Zo voldoet u aan AVG / GDPR

Over wat de nieuwe Europese wetgeving betekent voor uw ICT oplossingen en de omgang met persoonsgegevens

VOOR BETERE ICT BESLISSINGEN

ICT INFORMATIE CENTRUM

Zo voldoet u aan AVG / GDPR

Over wat de nieuwe Europese wetgeving betekent voor uw ICT oplossingen en de omgang met persoonsgegevens

Een uitgave van het ICT informatiecentrum, Houten

In samenwerking met KYOCERA Document Solutions Nederland B.V.

1e editie 2018 (01)

Voorwoord

In mei 2018 verandert er van alles aan de manier waarop u moet omgaan met persoonsgegevens. Dan treedt de Algemene Verordening Gegevensbescherming (AVG) of General Data Protection Regulation (GDPR) in werking. De wetgeving kan grote gevolgen hebben voor de ICT oplossingen die u gebruikt voor CRM, HRM, administratie of document management.

In dit e-boek dat het ICT informatiecentrum publiceert in samenwerking met kennispartner KYOCERA Document Solutions leest u over wat de AVG is, wat de gevaren ervan voor u zijn en wat u moet doen om tijdig aan de nieuwe privacywetgeving te voldoen. U maakt kennis met de belangrijkste feiten rondom de AVG. U krijgt basis- en kernaanbevelingen die u helpen om boetes te vermijden en om uw organisatie voor te bereiden op de AVG. En in zeven stappen wordt u uitgelegd hoe u ervoor zorgt dat uw organisatie klaar is voor de AVG.

Ofwel, beschikt u ergens in uw organisatie over persoonsgegevens, particulier en zakelijk, leest u dan dit boekje om tijdig maatregelen te treffen.

Succes met uw voorbereiding op de AVG!

ICTinformatiecentrum.nl

Meer informatie over ICT oplossingen

Het ICT informatiecentrum biedt u meer informatiebronnen over de toepassing, selectie en implementatie van ICT oplossingen. Op themagerichte websites vindt u informatie en overzichten van beschikbare oplossingen, leveranciers, dienstverleners rondom een specifiek ICT thema. Op algemene websites vindt u per thema alle leveranciers, whitepapers, boeken en berichten.

Themagerichte websites

CRMsystemen.nl	CRM en relatiebeheer, sales automation
ERPsystemen.nl	Financiële boekhouding, CRM , enz.
DMSsystemen.nl	Document management, ECM, (social) intranet
BIsystemen.nl	Business intelligence, big data, self service BI
HRMsystemen.nl	HRM software, e-HRM, ESS en MSS
WMSsystemen.nl	Warehouse management, voorraadbeheer
TMSsystemen.nl	Transport management
FinancialSystems.nl	Financiële software, (online) boekhouden
BPMsystemen.nl	Business process management
Overcloudcomputing.nl	Cloud computing, online software
Overdatacenters.nl	Datacenters, dataopslag

Algemene websites

ICTinformatiecentrum.nl	Overkoepelend
ICTleveranciers.nl	Overzicht van leveranciers
ICTwhitepapers.nl	Download van whitepapers, cases
ICTboekensite.nl	Aanvraag van boeken en publicaties
ICTberichten.nl	ICT nieuws

Inhoud

Gegevensbescherming in Nederland en de Europese Unie

In Nederland is het recht op privacy vastgelegd in de artikelen 10 tot en met 13 van de Nederlandse Grondwet. Een onderdeel van privacy, de verwerking van persoonsgegevens, wordt sinds 1 september 2001 nader geregeld in de Wet bescherming persoonsgegevens (WBP). Voordien werd dit in de Wet persoonsregistraties (WPR) geregeld. Naast de WBP regelen onder meer de Wet bescherming persoonsgegevens BES, de Wet basisadministraties persoonsgegevens BES en de Wet Politiegegevens de bescherming van persoonsgegevens. De organisatie die zich met de privacy van de Nederlandse burger bezighoudt, is de Autoriteit Persoonsgegevens.

De huidige Wet bescherming persoonsgegevens is de Nederlandse uitwerking van de Europese richtlijn bescherming persoonsgegevens (95/46/EG). De WBP is sinds 1 september 2001 van kracht.

Belangrijkste bepalingen Wet bescherming persoonsgegevens (WBP)
De belangrijkste bepalingen uit de WBP over het rechtmatig omgaan met persoonsgegevens, zijn als volgt samen te vatten:

- Persoonsgegevens mogen alleen in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier worden verwerkt.
- Persoonsgegevens mogen alleen voor bepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. En vervolgens alleen verder worden verwerkt voor doeleinden die daarmee verenigbaar zijn.
- Degene van wie persoonsgegevens worden verwerkt (de betrokkene genoemd), moet ten minste op de hoogte zijn van de identiteit van de organisatie of persoon die deze persoonsgegevens verwerkt (de zogeheten verantwoordelijke) en van het doel van de gegevensverwerking.
- De gegevensverwerking moeten op een passende manier worden beveiligd. Voor bijzondere gegevens, zoals over ras, gezondheid en geloofsovertuiging, gelden extra strenge regels.

De Europese Databeschermingsrichtlijn (officieel Richtlijn 95/46/EG)
In 2001 is de Wet bescherming persoonsgegevens (WBP) uitgevaardigd om de Nederlandse wetgeving af te stemmen op de Europese Databeschermingsrichtlijn uit 1995 (officieel Richtlijn 95/46/EG). Het primaire doel was om de bescherming van personen (zoals het verwerken van persoonsgegevens) af te stemmen op het vrije verkeer van personen en goederen in de EU. In de praktijk was het voor personen een manier om hun eigen persoonsgegevens te beheren. Daarom was Richtlijn 95/46/EG gebaseerd op **zeven principes**:

1. Kennisgeving: betrokkenen moeten ervan op de hoogte worden gesteld als hun gegevens worden verzameld.
2. Doel: gegevens mogen alleen worden gebruikt voor het vermelde doel en niet voor andere doelen.
3. Toestemming: gegevens mogen niet bekend worden gemaakt zonder de toestemming van de betrokkene.
4. Beveiliging: verzamelde gegevens moeten veilig worden bewaard en mogen niet misbruikt kunnen worden.
5. Openbaarmaking: betrokkenen moeten worden geïnformeerd over wie hun gegevens verzamelt.
6. Toegang: betrokkenen moeten toegang krijgen tot hun gegevens en in staat worden gesteld om eventuele onjuiste gegevens te corrigeren.
7. Aansprakelijkheid: betrokkenen moeten beschikken over een methode om gegevensverzamelaars aansprakelijk te stellen indien bovenstaande principes niet worden nageleefd. De lidstaten bepalen vervolgens zelf - binnen de grenzen van de Richtlijn- de voorwaarden waaronder het verwerken van de persoonsgegevens rechtmatig is. Binnen de Europese lidstaten werd de Richtlijn dan ook verschillend geïnterpreteerd.

Algemene Verordening Gegevensbescherming (AVG)

De Algemene Verordening Gegevensbescherming (AVG - officieel de Europese Verordening Gegevensbescherming (EU) 2016/679 van het Europees Parlement) werd aangenomen in april 2016 en vervangt eerdere verordeningen inzake gegevensbescherming, waaronder de Wet bescherming persoonsgegevens in Nederland. Aanvullende nationale wetgeving is niet nodig. De AVG wordt op 25 mei 2018 van kracht in heel Europa.

De primaire doelstelling van de AVG is dat burgers meer controle over hun persoonsgegevens krijgen. De bescherming van persoonsgegevens in de Europese Unie (EU) wordt verbeterd en gelijkgeschakeld, terwijl ook de export van persoonsgegevens buiten de EU wordt geregeld. Wanneer een organisatie te maken krijgt met een inbreuk in verband met persoonsgegevens, is afhankelijk van de ernst van de inbreuk onder de nieuwe Verordening het volgende van toepassing:

- Een organisatie moet de lokale autoriteit persoonsgegevens en indien mogelijk de eigenaren van de gelekte informatie op de hoogte stellen.
- Een organisatie kan een boete van maximaal 4% van de mondiale jaaromzet of € 20 miljoen krijgen.

De AVG voorziet echter in uitzonderingen op basis van de beveiligingsmaatregelen die binnen de organisatie zijn geïmplementeerd.

> **Voorbeeld**
> Bij een organisatie is sprake van een inbreuk in verband met persoonsgegevens. Deze organisatie heeft de gegevens door middel van versleuteling onbegrijpelijk gemaakt voor onbevoegden en is daarom niet verplicht om desbetreffende eigenaren van de gegevens op de hoogte te stellen. Dit is een belangrijk gegeven want hoewel het niet allesomvattend is, draagt het wel bij aan de naleving van de AVG en het mogelijk vermijden van een boete. De kans op een boete is ook kleiner indien de organisatie kan aantonen dat er sprake is van een ‘een inbreuk op beveiligde gegevens’.

Om te voldoen aan de AVG-bepalingen moeten organisaties mogelijk een of meer verschillende methoden voor versleuteling gebruiken voor omgevingen op locatie en in de cloud:

- Versleuteling van servers, inclusief bestanden, toepassingen, databases en virtuele machines.
- Versleuteling van pc's en harde schijven van randapparatuur, zoals printers; Versleuteling van opslag, waaronder NAS (network-attached storage) en SAN (storage area network).
- Versleuteling van netwerken, bijvoorbeeld via netwerkversleuteling met hoge snelheid zoals VPN's.

De 10 belangrijkste AVG feiten

De belangrijkste punten van de AVG en wijzigingen ten opzichte van de Europese Databeschermingsrichtlijn zijn hier opgesomd.

Verordening in plaats van richtlijn
Wat inhoudt dat dezelfde regelgeving is overgenomen door en van toepassing is in alle 28 EU-lidstaten.

Aanzienlijk verhoogde boetes
Bedrijven kunnen boetes worden opgelegd tot € 20 miljoen of 4% van de jaarlijkse wereldwijde omzet voor overtredingen van de wetgeving inzake gegevensbescherming. Het opgelegde bedrag zal afhangen van de ernst of herhaalde aard van een schending. Dit wordt bepaald door de toezicht-houdende autoriteit. Maar ook personen die willens en wetens AVG overtredingen toestaan kunnen persoonlijk verantwoordelijk worden gesteld en beboet.

Uitgebreide definitie van toestemming
Informatie van het Europees Parlement wijst op de bepalingen van de AVP inzake duidelijke en bevestigende toestemming voor de verwerking van particuliere gegevens door de betrokkene. Dit om consumenten meer controle te geven over hun privégegevens. Dit kan bijvoorbeeld betekenen dat er doormiddel van het actief aanvinken akkoord gegaan wordt met een verklaring of voorgestelde verwerking van de persoonsgegevens. Stille, standaard aangevinkte opties of leeglaten van de optie, zullen dus geen toestemming vormen. Het moet daarnaast ook net zo gemakkelijk zijn voor een consument om toestemming in te trekken als dat het is om hem te geven. De nieuwe AVG maakt ook een einde aan de kleine lettertjes in het privacy-beleid. Alle informatie moet in duidelijke taal worden gegeven voorafgaande aan het starten met het verzamelen of verwerken van gegevens.

Het recht om te worden vergeten
(Overweging 66) luidt: ‘ Ter versterking van het recht op vergetelheid in de online omgeving, dient het recht op wissen te worden uitgebreid door de

verwerkingsverantwoordelijke die persoonsgegevens openbaar heeft gemaakt te verplichten de verwerkingsverantwoordelijken die deze persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene heeft verzocht om het wissen van links naar, of kopieën of reproducties van die persoonsgegevens. Die verwerkingsverantwoordelijke dient daarbij, met inachtneming van de beschikbare technologie en de middelen waarover hij beschikt, redelijke maatregelen te nemen, waaronder technische maatregelen, om de verwerkingsverantwoordelijken die de persoonsgegevens verwerken, over het verzoek van de betrokkene te informeren.

Uitgebreide compliance
Directe toerekenbaarheid voor verwerker en verwerkingsverantwoordelijke van informatie: onder de oude regeling waren er geen verplichtingen voor de verwerkers (dat wil zeggen dienstverleners) van gegevens / informatie. Onder de AVG zijn verwerkers rechtstreeks aansprakelijk voor gegevensbeschermingsregels. Dit heeft een bijzondere impact op cloud providers, bijvoorbeeld die diensten bieden die de gegevens van de EU-bewoners bevatten. Om de naleving van deze verordening aan te kunnen tonen, dient de verwerkingsverantwoordelijke of de verwerker een register bij te houden van verwerkingsactiviteiten die onder zijn verantwoordelijkheid hebben plaatsgevonden.

Een document management systeem (DMS) of enterprise content management systeem (ECM) kan hierbij een goede ondersteuning bieden. Zie voor meer informatie hierover: DMSsystemen.nl.

Directe en indirecte identificatoren
In tegenstelling tot de oude richtlijn is in AVG vastgelegd wat onder persoonsgegevens wordt verstaan hier worden specifiek de criteria ‘locatiegegevens’ en ‘een online identificatoren’ aan toegevoegd.

Hieronder vallen onder andere:

- Connected devices; laptops, tablets, mobiele telefoon.

- Applicaties, tools en protocollen; IP-adressen (Internet Protocol), identificatie cookies.
- Andere, zoals Radio Frequentie Identificatie (RFID) tags
- IOT (Internet of Things).

Meldplicht datalekken
De AVG verplicht de verwerkingsverantwoordelijke om datalekken zonder onnodige vertraging en, indien mogelijk, uiterlijk 72 uur na de kennisgeving van de overtreding te rapporteren. Dit moet worden gerapporteerd aan de nationale gegevensbeschermingsautoriteit (AP of Autoriteit Persoons-gegevens in het geval van Nederland).

Bij de beoordeling van de gegevensbeveiligingsrisico's dient aandacht te worden besteed aan risico's die zich voordoen bij persoonsgegevens-verwerking, zoals de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot de doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig, hetgeen met name tot lichamelijke, materiële of immateriële schade kan leiden. Indien de persoonsgegevens onbegrijpelijk zijn gemaakt voor onbevoegden, zoals bijvoorbeeld versleuteling; is men vrijgesteld van rapportage.

Uitgebreide grenzen
De AVG is van toepassing op alle organisaties, ongeacht of ze gevestigd zijn in de EU. Als een organisatie goederen en diensten levert in de EU, dan moet het voldoen aan de AVG. De wet is dus van toepassing als u binnen de EU bent gevestigd, of diensten aanbiedt aan EU-ingezetenen, of het gedrag van EU-ingezetenen observeert.

Functionaris voor gegevensbescherming
De verwerkingsverantwoordelijke en de verwerker zijn verplicht een functionaris voor gegevensbescherming (FG) aan te wijzen indien zij op grote schaal en als onderdeel van hun kernactiviteiten regelmatig en systematisch individuen observeren of gevoelige persoonsgegevens verwerken.

Een functionaris voor gegevensbescherming kan ook een deeltijdrol zijn of gecombineerd worden met andere taken. Bij het uitvoeren van de rol moet de FG echter een onafhankelijke rapportage lijn hebben. De FG brengt rechtstreeks verslag uit aan de hoogste leidinggevende van de verwerkingsverantwoordelijke of de verwerker. Ter referentie de exacte mandaten (artikel 37) de volgende woorden:

- De verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, behalve in het geval van gerechten bij de uitoefening van hun rechterlijke taken.
- Een verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doel-einden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen.
- De verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens uit hoofde van artikel 9 en van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10.

Gegevensbeschermingseffect beoordeling
Organisaties hoeven, zodra de AVG geldt, niet voor elke gegevensverwerking een check uit te voeren. Deze is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacy risico oplevert voor de betrokkenen (de mensen van wie de organisatie gegevens verwerkt).

Dat is in ieder geval zo, als een organisatie:

- Systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profilering.
- Op grote schaal bijzondere persoonsgegevens verwerkt.
- Op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied, bijvoorbeeld met cameratoezicht.

Buiten deze drie situaties geeft de AVG geen overzicht van verwerkingen met een hoog risico. De werkgroep van Europese privacytoezichthouders

(WP 29) heeft criteria opgesteld om het risico te bepalen. Daarnaast publiceert de Autoriteit Persoonsgegevens (AP) op termijn een lijst van verwerkingen waarvoor een PIA verplicht is.

4 AVG fabels ontkracht

Fabel 1 - Ik moet een onafhankelijke en gekwalificeerde functionaris voor gegevensbescherming aanwijzen

De drie hoofdcriteria voor het aanwijzen van functionarissen voor gegevens-bescherming (artikel 35) indien uw kernactiviteiten inhouden:

- Stelselmatige en grootschalige monitoring van personen.
- Grootschalige verwerking van gevoelige gegevens.
- Overheidsinstanties.

De functionaris hoeft niet voltijds in dienst van de organisatie te zijn. Deze functie kan indien nodig worden uitbesteed. Als een organisatie niet onder de bovenstaande criteria valt, hoeft de organisatie geen externe persoon te benoemen. Er kan een werknemer worden aangewezen en het kan een deeltijdfunctie zijn of een functie die wordt gecombineerd met andere taken. Bij het uitvoeren van de functie moet de functionaris echter wel rapporteren aan een aangewezen onafhankelijke persoon (net zoals de meeste nalevingsfunctionarissen), bevoegdheden hebben en rechtstreeks aan de directie rapporteren zonder tussenkomst van derden. Van belang is dat de aangewezen persoon een professional op het gebied van gegevensbescherming met specialistische kennis van regelgeving inzake en toepassing van gegevens-bescherming. Zo kan deze functionaris zekerstellen dat uw organisatie de AVG nu en in de toekomst naleeft.

De aangewezen functionaris implementeert in het ideale geval een strategie en een project, met als primair doel om de AVG na te leven of te overtreffen. In het kader van het project moeten organisatorische, procedurele en technische maatregelen worden genomen waarmee de naleving aangetoond kan worden.

Fabel 2 - Ik heb niets te maken met het opslaan van gegevens, dus ik ben niet aansprakelijk onder de AVG

Onder de AVG moeten verwerkingsverantwoordelijken en verwerkers naleving van de AVG aantonen door gegevens nauwkeurig te verwerken. Onder de oude regelgeving

hadden verwerkers van gegevens/informatie (zoals serviceproviders) geen verplichtingen. Onder de AVG zijn verwerkers echter direct verantwoordelijk voor het naleven van regels inzake gegevensbescherming. Dit is met name van invloed op bijvoorbeeld cloudproviders, die services aanbieden waarbij gebruik wordt gemaakt van gegevens van EU-inwoners. De effecten van bovenstaand kunnen worden beperkt door middel van implementatie van een enterprise content management systeem (ECM) en gebruik van een geschikt document management systeem. Bijvoorbeeld informatie over wie de verwerker is? Wie is de Pagina 16 verwerkings-verantwoordelijke? Onderwerp van de verwerkte gegevens? Gegevenscategorieën? Gevoelige gegevens? Enzovoort.

Bedrijven moeten de AVG gebruiken als hoeksteen voor risicobeheersing. Aansprakelijkheid kent niet langer beperkingen: tegenwoordig zijn zowel de verwerkingsverantwoordelijke als de externe verwerkers evenredig aansprakelijk voor een inbreuk in verband met gegevens (zie artikelen 24, 26, 27, 28 en 29).

Fabel 3 - Ik heb een document management of content management systeem geïmplementeerd. Ik leef dus de AVG na.

De AVG geeft helaas geen duidelijke voorbeelden van de technologie en/of beveiliging die moet worden gebruikt. Er wordt alleen gesteld dat ‘passende’ en ‘moderne technische beveiligingsmaatregelen’ moeten worden geïmplementeerd. Dit is mogelijk met opzet vaag omschreven, omdat de technologie zich blijft ontwikkelen. De geïmplementeerde technologie moet dus ‘mee-ontwikkelen’. Het kan zijn dat uiteindelijk de rechter bepaalt wat ‘modern’ is of was ten tijde van een mogelijke inbreuk op gegevens.

Hoewel de vage regelgeving op dit gebied zich lastig laat interpreteren is, vindt KYOCERA dat de implementatie van één of meerdere technische oplossingen de naleving van de AVG eenvoudiger en efficiënter maakt ten opzichte van handmatige verwerking. Indien een bedrijf niet beschikt over de juiste processen en zich niet richt op wat in de AVG ‘de belichaming van het concept van privacy by design’ wordt genoemd, wordt de AVG niet per definitie nageleefd wanneer er een content management systeem aanwezig is.

Fabel 4 - Al mijn systemen zijn versleuteld. Ik leef dus de AVG na.

Met betrekking tot boetes zijn in de AVG geen belangrijke uitzonderingen opgenomen die worden gebaseerd op het wel of niet implementeren van de juiste beveiligingsmaatregelen door organisaties.

> **Voorbeeld**
> Bij een organisatie heeft zich inbreuk in verband met de persoonsgegevens voorgedaan. Deze organisatie heeft de gegevens die zijn uitgelekt naar een onbevoegde persoon, echter onbegrijpelijk gemaakt met behulp van versleuteling. In dit geval is de organisatie niet verplicht om de desbetreffende eigenaren van de gegevens op de hoogte te stellen. Dit is een belangrijk gegeven, want hoewel het niet allesomvattend is, draagt het wel bij aan de naleving van de AVG en het mogelijk vermijden van een boete.

Voorbereiden op de AVG in 7 stappen

Waar het uiteindelijk op neerkomt, is of er aan de nieuwe AVG wordt voldaan. Kan uw organisatie in een rechtbank de acties en processen die u heeft genomen om AVG te implementeren, voldoende verdedigen? Hierdoor vermindert de kans op aansprakelijkheid en een boete.

Voldoen aan de AVG houdt het proactief implementeren in van het juiste personeel, procedures en processen, om ervoor te zorgen dat gegevens adequaat worden beschermd en behandeld. Dit in plaats van te worden behandeld als ad-hoc en last-minute overweging.

Om te kunnen voldoen aan de in de AVG gestelde richtlijnen of deze te overtreffen, gaat om het uitvoeren van effectbeoordelingen op het gebied van gegevens-bescherming (zie artikel 35) en het introduceren van aanvullende technologie, zoals document management systemen, versleuteling, beveiligd transport en opslag van gegevens, enz.

Bedrijven zouden AVG moeten gebruiken als een hoeksteen voor hun risico-beperkingsproces. Er is geen mogelijkheid meer voor de aansprakelijkheid weg te lopen, aangezien zowel de beheerder als de onderaannemer gelijkwaardig zijn voor een inbreuk op gegevens (zie artikelen 24, 26, 27, 28 en 29).

Helaas, hebben veel organisaties last van een wildgroei van ongestructureerde en ongeautoriseerde applicaties die gebruikt worden om bestanden op te slaan en te beheren. Dit leidt tot verhoogde veiligheidsrisico's en verminderde productiviteit en informatiebeschikbaarheid binnen een organisatie. Bijkomend voordeel van voldoen aan de AVG is voor de organisatie dat ze meer inzicht, flexibiliteit en controle hebben over de gegevens, documenten, data en content.

De onderstaande aanbevelingen en acties zullen helpen om de nieuwe regels te begrijpen en te interpreteren en één enkel strategisch, gestructureerd, top-down, beleid en overzicht te hebben van geclassificeerde persoonlijke geïdentificeerde informatie.

Er zijn enkele basis- en kernaanbevelingen die KYOCERA voorstelt om de boete te vermijden en ervoor te zorgen dat uw organisatie aan de AVG voldoet. Neem daarom de volgende stappen in overweging.

Stel een verantwoordelijke aan

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensbescherming (FG) aan te stellen. Bepaal nu alvast of dit voor uw organisatie vereist is:

- De verwerking wordt verricht door een overheidsinstantie of overheids-orgaan, behalve in het geval van gerechten bij de uitoefening van hun rechterlijke taken.
- Een verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doel-einden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen.
- De verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens uit hoofde van artikel 9 en van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10.

Zo ja, wacht dan niet te lang met het werven van een FG. Om ervoor te zorgen dat uw organisatie de wetgeving nakomt en onderhoudt is het van belang dat de aangestelde persoon een professional is op het gebied van gegevensbescherming met deskundige kennis en ervaring op de gegevens-beschermingswetgeving

De aangewezen persoon zal een strategie en project moeten implementeren, met als hoofddoel het voldoen aan / overtreffen van AVG-naleving. Het project moet organisatorische, procedurele en technische maatregelen uitvoeren en vastleggen om aan de controle eis te voldoen.

Informeer uzelf en uw organisatie

De AVG wordt op 25 mei 2018 actief. Het is daarom van essentieel belang dat u zich nu op de hoogte stelt en op de hoogte blijft van de informatie

betreffende de AVG. Er is een enorme hoeveelheid informatie en begeleiding met betrekking tot de AVG te vinden op de website van de Autoriteit Persoonsgegevens.

Zorg ervoor dat de relevante mensen in uw organisatie (zoals beleids-makers) op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Houd er rekening mee dat de implementatie van de AVG veel kan vragen van de beschikbare mankracht en middelen en begin er daarom op tijd mee.

De Autoriteit Persoonsgegevens (AP) biedt instrumenten die u kunnen helpen om de AVG na te leven, zoals guidelines die zijn opgesteld samen met de andere privacy toezichthouders in Europa. Bedenk dat de AP uw organisatie sancties kan opleggen van maximaal 20 miljoen euro of 4% van uw wereldwijde omzet als u zich niet aan de nieuwe privacywetgeving houdt.

Onderzoek

De AVG geeft niet veel exacte aanwijzingen over welke technologie (zie de overwegingen 66, 67, 68, 71, 78, 81, 156, 168) en beveiliging (zie artikel 32) moet worden toegepast gegevensbescherming te bereiken. Daarentegen wordt het omschreven als ‘ Rekening houdend met de stand van de techniek, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen.

De onduidelijkheid van de AVG met betrekking tot de precieze invulling van technologie die moet worden gebruikt, maakt de interpretatie van de verordening lastig.

Het is logisch om te stellen dat de implementatie van een technische oplossing de naleving van de AVG zal vereenvoudigen en efficiënter maken in vergelijking met handmatige verwerking. Het is hoogstwaarschijnlijk ook de meest kosteneffectieve optie voor de toekomst om aan de volgende eisen te kunnen voldoen:

- Gegevens juistheid (Artikel 5 – actuele data).
- Recht van inzage (Artikel 15 – het vermogen van een bedrijf om aan een aanvraag tot inzage van gegevens te voldoen).
- Recht van rectificatie en wissen van gegevens (ook bekend als recht op vergetelheid) (zie artikelen 16 en 17).

Breng uw gegevensverwerkingen in kaart. Documenteer welke persoons-gegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt. Onder de AVG heeft u een documentatieplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt. U kunt het overzicht ook nodig hebben als betrokkenen hun privacy-rechten uitoefenen.

Als zij u vragen hun gegevens te corrigeren of verwijderen, moet u dit doorgeven aan de organisaties waarmee u hun gegevens heeft gedeeld. Vermeld in het overzicht ook per categorie van gegevens op basis van welke wettelijke grondslag u deze gegevens verwerkt. Beroept u zich bijvoorbeeld op een gerechtvaardigd belang of vraagt u toestemming aan de betrokkenen? Technologie zal u helpen dit te bereiken.

Technologie
In een organisatie kunnen een groot aantal toegangs- en uitgangspunten bestaan waaruit gegevens, waaronder persoonsgegevens, kunnen vloeien. Deze omvatten naast elektronisch (e-documenten) ook de traditionele papierformaten. Het is belangrijk om te begrijpen waar deze gegevens worden vastgelegd, verwerkt, uitgevoerd en behouden. Het uitvoeren van een grondig onderzoek hiervan met bijzondere aandacht voor de persoons-gegevens, is de eerste stap naar een goed record management systeem dat voldoet aan de richtlijnen van AVG.

Behandeling van persoonsgegevens moet beperkt blijven tot wat nodig is en gekoppeld is aan het doel ervan (data minimalisatie en opslag beperking principes). Onder de AVG is er een nieuwe documentatieplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt.

DMS / ECM

De implementatie van technologie, zoals een elektronisch document management systeem of content management systeem, kan een van de belangrijkste enablers zijn bij het omgaan met persoonsgegevens binnen de AVG. Bij het selecteren van een dergelijk systeem, zijn er onderstaande richtlijnen die u kunnen helpen:

- **Vertrouwelijkheid -** Door informatie te beschermen tegen onbevoegde toegang en openbaarmaking.
- **Integriteit -** Door de juistheid en volledigheid van de informatie te waarborgen en zijn onbevoegde wijziging of verwijdering te voorkomen.
- **Beschikbaarheid -** Door te garanderen dat gegevens en bijbehorende diensten veilig zijn voor geautoriseerde gebruikers, wanneer en waar nodig.
- **Register van de verwerkingsactiviteiten -** Elke verwerkingsverantwoordelijke houdt een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden.

Een document management oplossing moet:

- Voorzien zijn van een geïntegreerde beveiliging en compliance (privacy by design & privacy by default) vanaf het begin van de vastlegging (data capture), gedurende het gehele proces (data integratie) tot het verwijderen van de gegevens (data deletion).
- Gebruikers het vertrouwen geven dat wat ze doen veilig is door beveiligingssleutels, twee stappen verificatie, tokens en encryptie te implementeren.
- De kans op datalekken verminderen door document types te scheiden. Classificeer en definieer gegevens bij vastlegging. Worden de gegevens als persoonlijk beschouwd en wat is de minimale en maximale bewaar termijn (retentieplan). Op deze manier worden gegevens voordat ze in het DMS worden opgeslagen en verwerkt kunnen worden voorzien van de juiste classificatie van privégegevens en de retentieregels eromheen, waardoor de kans op datalekken, hackeraanvallen, interne dreigingen en diefstal aanzienlijk afnemen of worden voorkomen.

- De persoonsgegevens op een veilige manier maar eenvoudig vindbaar voor geautoriseerde verwerkers bewaren.
- nzichtelijk maken wie toegang heeft (gehad) tot persoonlijke gegevens en welke verwerkingen er zijn uitgevoerd (audit trail).

Versleuteling
Versleuteling (encryptie) is een van de technologieën die specifiek in AVG zijn genoemd, als een beveiliging tegen verlies van persoonsgegevens, en daarom belangrijk tegen een organisatorische datalek. Versleuteling is belangrijk, omdat in het geval van een datalek, de AVG zegt dat de indien de persoonsgegevens onbegrijpelijk gemaakt zijn voor onbevoegden door versleuteling de organisatie niet verplicht is om de betrokken in kennis te stellen.

Informatie op dataopslag, netwerkarchitecturen en randapparatuur zoals pc's, USB-sticks en MFP's en printers moeten worden gecodeerd om gegevens te beveiligen.

Continuïteits- / verbeteringsplan
Organisaties moeten begrijpen dat als het initiële project is afgerond en de organisatie voldoet aan de AVG het daar niet eindigt. Een continuïteits- / verbeterplan moet er voor zorgen dat de veiligheid van persoonsgegevens continu wordt bekeken en indien mogelijk verbeterd. Dat persoons-gegevens volgens de retentie regels worden verwijderd of bewaard en dat processen worden aangepast en geoptimaliseerd.

De functionaris voor de gegevensbescherming is cruciaal voor deze rol, zowel als een sponsor of als actieve deelnemer. De FG moet door de directie worden gesteund om gericht en op het juiste moment te kunnen handelen.

Beveiliging van uw printerpark

In vergelijking met de stand alone kopieermachines van voorheen, is er veel veranderd. Tegenwoordig zijn printers en multifunctionals (MFP's) intelligente, via een netwerk verbonden machines, die evenals een pc een scherm, toetsenbord, harde schijf (die mogelijk gevoelige informatie kan opslaan) en besturingssysteem (OS) bevatten.

Toenemende cybercriminaliteit die direct gericht is op netwerkapparatuur, zoals printers, is aangemerkt als een zwakke link in de verdediging tegen bedrijfsdiefstal en een kwaadaardige aanval. Veel organisaties zien de beveiliging van een printer echter over het hoofd. Hierdoor kunnen printers worden besmet en uiteindelijk het gehele netwerk in gevaar brengen met mogelijk diefstal van gegevens tot resultaat. Om de zaak te compliceren bevat de wijzigingen in de AVG-wetgeving potentiële grote financiële en juridische maatregelen bij het niet naleven van deze wetgeving.

Artikel 34
Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene.
Artikel 3 en 3a melden dat:

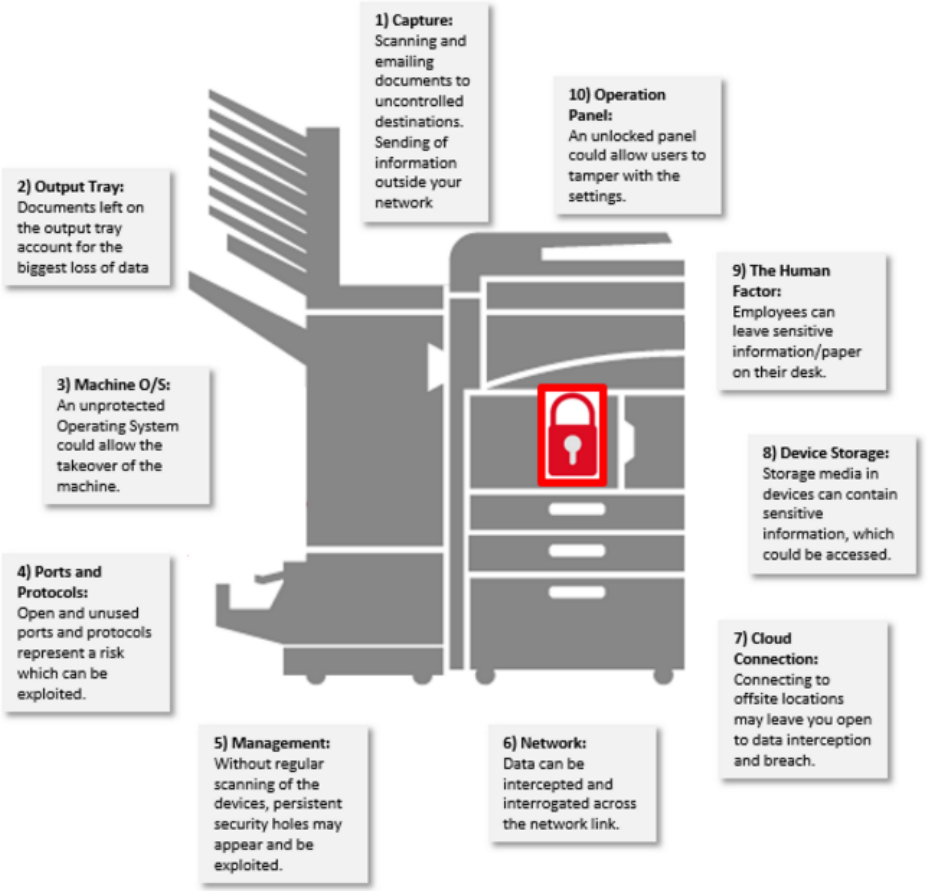
''De bedoelde mededeling aan de betrokkene is niet vereist wanneer de volgende voorwaarde is vervuld:

De verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling. ''

Dit is definitief en betekent dat organisaties onmiddellijk actie moeten ondernemen en het printerpark in hun algemene gegevensbescherming- en beveiligingsstrategie opnemen.

De kwetsbaarheden ten aanzien van de beveiliging van een MFP zijn hier voor u geëvalueerd; welke kunnen worden verminderd of voorkomen door de beveiligings-

maatregelen (inclusief encryptie van MFP-harde schijven) die hieronder zijn beschreven te implementeren.



1. Afvangen

Bij het kopiëren kunnen de volgende functies ongeautoriseerde kopieën voorkomen en de document beveiliging verbeteren. KYOCERA MFP's hebben de volgende kopieermogelijkheden / restrictieve maatregelen:

- **Tekststempel / Bates-stempel**
  Gebruikers kunnen afhankelijk van het type document dat zij afdrukken documentstempels selecteren zoals 'vertrouwelijk', 'niet dupliceren' en 'privacy'. Deze worden op het geprinte document over de tekst geprint. Gebruikers kunnen indien nodig de tekst voor de stempel naar wens aanpassen. De Bates-stempelfunctie 'serienummer' print het serienummer van de machine die wordt gebruikt voor de opdracht en een nummer-functie die paginanummers in volgorde op de gedrukte documenten print. Bovendien zijn ook de functie 'datum' en 'gebruikersnaam' beschikbaar.
- **Veiligheid watermerk**
  Het gedrukte document kan worden voorzien van een onzichtbaar beveiligingswatermerkpatroon of tekst. Wanneer geprinte documenten die van dit patroon zijn voorzien worden gekopieerd, wordt het beveiligings-watermerkpatroon zichtbaar. Dit geeft duidelijk aan dat er een onbevoegde kopie is gemaakt.
- **Document Guard Kit**
  De Document Guard Kit biedt een optionele functie die een beveiligings-patroon in een document inbrengt. Wanneer gebruikers het document met een speciaal beveiligingspatroon kopiëren, scannen of faxen, stopt de machine met werken en ongeautoriseerd kopiëren verhinderd. Dit voorkomt het lekken van waardevolle informatie. Als de Document Guard Kit niet op het apparaat is geïnstalleerd, verschijnt het beveiligings-watermerkpatroon, waarbij gebruikers worden gewaarschuwd dat het een onbevoegde kopie is.
- **Bevestig en verander e-mail / scan- / verzendbeperkingen**
  Een ander gebied dat kan helpen bij het afvangen van documenten en het beheersen van waar deze worden afgeleverd zodra ze worden gescand is. Bijvoorbeeld; e-mail bestemmingen kunnen worden beperkt door gebruik te maken van de e-mail verzendbeperkingsfunctie. Toegestane bestemmingsadressen worden vooraf geregistreerd, zodat e-mails alleen naar de toegestane geregistreerde bestemmingsadressen kunnen worden

verzonden. verboden bestemmingsadressen kunnen ook vooraf worden vastgelegd, zodat e-mails naar die bestemming worden geweigerd.

De Koyocera MFPs / printers hebben de mogelijkheid om e-mail attachments af te drukken. E-mail ontvangst kan worden beperkt door de 'e-mail afzender beperking functie. Toegestane afzenderadressen worden vooraf geregistreerd, zodat alleen e-mails van de toegestane afzender kunnen worden ontvangen. Verboden afzender-adressen kunnen ook vooraf worden geregistreerd.

2. Uitvoerlade

Er zijn veel verschillende soorten printcontrolesystemen beschikbaar, die kosten-besparing en beheer bieden. Deze bieden de mogelijkheid om beveiliging te regelen voor informatie die over het netwerk gaat. Het basisprincipe van print control oplossingen is dat de gebruiker een opdracht print naar een gedeelde 'virtuele' wachtrij die op een centrale printserver wordt gehost. De opdracht wordt op die server vastgehouden totdat de gebruiker zich bij een machine authenticeert en de opdracht(en) selecteert die hij wil afdrukken. De afdruktaak wordt dan de betreffende machine gestuurd en geprint. Auditinformatie wordt vervolgens geregistreerd op de server voor rapportagedoeleinden.

Deze methode biedt een aantal voordelen, namelijk:

- Opdrachten worden geprint terwijl de gebruiker aanwezig is bij de machine.
- Er wordt geen informatie bewaard op de machine.
- Beperkingen op gebruikersrechten kunnen worden ingeregeld.
- Afdrukkosten worden verminderd.
- Het zorgt voor verbeterde beveiliging van het apparaat.

3. Machinebesturingssysteem

Om bescherming te bieden tegen mogelijke cyber- en hack dreigingen, wordt door alle KYOCERA-printers bij het opstarten een zelfhelende / zelf beschermende controle uitgevoerd. Als een configuratie of belangrijke parameters zijn gewijzigd zonder autorisatie zal de machine een passende foutmelding geven.

4. Poorten en protocollen

KYOCERA kan protocollen uitschakelen die niet nodig zijn / specifieke communicatie-poorten vergrendelen op:

- Netwerkbeveiligingsniveau: MFP's / printers kunnen communicatie op het netwerk beperken om alleen via een bepaald bereik van IP-adressen en poortnummers te verzenden en ontvangen
- IP-adresfilterniveau: hiermee wordt de toegang vanaf het netwerk tot de MFP's / printers beperkt tot een bepaal bereik van IP-adressen of type protocol.

Gebruik veilige communicatieprotocollen

Beveiligde communicatieprotocollen zorgen voor een bescherming van het netwerkcommunicatiekanaal. Afhankelijk van het doeleinden of versleutelschema, zijn er verschillende protocollen beschikbaar, waardoor gegevens effectief beschermd worden tegen veranderingen of lekken via het netwerk.

Het gebruik van een netwerkverificatieprotocol is een effectieve methode om authenticatie te verkrijgen voor beveiligde communicatie. De MFP's / printers ondersteunen IEEE802.1x-netwerkverificatie, SMTP-verificatie en POP voor SMTP-verificatieprotocol, bijvoorbeeld bij het gebruik van 'send to email'.

Schakel de USB-poortfuncties en optionele interfaces uit

Als een USB-geheugen op de machine wordt aangesloten, bestaat er een risico op verlies van gegevens of onbevoegde toegang tot gegevens die op het apparaat zijn vastgelegd. De beheerder kan de USB Storage Class uitschakelen waardoor het gebruik van USB opslagmedia wordt uitschakelt, maar de verbinding van andere USB-apparaten zoals kaartlezers, toetsenborden enz. mogelijk blijft. De beheerder kan ook de optionele interfaces (sloten 1 en 2) uitschakelen om te voorkomen dat ongeautoriseerde interfaces worden aangesloten.

5. Beheer

Machines worden vanuit de fabriek geleverd met een standaard wachtwoord. Het wordt sterk aangeraden om dit te veranderen. Kies een passend sterk wachtwoord dat voldoet aan het lokale beleid en gebruik geen bestaande gebruikersnaam / wachtwoord van een computer account.

> **Opmerking:** Bewaar het wachtwoord goed. Als een MFP-wachtwoord wordt vergeten kan dit alleen worden verholpen door de machine terug te zetten naar de fabrieks-instellingen.

> **ID-kaart / RFID-toegang**
> Als proximity ID media wordt gebruikt als toegangscontrole tot het gebouw of voor tijdregistratie, kan hetzelfde ID-medium worden gebruikt voor gecontroleerde toegang tot de printers en MFP's te geven. Dit is zowel gebruiksvriendelijke en efficiënt. Door dit te combineren met de opslagfunctionaliteit van de MFP, kunnen opdrachten worden geprint op basis van toegangs-authorisatie.

6. Netwerk

Doordat moderne multifunctionals intelligentie bevatten in de vorm van een besturingssysteem, maakt dit ze een potentieel doelwit voor cyber-bedreiging en voor diefstal van zowel gegevens als gebruikers- en netwerk-informatie.

Met behulp van enterprise grade beveiliging binnen het netwerk kan al het binnenkomende en uitgaande verkeer naar de MFP-vloot worden gemonitord op mogelijke bedreigingen. Malware overschaduwt inmiddels de traditionele virussen als de meest voorkomende bedreiging op het internet. Nieuwe generaties van geavanceerde malware worden vaak aangeduid als Advanced Persistent Threats (APTs).

7. Cloud connectiviteit

In de afgelopen tijd hebben sommige printcontrolesystemen zich verder ontwikkeld om problemen met betrekking tot bandbreedte en documentbeveiliging aan te pakken als via cloud-gebaseerde servers wordt geprint. Een proces als 'Local Print Spooling' kan worden ingezet door een pc of MFP in het lokale netwerk aan te wijzen om de afdruktaak vast te houden, waarbij alleen de rapportage informatie en

afdrukbeleid informatie naar de server wordt verzonden. Zodra een gebruiker zich op een MFP aanmeld, wordt de printopdracht verzonden naar het geselecteerde apparaat en geprint. Deze methode vermindert het gebruik van de bandbreedte aanzienlijk en houdt documenten binnen de lokale netwerkgrens. De toevoeging van een aparte server kan ook worden gebruikt zo kunnen lokaal machines, gebruikers en gebruiks-informatie worden beheert welke weer kunnen worden gesynchroniseerd met een centrale master server.

Met bovenstaande toepassingen kan ook de toegang tot scannen, bestemmingsbeperkingen en andere functionaliteiten worden beperkt op basis van globale, groeps- of individuele behoeften.

Een Virtual Private Network (VPN) is een zeer veilige methode om een kantoor netwerk te verbinden via een openbaar netwerk. KYOCERA maakt voor het beveiligen van afdrukinformatie in over het netwerk gebruik van VPN's. Alle gegevens die over deze verbindingen worden getransporteerd, worden in hoge mate gecodeerd. VPN's vereisen gespecialiseerde apparatuur en om de VPN 'tunnel' te maken, inrichting door een goed gekwalificeerde technicus.

Er zijn twee typen VPN in gebruik:

- Een site-to-site verbinding – die meestal gebruikt wordt om kantoren of gebouwen te verbinden.
- Een client-based connection – Deze worden gebruikt om locaties op een 'ad-hoc' manier met elkaar te verbinden; Bijvoorbeeld wanneer een mobiele 4G-router wordt aangesloten op een cloud-based server.

8. Data opslag
Gevoelige of vertrouwelijke informatie kan op de HDD of SSD van de machine worden opgeslagen waarvoor extra beveiliging kan worden geïmplementeerd. Deze voldoet aan de Common Criteria Certification (ISO 15408) en kan gebruikt worden om ofwel A) de HDD / SSD te versleutelen of B) de gegevens overschrijven:

- **HDD / SSD-versleuteling**
  HDD / SSD-versleutelingsfunctie is een beveiligingsfunctie die documenten, gebruikersinstellingen en machine informatie op de harde schijf of SSD

versleutelt. Encryptie wordt toegepast op de data met behulp van de 128-bits en 256-bits AES (Advanced Encryption Standard: FIPS PUB 197) algoritme. Als de HDD of SSD uit de MFP wordt verwijderd, is gevoelige of vertrouwelijke informatie die is opgeslagen op de HDD of SSD niet toegankelijk.

- **HDD overschrijven-wissen**
  HDD overschrijven-wissen is een beveiligingsfunctie die het onmogelijk maakt dat een onbevoegde toegang krijgt tot informatie als gebruikers-instellingen, machine informatie en beeldgegevens die op de HDD zijn opgeslagen.

Bij het afdrukken of kopiëren wordt gescande data tijdelijk opgeslagen op de HDD en vervolgens geprint. Gebruikers maken ook diverse instellingen en voegen informatie toe, zoals scanbestemmingen en e-mailadressen die op het apparaat zijn opgeslagen. Deze informatie blijft op de vaste schijf totdat de gegevens zijn overschreven met andere gegevens, zelfs na het uitvoeren of verwijderen van de informatie door gebruikers. Er bestaat een kans dat de gegevens op de vaste schijf kunnen worden hersteld met behulp van hiervoor ontwikkelde gereedschappen en hulpprogramma's met datalekken als gevolg.

De functie HDD overschrijven-wissen is er op gericht om de op de harde schijf opgeslagen informatie te overschrijven met willekeurige betekenisloze data, zodat de werkelijke gegevens niet kunnen worden hersteld. Het proces van overschrijven wordt automatisch uitgevoerd, zodat de gebruiker of beheerder hier geen omkijken naar heeft. De HDD-gegevens worden direct overschreven, ook als de betreffende opdrachten tijdens het uitvoeren of op direct na het voltooien worden geannuleerd. Er zijn drie overschrijven-wissen methoden beschikbaar.

Dit zijn:

- Eenmalig overschrijven-wissen – Onnodige informatie wordt één keer overschreven met null-gegevens, waardoor de gegevens moeilijk kunnen worden hersteld.
- Drie-keer overschrijven-wissen – Onnodige informatie wordt tweemaal overschreven met willekeurige data en vervolgens eenmaal met null data. De drie-keer overschrijven-functie voorkomt de mogelijkheid om de data te

herstellen volledig, zelfs als u gebruik maakt van hoogwaardige restauratietechnieken. De drie-keer overschrijven-methode is strenger dan de eenmalige overschrijding methode. Bij overschrijving van bulkgegevens kan de methode met drie keer overschrijven, langer duren

- Het Amerikaanse ministerie van defensie DoD 5220.22-M (drie pass) – De DoD 5220.22-M drie-pass is de beveiligingsmodus van het hoogste niveau, in vergelijking met 'eenmalig overschrijven-wissen' en 'drie keer overschrijven-wissen'. Het vermindert het risico op informatielekkage aanzienlijk.

Taakopslag

Op de MFP kunnen gebruikersboxen, job boxen en / of faxboxen worden aangemaakt waarin ontvangen en geprinte gegevens opgeslagen kunnen worden. Toegang tot de opgeslagen gegevens in deze boxen kan op de volgende manieren worden beperkt:

Gebruikersbox

Gebruikers kunnen gebruikersboxen aanmaken om gegevens op de MFP op te slaan. Instellingen / beperkingen voor het gebruik, data bewaartermijn en wachtwoorden kunnen allemaal worden ingegeven voor deze boxen. Een gebruikersbox kan alleen worden geopend door een gebruiker die geregistreerd is als eigenaar voor deze box en kan dus niet door een onbevoegde gebruiker worden geopend. Een gedeelde box kan worden aangemaakt zodat gebruikers die niet geregistreerd zijn als eigenaar toegang hebben.

Na een termijn die door de beheerder is ingesteld, worden de opgeslagen documentgegevens automatisch gewist, zodat effectief HDD zelfbeheer en gegevensbeveiliging mogelijk is.

Job box

Gegevens voor privéafdrukken, snel kopiëren, proefafdrukken en opgeslagen opdrachten kunnen opgeslagen worden in een job box, die niet door gebruikers zelf kan worden gemaakt of verwijderd. De job box kan met PIN-code beveiligd zijn om de toegang tot de gegevens te controleren. De opgeslagen documentgegevens kunnen na een bepaalde tijd automatisch

worden gewist, waardoor effectieve HDD-zelfbeheer en gegevensbeveiliging mogelijk zijn.

Faxbox
Deze box ontvangt faxopdrachten. De per fax ontvangen gegevens kunnen worden weergegeven op het paneel van de MFP, zodat gewenste faxen direct kunnen worden afgedrukt, terwijl ongewenste faxen kunnen worden verwijderd.

9. De menselijke factor
KYOCERA probeert te voorkomen dat er geprint wordt waar printen niet nodig is. Ze willen mensen niet verhinderen te printen. Ze denken dat gebruikers soms, en niet allemaal, eraan herinnerd moeten worden dat papier, inkt en toner verspillen niet bijdraagt aan een economisch of milieuvriendelijk beleid.

Veel IT-managers zijn het er over eens dat een goede informatievoorziening en bewustwording betreffende kostenbesparing de ideale manier is om een printbeleid te laten slagen. Toch zie je dat er een sterke verschuiving is naar beleid afdwingen en automatisering. Goede print management software maakt het namelijk mogelijk om direct met de kostenbesparing ook een printbeveiligingsbeleid in te voeren en de efficiëntie voor de organisatie te verbeteren.

10. Bedieningspaneel
De gedeeltelijke vergrendelingsfunctie maakt het mogelijk bepaalde functies uit te schakelen en beschikt over drie niveaus: gebruik van het bedieningspaneel, taakbeheer / uitvoering en papierinstellingen. De bedieningspaneel vergrendeling biedt de mogelijkheid om de toegang tot de systeeminstellingen en de annuleringsinstellingen te blokkeren

Gebruik een verificatiemethode
KYOCERA-machines ondersteunen een aantal verschillende manieren om gebruikers zich te laten aanmelden. Toegang is mogelijk op drie niveaus – gebruiker, beheerder en machinebeheerder. De beveiligingsniveaus kunnen alleen door de machinebeheerder worden aangepast. Gebruikers die niet inloggen op de machine kunnen de beperkte functies van de machine gebruiken.

Lokale authenticatie
Authentiseert gebruikers op basis van de gebruikersgegevens die zijn geregistreerd in de lokale gebruikerslijst in de MFP / printer. Alleen geregistreerde gebruikers krijgen toegang tot de machine.

Netwerkauthenticatie
Authenticatie via een domeincontroller. NTLM- en Kerberosmethoden worden ondersteund. Een wachtwoordbeleid kan worden ingevoerd om wachtwoordcomplexiteit en wachtwoordleeftijd te handhaven, samen met de registratie van mislukte pogingen.

Gastfunctie
Wanneer de gebruiker login is ingeschakeld, kan een gastmodus worden toegevoegd zodat alleen bepaalde functies van de machine kunnen worden geopend zonder dat authenticatie vereist is. Dit kan ook gebruikt worden om de bedrijfskosten te verminderen, bijvoorbeeld door het kopiëren in kleur alleen beschikbaar te stellen voor gebruikers die inloggen. Dit beveiligingsniveau kan de organisatie tegen informatie lekken beschermen, terwijl de gebruiksvriendelijkheid behouden blijft.

Veilige afdrukken
Secure Print is een functionaliteit voor MFP's / printers en kan gebruikt worden voor het afdrukken van bedrijfsvertrouwelijke of persoonlijke documenten zonder dat er geprinte documenten onbeheerd op de machine achterblijven.

Privé-afdrukken
Met privéafdruk wordt een printopdracht vastgehouden op de MFP / printer totdat door de gebruiker het juiste wachtwoord is ingevoerd via het bedieningspaneel van de machine. Deze functie vereist dat de gebruiker een toegangscode instelt in de driver welke dan ook weer gebruikt wordt om de opdracht vrij te geven. Nadat het afdrukken is voltooid, worden de gegevens gewist. Als de machine wordt uitgezet voordat het document is geprint worden de gegevens eveneens gewist.

Kennispartner

KYOCERA Document Solutions Nederland streeft naar 100% klanttevredenheid door het leveren van betrouwbare, professionele document- en informatiemanagementsystemen. Het bedrijf voert daarnaast een uitgebreid portfolio zwart-wit en kleurenprinters en multifunctionals.

De filosofie is dat economie en ecologie hand in hand gaan. KYOCERA Document Solutions Nederland maakt zich sterk voor de bescherming van het milieu, gaat zuinig om met natuurlijke hulpbronnen en streeft er als bedrijf naar een voorbeeldfunctie te vervullen op het gebied van maatschappelijk verantwoord ondernemen.

KYOCERA Document Solutions - Beechavenue 25 | 1119 RA Schiphol-Rijk
T +31 (0)20 587 7200 | kyoceradocumentsolutions.nl

ICT informatiecentrum

Dit boek is een uitgave van het ICT informatiecentrum. Met meer dan 200.000 gebruikers is het ICT informatiecentrum sinds 2001 het grootste zelfstandige en onafhankelijke informatieplatform voor bedrijven en overheden in Nederland en België over de selectie, implementatie en toepassing van ICT oplossingen.

Met de publicatie van gratis beschikbare online informatie, boeken, whitepapers, informatiepakketten, nieuws, checklists en andere media beoogt het ICT informatiecentrum een bijdrage te leveren aan goede beslissingsprocessen rondom investeringen in hard- en software en de toepassing ervan in de praktijk.

Het ICT informatiecentrum is onafhankelijk in de samenstelling van publicaties. Deze staan altijd onder eigen redactie en komen tot stand in samenwerking met onafhankelijke ICT redacteuren en externe kennispartners. Indien kennispartners verbonden zijn aan leveranciers van commerciële ICT producten of diensten, dan wordt hiervan altijd melding gemaakt, zodat in alle gevallen duidelijk is vanuit welk belang een publicatie tot stand is gekomen.

Kijk voor alle (gratis) kennis en informatie over bedrijfssoftware en andere ICT thema's op ICTinformatiecentrum.nl