezichthoudende autoriteit.
- Ook personen die betrokken zijn bij het gegevenslek moeten hierover worden geïnformeerd.

Niet-naleving van de AVG kan resulteren in **boetes tot 20 miljoen euro of 4% van de wereldwijde inkomsten van het bedrijf**, afhankelijk van wat het hoogste bedrag is. Verder heeft een persoon op wie de gegevens betrekking hebben, het recht om een organisatie voor het gerecht te dagen.

Registratie

- Lokale overheden hoeven niet meer te worden geïnformeerd over het feit dat er persoonsgegevens worden verwerkt.
- Organisaties zijn zelf verantwoordelijk voor het bijhouden van een dossier over hun verwerkingsactiviteiten.

Gegevensbeschermingseffectbeoordelingen en veiligheid

- GBEB's zijn een middel om hoge risico's voor het recht op privacy van individuele personen te herkennen.
- Veiligheidseisen en -aanbevelingen moeten gebaseerd zijn op een risicobeoordeling.

Gegevensbeheer en verantwoordingsplicht

- Organisaties moeten ook kunnen aantonen dat ze voldoen aan de AVG.

DE ALGEMENE VERORDENING GEGEVENSBESCHERMING

Op wie is het van toepassing?

De invoering van de AVG in mei 2018
heeft invloed op de volgende functies:

Gegevensbeheerders – zij beslissen hoe en waarom persoonsgegevens
worden verwerkt

Gegevensverwerkers – mensen die handelen namens de beheerder

Deze twee personen zijn er verantwoordelijk voor dat hun klanten volledig
voldoen aan alle aspecten van de AVG om te voorkomen dat ze boetes
krijgen.

Een gegevensverwerker of gegevensbeheerder **moet wellicht een
toezichthouder voor gegevensbescherming benoemen** en een dossier
bijhouden van alle verwerkingsactiviteiten die ze uitvoeren namens hun
klanten.



AVG heeft betrekking op persoonsgegevens en gevoelige persoonsgegevens in elektronische en fysieke vorm

Het is belangrijk te overwegen op welk soort gegevens de AVG van toepassing is, alvorens een beleid voor uw organisatie op te stellen.

Gegevens die binnen het toepassingsgebied van de AVG behoren, bestaan onder meer uit informatie over een te identificeren persoon. Enkele voorbeelden van persoonsgegevens die onder de AVG vallen zijn de volledige naam, het e-mailadres en het telefoonnummer.

De AVG legt ook aanvullende bescherming op voor een **subcategorie persoonsgegevens, de zogenaamde gevoelige persoonsgegevens**.

De AVG heeft betrekking op persoonsgegevens die door organisaties worden behandeld in zowel **elektronische als fysieke vorm**, zoals papieren documenten.

Een bedrijfskader voor naleving van de AVG

Organisaties hebben drie hoofdgebieden die moeten worden beoordeeld om te voldoen aan de AVG. Door zich te richten op deze drie gebieden, kunnen bedrijven duidelijke kaders scheppen voor hun veiligheidsbeleid op elk gebied, om naleving aan alle aspecten van de AVG te ondersteunen.

Deze gebieden zijn:

Mensen

Het is van kritiek belang dat het personeel dat binnen een organisatie gegevens verwerkt hiervoor zelf verantwoordelijkheid neemt. Een organisatie moet voor elke afzonderlijke werknemer duidelijke regels opstellen over een correct beheer van alle gegevens die het bedrijf bezit, zowel elektronisch als op papier. Deze regels vloeien voort uit de eisen van de AVG met betrekking tot de omgang met alle gegevens. Zo is het mogelijk dat u duidelijke regels wilt introduceren over het gebruik van papieren documenten met gevoelige informatie en over het correct vernietigen van gebruikte documenten op basis van het gevoeligheidsniveau van de gegevens die erin staan.

Processen

Dit heeft betrekking op de processen binnen de organisatie. Een voorbeeld is het beheren van de manier waarop gegevens over klanten worden gebruikt, zoals verwerking of archivering. Het is van cruciaal belang dat bedrijven al hun huidige processen met betrekking tot gegevens opnieuw beoordelen. Als er binnen de bestaande procedures hiaten of zwakke punten bestaan, dan moet het bedrijf een kaderplan ontwikkelen om dergelijke problemen op te lossen, zodat de AVG wordt nageleefd.

Technologie

Ook moeten de huidige capaciteiten en benodigdheden op IT-gebied worden beoordeeld en indien nodig worden bijgesteld voor mei 2018. Elk afzonderlijk bedrijf moet garanderen dat bestaande systemen die niet geheel voldoen aan de voorschriften, worden verbeterd of vervangen om te voorkomen dat er boetes worden opgelegd nadat de AVG in werking is getreden.

Waarom is veiligheid van papier van belang?

Nu we hebben besproken wat bedrijven volgens de AVG moeten doen, willen we benadrukken dat het belangrijk is dat organisaties voldoen aan de veiligheid van informatie op papier. Ook bespreken we waarom dit een belangrijk aandachtspunt is voor bedrijven bij hun voorbereidingen voor de AVG.

Uit een onderzoek in 2014 van PwC en Iron Mountain² - een bedrijf dat dossiers beheert - onder middelgrote Europese bedrijven naar de manier waarop informatierisico's worden gezien en beheerd, blijkt dat twee derde van de respondenten beheersing van de risico's die samenhangen met papieren dossiers van het grootste belang acht.



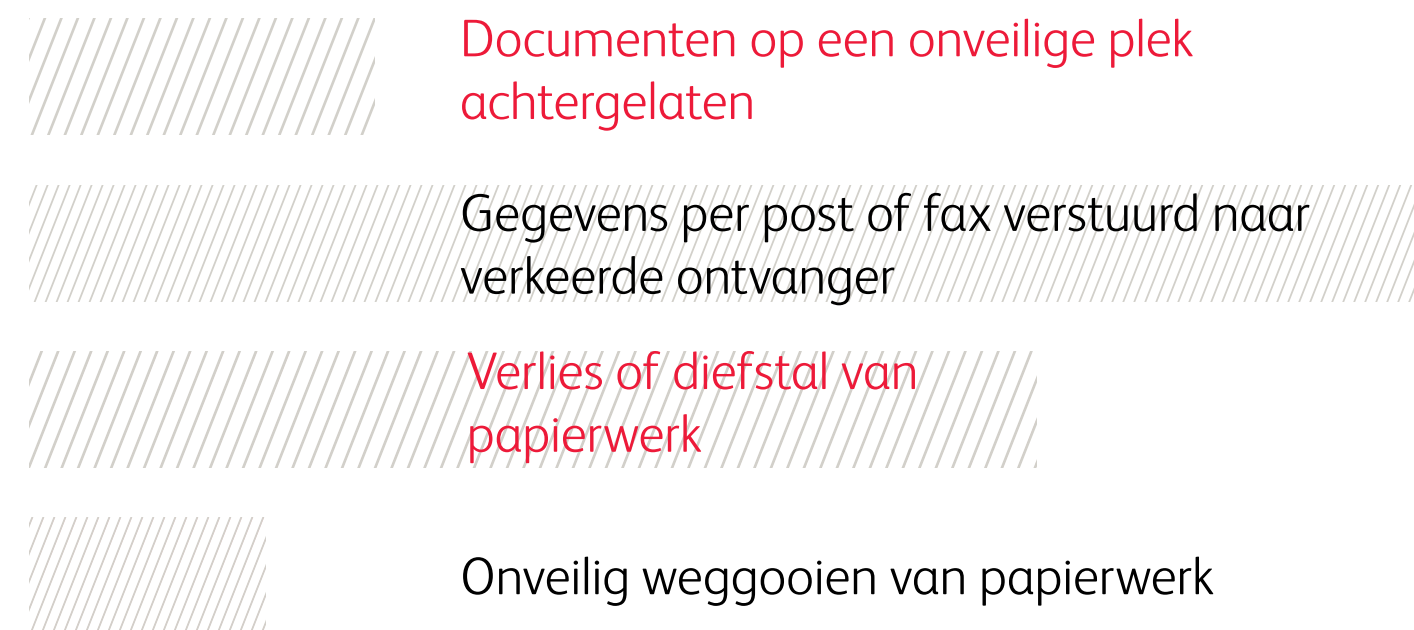
Hoewel digitale bedreigingen bij organisaties hoog op de agenda staat, zou het een vergissing zijn om te denken dat er geen veiligheidsrisico's meer bestaan voor papieren documenten.

Papierwerk is nog steeds de bron van veel voorkomende informatielekken

Van de 598 incidenten op het gebied van gegevensbescherming die tussen juli en september 2016 zijn geregistreerd door de Information Commissioner's Office (ICO, een Britse instantie voor gegevensbescherming), was:

14% te wijten aan verlies of diefstal van papierwerk, **19%** aan verkeerde adressering **en 4%** aan het achterlaten van documenten op een onveilige plek. **Nog eens 3%** was te wijten aan een onveilige vernietiging van het papier. Dus ondanks een exponentiële toename van digitale technologieën, was **40% van de incidenten** toe te schrijven aan papier.

40% van de incidenten op het gebied van gegevensbescherming in het Verenigd Koninkrijk zijn toe te schrijven aan papier



Incidenten op het gebied van gegevensbescherming

De rol van werknemers is van kritiek belang voor de naleving van de AVG

Als we kunnen concluderen dat het beveiligen van papieren documenten zeer belangrijk is voor de informatieveiligheid, dan vragen we ons af wat organisaties hieraan kunnen doen?

Rexel is gespecialiseerd in de levering van papierversnietigers. Omdat we rechtstreeks samenwerken met bedrijven zoals Kensington - wereldleider in fysieke beveiliging van IT-hardware - en de inzichten van klanten delen, beschikken we over waardevolle informatie over de behoeften en problemen van organisaties die zichzelf willen beschermen en willen voldoen aan de AVG.

Op basis hiervan denken we dat organisaties worden geconfronteerd met twee belangrijke barrières voor het doeltreffend vernietigen van hun documenten:

Ontbreken van bewustzijn

In een werkomgeving die steeds digitaler wordt, letten bedrijven niet op het belang van papier en nemen zich dus niet de tijd om veiligheidsproblemen die verband houden met papieren documenten op te lossen. Zelfs al bestaat er een beleid, dan nog ontbreekt het vaak aan bewustzijn als de regels niet doeltreffend worden gecommuniceerd op elk bedrijfsniveau.

Gebruiksgemak

De beschikbaarheid van geschikte papierversnietigers is van cruciaal belang voor het slagen van een beleid inzake het vernietigen van papier. Organisaties of kantoren vertrouwen te vaak op ineffectieve, handmatige papierversnietigers die niet voldoen aan de eisen, zodat hun werknemers de documenten niet effectief en productief kunnen vernietigen.

Zodra de barrières voor het invoeren van een doeltreffend papierversnietigingsbeleid binnen de organisatie zijn aangetoond, is de volgende stap het zoeken naar een geschikte oplossing.

De rol van werknemers #1 bij naleving van de AVG

Ontbreken van bewustzijn

Werknemers voeren over het algemeen activiteiten uit die door hun managers zijn bestempeld als prioriteit.

In dit licht kan een duidelijk en strikt beleid inzake het vernietigen van papier veel inefficiënt werk voorkomen.

Uit het onderzoek van PwC/Iron Mountain van 2014 blijkt dat slechts 40 % van het middenbedrijf duidelijke richtlijnen heeft voor het personeel over het weggooien en archiveren van papieren documenten, en slechts 27 % een bedrijfsbeleid heeft opgesteld voor de beveiliging, opslag en verwijdering van vertrouwelijke informatie.



De rol van werknemers #2 bij naleving van de AVG

Gebruiksgemak

Een tweede veel voorkomende oorzaak waarom werknemers geen gevoelige documenten vernietigen is dat de taak lastig en tijdrovend is.

Ook al kunnen de werknemers gebruik maken van papierversnietigers, dan nog zullen niet alle werknemers gevoelige documenten vernietigen als deze taak lastig is of veel tijd kost.

Het is dan ook niet verrassend dat organisaties niet willen investeren in papierversnietigers die hun werknemers niet willen gebruiken omdat ze weinig productief of onhandig in gebruik zijn. Deze problemen moeten dus eerst worden opgelost om maximaal gebruik te garanderen.



**Verhoog de productiviteit
van uw werknemers
met papierversnietigers
met automatische invoer**

Conclusie:

Papierversnieters met automatische invoer zijn een directe oplossing voor organisaties om hun personeel te stimuleren zorgvuldig om te gaan met informatie op papier.

Uit ons onderzoek⁴ blijkt dat 53 % van de werknemers papier in stapels vernietigt. Ze verzamelen dus verschillende documenten alvorens ze in één keer naar de papierversniet te brengen.

Uit onafhankelijk onderzoek is gebleken dat werknemers die hun documenten in stapels mogen vernietigen hier **98% minder tijd voor nodig hebben**⁵ en eerder geneigd zijn om vaker papier te vernietigen.



Benodigde tijd om
500 vel papier te
vernietigen

14:25 s
handmatig

00:14 s met
Rexel Auto+
papier-
vernietigers

6 kernpunten van AVG ter overweging



1. Overwegen een toezichthouder voor gegevensbescherming te benoemen

Deze toezichthouder moet volledig op de hoogte zijn van de verantwoordelijkheden van de organisatie met betrekking tot AVG en zeer goed begrijpen wat binnen uw organisatie gezien moet worden als ‘persoonlijk’, waar dit wordt bewaard, wie er toegang toe heeft, hoe informatielekken zijn te vinden en aan wie dit moet worden gerapporteerd. **De toezichthouder voor gegevensbescherming hoeft geen medewerker te zijn – u kunt deze taak ook uitbesteden.**



2. Uw systemen analyseren

Beoordeel alle contracten, technologische ondersteuning, procedures en instrumenten die betrekking hebben op het verwerken, behandelen, opslaan en verwijderen van gegevens, zodat u alle tekortkomingen of hiaten die moeten worden verholpen kunt vinden.



3. Een strategie ontwikkelen

Stel een nieuwe strategie op die gegarandeerd voldoet aan de AVG. Deze strategie kan leiden tot nieuwe investeringen in technologie, een herziening van de personeelsprocedures en de verantwoordelijkheden voor gegevensverwerking en nieuwe rollen creëren binnen de organisatie.



4. Een nieuw organisatiebeleid implementeren

De volgende stap naar naleving van de AVG is uw plan in de praktijk brengen binnen alle niveaus van de organisatie. Investeer in nieuwe technologieën en systemen die nodig zijn op de werkplek en stel een informatieve gids samen over het omgaan met en verwerken van gegevens.



5. Het personeel erbij betrekken

Introduceer uw nieuwe nalevingsbeleid bij het voltallige personeel; stel trainingen, informatie en gidsen beschikbaar voor werknemers, zodat ze zich bewust zijn van de veranderingen die plaatsvinden en van hun verantwoordelijkheden wat betreft het naleven van de AVG door het bedrijf.



6. Beoordelen en verbeteren

Nadat u uw plan om te voldoen aan de AVG heeft geïntroduceerd, is het tijd dit te beoordelen en indien nodig te verbeteren voordat de verordeningen van kracht worden. Als u ruim van tevoren eventueel noodzakelijke verbeteringen kunt vaststellen, zal uw organisatie de veranderingen voor mei 2018 op succesvolle en efficiënte wijze hebben doorgevoerd, zodat u volledig voldoet aan de eisen.

BRONNEN

- 1 envirowaste.co.uk/blog/articles/third-companies-shred-private-documents
- 2 Beyond good intentions: The need to move from intention to action to manage information risk in the mid-market, PwC report in conjunction with Iron Mountain, June 2014.
- 3 ico.org.uk/action-weve-taken/data-security-incident-trends
- 4 Evaluating Auto Feed Shredders. Opgesteld voor ACCO Brands door Deep Blue Insight.
- 5 Onafhankelijke test door Intertek Testing & Certification Ltd, juni 2012.
Maximale besparing bij gebruik van de Auto+ 500X in plaats van een traditionele papierversnietiger in dezelfde prijsklasse.
Uit onderzoek blijkt dat het gemiddeld 14 minuten en 25 seconden duurt om 500 vel papier in een traditionele handmatige papierversnietiger in te voeren en slechts 14 seconden om dit in een Auto+ 500X papierversnietiger te doen.

