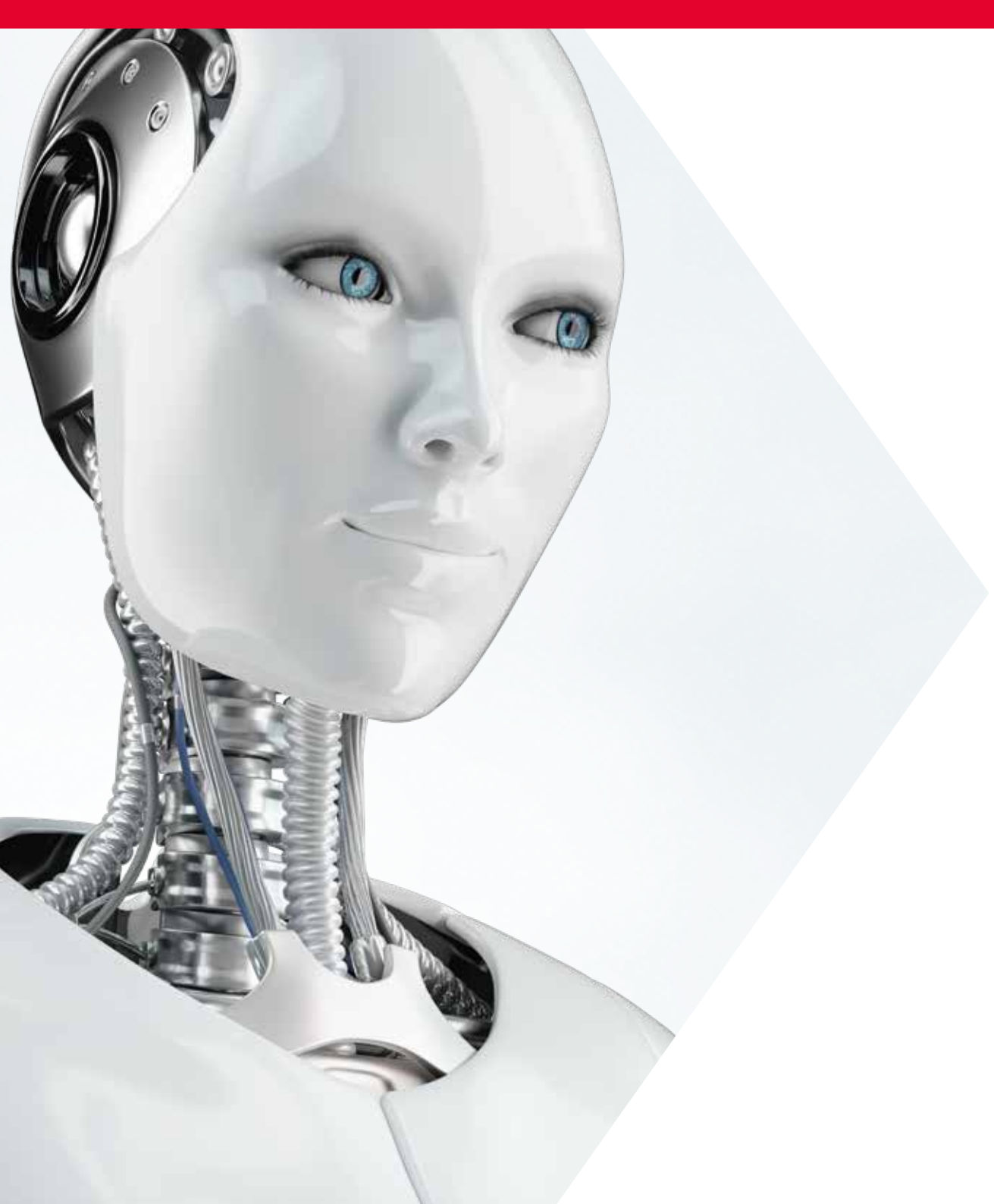


Intelligent papier vernietigen

Voor een generatie die voldoet aan de AVG

Waarom een veiligheidsbeleid voor papier een integraal onderdeel is voor de 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.

WORD AVG-PROOF*

* papier vernietigen ondersteunt de naleving van de AVG

Aangeboden door Viking

Over dit document

Deze whitepaper geeft u **een overzicht van de doelstellingen van de AVG**, de problemen die dit kan geven voor organisaties en biedt ondersteunende richtlijnen voor bedrijven om aan deze nieuwe wetgeving te voldoen.

Het doel van deze whitepaper is u een introductie te geven over de Algemene Verordening Gegevensbescherming (AVG) van de EU en over de manier waarop deze van invloed is op verschillende bedrijven, zodat u een kader kunt scheppen voor een veiligheidsbeleid voor uw eigen bedrijf nu deze wetgeving van kracht wordt.

Wat is de AVG eigenlijk? Deze verordening verplicht organisaties om goede veiligheidspraktijken toe te passen op zowel elektronische gegevens als gegevens op papier en om, in het geval van een datalek, de (mogelijke) 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, wordt er weinig aandacht besteed aan de beveiliging van gegevens op papier. Zo geeft bijna twee derde van de kantoren toe vertrouwelijke informatie niet te vernietigen[1]. 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 papiervernietigers - organisaties om hun beveilingsbeleid en -praktijken voor zowel gegevens op papier als elektronische gegevens te herzien.

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 datalekken
Het recht om te worden geïnformeerd in geval van een datalek.

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.

DE ALGEMENE VERORDENING GEGEVENSBESCHERMING

› 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 (Wbp):

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 datalekken

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

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.

Gegevensbeschermingseffect-beoordelingen 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 kunnen aantonen dat ze voldoen aan de AVG.

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

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.

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

AVG heeft betrekking op alle soorten persoons-gegevens in elektronische en fysieke vorm

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

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 bedrijfs-kader voor de naleving van de AVG

Organisaties hebben drie hoofdgebieden die beoordeeld moeten worden 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 aan alle aspecten van de AVG te voldoen.

Deze gebieden zijn:

Mensen

Het is van 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. 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.

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 Mountain[2] - 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.

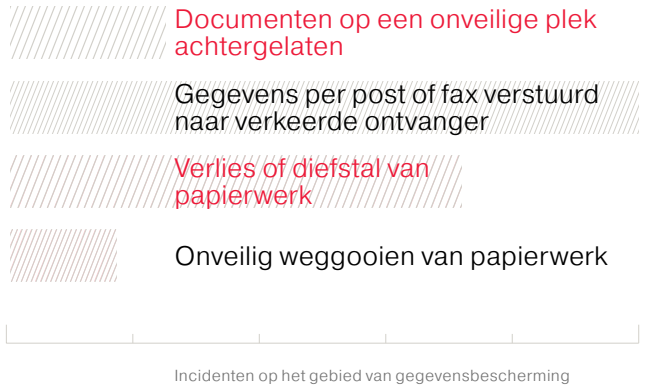
Hoewel digitale bedreigingen bij organisaties hoog op de agenda staat, zou het een vergissing zijn om te denken dat **er geen veiligheids-risico's meer bestaan voor papieren documenten**.

Papierwerk is nog steeds de bron van veel voorkomende datalekken

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 **en 19%** aan verkeerde adressering. **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[3].

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 cruciaal 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 papiervernietigers. 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 geven 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 papiervernietigers is van cruciaal belang voor het slagen van een beleid inzake het vernietigen van papier. Organisaties of kantoren vertrouwen te vaak op ineffectieve, handmatige papiervernietigers 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 papiervernietigingsbeleid binnen de organisatie zijn aangetoond, is de volgende stap het zoeken naar een geschikte oplossing.

Oplossing één voor 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[2] 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.

Oplossing twee voor 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 papiervernietigers, 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 papiervernietigers 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.

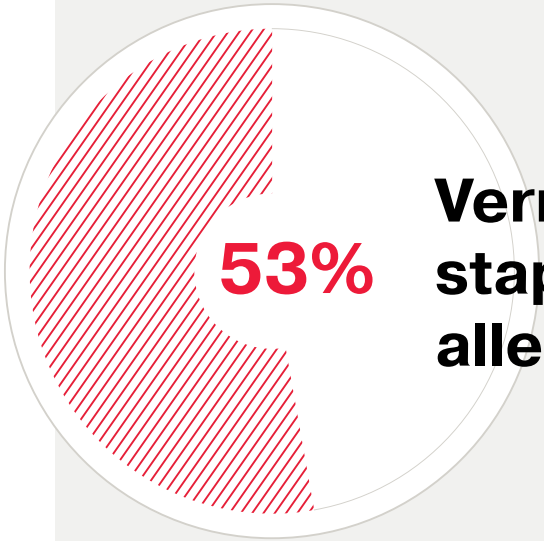
Verhoog de productiviteit van uw werknemers met papier-vernietigers met auto-matische invoer

Conclusie

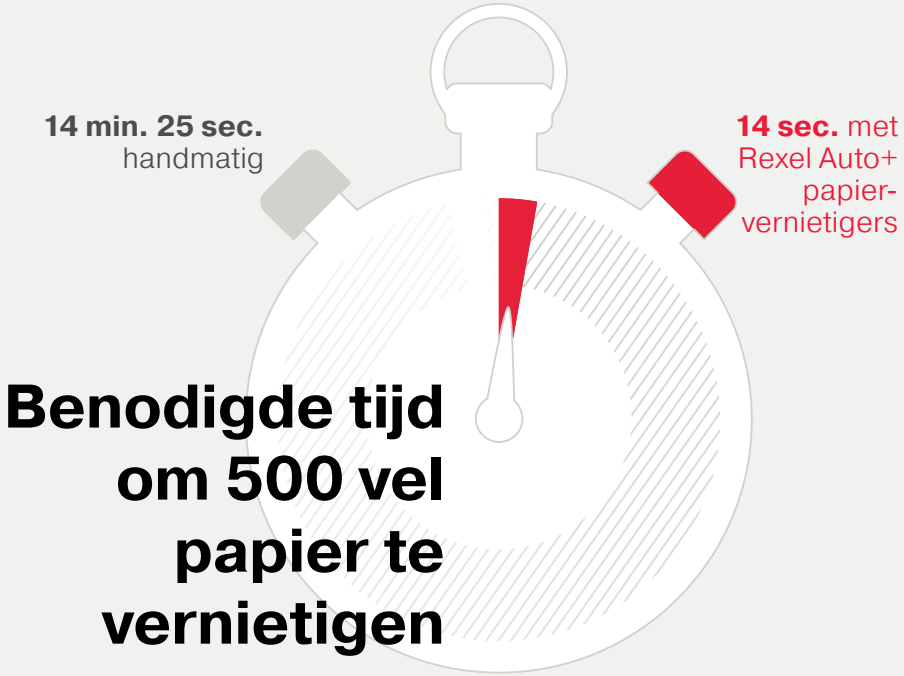
Zorg voor een werkend veiligheidsbeleid voor papier met Auto+ SmarTech papiervernietigers

Bij onze Auto+ SmarTech papiervernietigers wordt papier automatisch ingevoerd, waarbij monitoring en onderhoud vanuit meerdere locaties mogelijk is. Hierdoor is dit een directe oplossing om de naleving door werknemers van papierbeveiliging te stimuleren. Uit onderzoek[4] blijkt dat 53% van de werknemers papier in stapels vernietigt[5]. Ze verzamelen dus verschillende documenten alvorens ze in één keer naar de papiervernietiger te brengen.

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



Vernietigd in stapeltjes of alles in één keer



Benodigde tijd om 500 vel papier te vernietigen

6-Stappen AVG plan voor uw organisatie

1. Een toezichthouder voor gegevensbescherming 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 datalekken te vinden zijn en aan wie dit moet worden gerapporteerd. Deze taak als toezichthouder kunt u ook uitbesteden.

2. Uw systemen analyseren

Beoordeel alle contracten, technologische ondersteuning, procedures en instrumenten die betrekking hebben op alle gegevens handelingen, 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, moet het voortdurend worden herzien en verbeterd, zelfs nadat de voorschriften van kracht zijn geworden. Door voortdurend noodzakelijke verbeteringen te identificeren, zal uw organisatie de naleving van AVG op succesvolle en efficiënte wijze doorvoeren.

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. Prepared for ACCO Brands by Deep Blue Insight

5 Onafhankelijke test door Intertek Testing & Certification Ltd, juni 2012.

- Maximale besparing bij gebruik van de Auto+ 500X met SmarTech in plaats van een traditionele papiervernietiger in dezelfde prijsklasse
- Uit onderzoek blijkt dat het gemiddeld 14 minuten en 25 seconden duurt om 500 vel papier in een traditionele handmatige papiervernietiger in te voeren en slechts 14 seconden om dit in een Auto+ 500X papiervernietiger met SmarTech te doen.

www.rexeleurope.com

Voor meer informatie kunt u contact opnemen met:

Acco Brands
Vijzelmolenlaan 6
3447 GX Woerden,
Nederland
infonl@acco.com
Tel: 0348 - 415 084

Acco Brands
Industriepark-Noord 29
9100 Sint Niklaas, België
infobe@acco.com
Tel: 03 -760 33 11