KYOCERA DOCUMENT SOLUTIONS NEDERLAND WAT IS DE AVG?

KYOCERA
Document Solutions

INHOUD

AVG – MANAGEMENTSAMENVATTING

De nieuwe Algemene Verordening Gegevensbescherming (Internationaal GDPR – General Data Protection Regulation) is de grootste ontwikkeling op het gebied van gegevensbescherming in de afgelopen 20 jaar. Organisaties in de hele wereld zullen met deze wet te maken krijgen. De AVG betreft de bescherming van persoonsgegevens van of met betrekking tot inwoners van de EU, die kunnen leiden tot directe of indirecte identificatie. De regelgeving is van toepassing op alle inwoners van de EU en houdt niet op bij de Europese grenzen. Ook organisaties buiten Europa die gegevens opslaan en/of verwerken, moeten zich aan deze wet houden.

Vanwege het grote geografische toepassingsgebied van de AVG hebben bedrijven tot 25 mei 2018 de tijd om de noodzakelijke maatregelen te nemen zodat zij aan de nieuwe regelgeving voldoen. Wanneer zij dit niet doen, kunnen ze een boete van maximaal € 20 miljoen of 4% van de jaaromzet (het hoogste bedrag is van toepassing) opgelegd krijgen bij inbreuk in verband met persoonsgegevens.

Niet alleen is het van belang dat bedrijven op de hoogte zijn van deze wijziging en dat zij hun strategie bepalen, maar mogelijk houdt de oplossing voor een deel in dat zij een document-/contentmanagementsysteem moeten implementeren. Bij versleuteling van de harde schijven van onder andere pc's, servers, netwerken en printers zal de impact na een datalek in verband met persoonsgegevens waarschijnlijk minimaal zijn. Met dergelijke tools zijn functies met betrekking tot de verwerking van persoonsgegevens geautomatiseerd. U kunt hierbij denken aan identificatie, classificatie, bewaking, tracering en -heel belangrijk- de vereiste bewaartermijnen conform de richtlijnen en tijdlijnen van de AVG.

Organisaties mogen niet langer wachten. Zij moeten als ze dat al niet hebben gedaan- direct hun bestaande processen, beleid en apparatuur onder de loep nemen en de implementatie van de nieuwe wijzigingen conform de AVG-richtlijnen en -tijdlijnen plannen.

De Europese Commissie werkt nauw samen met de autoriteiten voor persoonsgegevens van de lidstaten (zie grond 20 [1*]), in Nederland, de Autoriteit Persoonsgegevens (AP), https://autoriteitpersoonsgegevens.nl/, ten behoeve van een uniforme toepassing van de nieuwe regels. Ook zal de Europese Commissie burgers informeren over hun rechten en bedrijven over hun plichten.

[1*] Grond 20 stelt: "20) Het feit dat gegevens worden verwerkt door een persoon die is gevestigd in een land buiten de EU, mag de bescherming van personen als bepaald in deze verordening niet in de weg staan; in een dergelijk geval valt de verwerking onder de wet van de lidstaat waar de gebruikte middelen zich bevinden, en moet gewaarborgd worden dat de rechten en verplichtingen waarin de onderhavige verordening voorziet, in de praktijk worden nageleefd". (Bron: AVG)

INLEIDING GEGEVENSBESCHERMING IN NEDERLAND EN DE EU

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 basis-administraties 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 (Wbp)** is de Nederlandse uitwerking van de **Europese richtlijn bescherming persoonsgegevens (95/46/EG)**. De Wbp is sinds 1 september 2001 van kracht.

Belangrijkste bepalingen 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**:

- Kennisgeving: betrokkenen moeten ervan op de hoogte worden gesteld als hun gegevens worden verzameld;
- Doel: gegevens mogen alleen worden gebruikt voor het vermelde doel en niet voor andere doelen;
- Toestemming: gegevens mogen niet bekend worden gemaakt zonder de toestemming van de betrokkene;
- Beveiliging: verzamelde gegevens moeten veilig worden bewaard en mogen niet misbruikt kunnen worden;
- Openbaarmaking: betrokkenen moeten worden geïnformeerd over wie hun gegevens verzamelt;
- Toegang: betrokkenen moeten toegang krijgen tot hun gegevens en in staat worden gesteld om eventuele onjuiste gegevens te corrigeren; en
- 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.

De Algemene Verordening Gegevensbescherming (AVG) (officieel Verordening (EU) 2016/679)

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 (Wbp) in Nederland.). Aanvullende nationale wetgeving is niet nodig. De AVG wordt op **25 mei 2018** van kracht in heel Europa. Onderstaande afbeelding geeft een overzicht van de wetgeving inzake gegevensbescherming in de loop der jaren.

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); en
- Versleuteling van netwerken, bijvoorbeeld via netwerkversleuteling met hoge snelheid zoals VPN’s.

AVG - EEN OVERZICHT VAN NALEVING/ REGELGEVING

Het oorspronkelijke Europese kader voor de Databeschermingsrichtlijn (Richtlijn 95/46/EG) bestond sinds oktober 1995. Door de ontwikkelingen op IT-gebied, zoals internet, sociale media, online bankieren, diensten/oplossingen in de cloud, zijn enkele tekortkomingen van deze oude richtlijn aan het licht gekomen. Dit heeft ertoe geleid dat op 27 april 2016 de nieuwe Europese Verordening persoonsgegevens (EU) 2016/679 van het Europees Parlement de oude richtlijn heeft vervangen. Deze Verordening staat beter bekend als de Algemene Verordening Gegevensbescherming (AVG) of General Data Protection Regulation (GDPR). Het primaire doel van deze Verordening is om de stroom van persoonsgegevens en de daarbij behorende regelgeving in de 38 Lidstaten van de EU in goede banen te leiden.
In deze sectie van het document worden de belangrijkste effecten en wijzigingen in het kader van de AVG besproken (zie http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=NL).
In deze sectie wordt ook meer informatiegegeven over tools en technologie, zoals documentbeheer en daaraan gekoppelde systemen/oplossingen, versleuteling en de relatie en het onderlinge verband met de AVG.

De belangrijkste punten van de AVG en wijzigingen ten opzichte van de Europese Databeschermingsrichtlijn zijn:

- Verordening in plaats van richtlijn: de nieuwe Europese Verordening persoonsgegevens
  - (EU) 2016/679 van het Europees Parlement/General Data Protection Regulation (GDPR)
  - is wetgeving. Dit betekent dat in alle 28 Lidstaten van de EU dezelfde wet wordt aangenomen en van kracht is. Er zijn dus geen lokale 'kopieën/interpretaties' per Europese Lidstaat (wat wel het geval is bij een richtlijn).
- Aanzienlijk hogere boetes: bedrijven kunnen nu boetes tot maximaal € 20 miljoen of 4% van de jaaromzet krijgen als ze de wet inzake persoonsgegevens overtreden. De hoogte van de boete is afhankelijk van de ernst of herhaling van een overtreding.
- Dit wordt bepaald door de toezichthoudende autoriteit van het desbetreffende land. Naast de boetes kunnen zijn ook de volgende sancties mogelijk:
  - Verplichte auditrechten van de desbetreffende autoriteit persoonsgegevens; en
  - Sommatie tot nakoming. Meer informatie hierover wordt in de loop der tijd verstrekt door het Information Commissioners Office (ICO).

Sancties in Nederland: Bestuursdwang en last onder dwangsom
Bij het niet naleven van wettelijke verplichtingen kan de AP (Autoriteit Persoonsgegevens) besluiten om gebruik te maken van de Bevoegdheid (artikel 65 Wbp) een last onder bestuursdwang of een last onder dwangsom op te leggen. Deze mogelijkheid bestaat op grond van artikel 5:20, eerste lid, van de Algemene wet bestuursrecht (Awb) ook wanneer de AP medewerking vordert aan een door de AP ingesteld onderzoek maar deze medewerking niet wordt verleend.

In 2016 is 20 keer een procedure gestart om een last onder dwangsom op te leggen. Veelal nemen de onderzochte bedrijven en organisaties echter al maatregelen om de geconstateerde overtredingen te beëindigen voordat de AP daadwerkelijk een last onder dwangsom oplegt.

Bestuurlijke boete
Per 1 januari 2016 is de boetebevoegdheid van de AP uitgebreid. De toezichthouder kan nu organisaties die de Wbp overtreden een boete opleggen van maximaal € 820.000.
Als sprake is van een overtreding van de Wbp die opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid, kan de AP direct een boete opleggen. In andere gevallen gaat hier een bindende aanwijzing aan vooraf. De AP heeft in 2016 geen gebruik gemaaktt van de bevoegdheid om direct een boete op te leggen. Ook heeft de AP geen bindende aanwijzing opgelegd.

Sancties	2014	2015	2016
Bestuursdwang en last onder dwangsom	13	13	13
Boete	0	0	0
Incasso/invorderingsbeschikking	0	0	0

Bron: Autoriteit Persoonsgegevens I Bijlage Jaarverslag 2016

- Personen krijgen meer rechten: onder de AVG betekent dit bijvoorbeeld ondubbelzinnige toestemming om privégegevens te gebruiken, het recht op vergetelheid en het recht op overdraagbaarheid van gegevens.
- Betere definitie van toestemming: in het persbericht van het Europees Parlement worden de bepalingen van de AVG over duidelijke en bevestigende toestemming voor het verwerken van de privégegevens van de betreffende persoon benadrukt. Deze bepalingen geven consumenten meer controle over hun privégegevens. Hieronder valt bijvoorbeeld het aanvinken van een selectievakje bij bezoek aan een website of een andere verklaring of actie waaruit duidelijk blijkt dat de persoon akkoord gaat met de voorgestelde verwerking van de persoonsgegevens. Zwijgen, vooraf aangevinkte selectievakjes of inactiviteit zijn dus geen vorm van toestemming. Het moet voor de consument net zo eenvoudig zijn om de toestemming in te trekken als te geven. De nieuwe AVG maakt ook een einde aan de 'kleine lettertjes' in privacybeleid. De informatie moet nu in duidelijke taal worden verstrekt voordat de gegevens worden verzameld.
- Het recht op vergetelheid (grond 66) stelt:'Ter versterking van het recht op vergetelheid in de onlineomgeving dient het recht op wissing 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 verwerkingsver antwoordelijke 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.'
- Het recht op overdraagbaarheid van gegevens: personen hebben het recht op eenvoudigere mechanismen voor het overdragen van hun persoonsgegevens tussen providers, ook al zijn er vragen gerezen over de administratieve last die hierdoor bij de verwerkingsverantwoordelijken wordt gelegd. Artikel 20 van de AVG stelt:
  1. De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen, en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt, indien:
     a) de verwerking berust op toestemming uit hoofde van artikel 6, lid 1, punt a), of artikel 9, lid 2, punt a), of op een overeenkomst uit hoofde van artikel 6, lid 1, punt b); en
     b) de verwerking via geautomatiseerde procedés wordt verricht.
  2. Bij de uitoefening van zijn recht op gegevensoverdraagbaarheid uit hoofde van lid 1 heeft de betrokkene het recht dat de persoonsgegevens, indien dit technisch mogelijk is, rechtstreeks van de ene verwerkingsverantwoordelijke naar de andere worden doorgezonden.

TalkTalk

1) Telecombedrijf TalkTalk heeft een recordboete van £ 400.000 gekregen van het ICO omdat de beveiliging onvoldoende was. Een cyberaanvaller had 'eenvoudig' toegang had tot klantgegevens. Uit het uitgebreide onderzoek van het ICO bleek dat een aanval op het bedrijf in oktober 2015 voorkomen had kunnen worden als TalkTalk basismaatregelen had genomen om de informatie van klanten te beschermen. ICO-onderzoekers stelden vast dat de cyberaanval tussen 15 en 21 oktober profiteerde van technische kwetsbaarheden in de systemen van TalkTalk. De aanvaller had toegang tot de persoonsgegevens van 156.959 klanten, waaronder namen, adressen, geboortedata, telefoonnummers en e-mailadressen. Bij 15.656 klanten had de aanvaller ook toegang tot de bankgegevens en bankcodes. "Ondanks de kritiek uit sommige hoeken dat het bedrijf er goed vanaf is gekomen en dat onder de nieuwe Europese Verordening persoonsgegeven (AVG) het bedrijf een boete van £ 70 miljoen had kunnen krijgen [1]".

[1] http://www.decisionmarketing.co.uk/news/talktalk-could-have-faced-70m-fine-under-gdpr

1. De uitoefening van het in lid 1 van dit artikel bedoelde recht laat artikel 17 onverlet. Dat recht geldt niet voor de verwerking die noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend. Het in lid 1 bedoelde recht doet geen afbreuk aan de rechten en vrijheden van anderen.'

- Strengere naleving: verwerkingsverantwoordelijken en verwerkers moeten naleving van de AVG aantonen door dossiers nauwkeurig te verwerken. Directe aansprakelijkheid voor verwerkers en verwerkingsverantwoordelijken. Volgens de oude regelgeving hadden verwerkers van gegevens/informatie (zoals serviceproviders) geen verplichtingen. Onder de AVG zijn verwerkers direct verantwoordelijk voor het naleven van de 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 verkleind door implementatie van een contentmanagementsysteem (cms). Bijvoorbeeld informatie over wie de verwerker is? Wie is de verwerkingsverantwoordelijke? Welke gegevens worden verwerkt? Gegevenscategorieën? Gevoelige gegevens? Enzovoort. Deze informatie is vereist om te kunnen voldoen aan de strengere eisen die worden gesteld aan naleving.
- Directe en indirecte identificatoren: in tegenstelling tot de oude richtlijn is de AVG overduidelijk over de criteria die worden gebruikt voor het identificeren van personen. Deze criteria bevatten in het bijzonder criteria voor 'locatiegegevens' en 'een online identificator' (bijvoorbeeld Unique Identifiers (UID's) (zie de definitie van 'persoonsgegevens' in de woordenlijst).

- Verplichte melding van inbreuk: de AVG verplicht gegevensverwerkers om **inbreuken in verband met gegevens zonder onredelijke vertraging en, indien mogelijk, niet later dan 72 uur** na de kennisneming van de inbreuk te melden. Dergelijke inbreuken moeten worden gemeld bij de nationale autoriteit voor gegevensbescherming (de Autoriteit Persoonsgegevens (AP) in NL) 'Bij de beoordeling van de gegevensbeveiligings-risico's dient aandacht te worden besteed aan risico's die zich voordoen bij persoonsgegevensverwerking, zoals **de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot de door-gezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig, hetgeen met name tot lichamelijke, materiële of immateriële schade kan leiden.'** U bent vrijgesteld als het onwaarschijnlijk is dat de informatie persoonlijk letsel veroorzaakt of een hoog risico voor de persoon vormt. Inbreuk op versleutelde gegevens hoeft niet te worden gemeld.
- Toepassing buiten de EU/extraterritoriale toepassing: de richtlijn is van toepassing op alle organisaties, ongeacht de aanwezigheid in de EU. Als een organisaties handelt met/ goederen en services aanbiedt binnen de EU, moet de organisatie voldoen aan de AVG. De wetgeving is daarom van toepassing als u binnen de EU bent gevestigd; of services aan EU-inwoners biedt of het gedrag van de EU-inwoners volgt.
- Functionarissen voor gegevensbescherming: entiteiten die, op grote schaal en als onderdeel van de kerntaken, regelmatig en systematisch de betrokkenen monitort of gevoelige persoonsgegevens verwerkt moeten een functionaris voor gegevensbescherming aanwijzen. Bedrijven in het MKB (ondernemingen met maximaal 250 werknemers) zijn vrijgesteld indien gegevensverwerking niet onder de kern-activiteiten van het bedrijf valt. Een organisatie met minder dan 250 mensen in dienst, hoeft geen dossiers bij te houden (tenzij de organisatie persoonsgegevens verwerkt die zijn geclassificeerd als 'hoog risico').

De drie hoofdcriteria voor het aanwijzen van functionarissen voor gegevensbescherming (artikel 35) indien uw kernactiviteiten ínhouden:

- stelselmatige en grootschalige monitoring van personen;
- grootschalige verwerking van gevoelige gegevens;
- overheidsinstanties.

De exacte formulering van artikel 35 ter referentie:

"a) een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;

b) grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10; of
c) stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten."

De functie 'functionaris voor gegevensbescherming' kan een deeltijdfunctie zijn of worden gecombineerd met andere taken. Bij het invullen van de functie moet de functionaris wel rapporteren aan een onafhankelijke persoon (zoals de meeste nalevingsfunctionarissen), bevoegdheden krijgen en direct rapporteren aan het bestuur, zonder tussenpersonen.

Andere belangrijke AVG-wijzigingen zijn:

- Verzoek toegang tot gegevens: de wettelijke kosten van € 6,35 voor een toegangsverzoek worden afgeschaft, maar organisaties zullen een nieuwe bepaling invoeren die het de verwerkingsverantwoordelijke mogelijk maakt om in het geval van ongegronde of buitensporige verzoeken een redelijk bedrag in rekening te brengen of het verzoek af te wijzen. Dat wil zeggen dat de toezichthoudende autoriteit van het land waarschijnlijk boetes zal opleggen in plaats van wettelijke kosten voor verzoeken tot toegang tot gegevens in rekening te brengen.
- Onestopshop: het oorspronkelijke voorstel van de commissie voor een onestopshop-mechanisme werd zoals verwacht aanzienlijk afgezwakt. Momenteel hebben multinationals met meerdere vestigingen in Europa te maken met de toezichthoudende autoriteit van de Lidstaat waarin het bedrijf zijn 'hoofdvestiging' heeft. Er zijn echter omstandigheden waarin de leidende toezichthouder moet samenwerken met de autoriteit van andere betrokken Lidstaten.
- Gegevensbeschermingseffectbeoordelingen (artikel 35 van de AVG stelt dat gegevensbeschermingseffectbeoordelingen verplicht zijn voor organisaties met technologieën en processen die waarschijnlijk resulteren in een hoog risico voor de rechten van de betrokkenen. Zie https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/privacy-impact-assessment-pia).
- Ingangsdatum: de AVG wordt op 25 mei 2018 van kracht. Alle organisaties die de persoonsgegevens van EU-inwoners verwerken, moeten zich houden aan een aantal bepalingen. Doen zij dit niet, dan riskeren ze aanzienlijke boetes.

Voor meer informatie kunt u terecht op:
AVG-VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN VAN DE RAAD van 27 april 2016 -
http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=NL

AVG EN TECHNOLOGIE

Printers

De kantoorprinters van nu hebben een grote ontwikkeling doorgemaakt en zijn al lang niet meer de op zichzelf staande machines van toen. Tegenwoordig zijn printers en MFP's (multifunctionals - multifunctionele apparaten) intelligente netwerkapparaten met -net zoals een pc- een scherm, een toetsenbord, een harde schijf (waarop mogelijk gevoelige gegevens worden opgeslagen) en een besturingssysteem.

De toegenomen cybercriminaliteit die direct is gericht op netwerkapparatuur, zoals printers, vormt een zwakke schakel in de bescherming tegen diefstal van bedrijfsgegevens en kwaadaardige aanvallen. Van printers zijn kwetsbaarheden bekend die inbreuk op een zakelijk netwerk mogelijk maken.

De meeste ondernemingen denken er niet aan om hun printers te beveiligen. De printers kunnen dan ook worden geïnfecteerd met malware, waardoor het hele netwerk gevaar loopt. Om het nog complexer te maken wordt de regelgeving gewijzigd. Een van die wijzigingen is de AVG, die rampzalige financiële en juridische gevolgen kan hebben bij niet-naleving. Organisaties moeten onmiddellijk maatregelen nemen en MFP's opnemen in hun algemene strategie inzake gegevensbescherming.

In de AVG worden twee technologische kerngebieden genoemd die van belang zijn voor naleving van de regelgeving inzake persoonsgegevens:

- 1) Gegevensbeheer: het verzamelen, bewaren en vernietigen van gegevens (end-to-end-oplossing voor gegevensbeheer; en

- 2) Beveiliging/versleuteling van gegevens: het verwerken van en omgaan met gegevens, waaronder de versleuteling van gegevens. De AVG geeft helaas niet duidelijk aan welke technologie (zie grond 66, 67, 68, 71, 78, 81, 156, 168) en/of beveiliging (zie artikel 32) kan worden gebruikt. Er wordt alleen vermeld dat de 'passende' en 'moderne technische beveiligingsmaatregelen' moeten worden geïmplementeerd.

Mogelijk is dit met opzet vaag omschreven omdat de technologie zich blijft ontwikkelen. De gebruikte technologie moet dus mee-ontwikkelen. Het is mogelijk dat uiteindelijk de rechter bepaalt wat 'modern' is/was ten tijde van een mogelijke inbreuk.

Hoewel de vage regelgeving op dit gebied zich lastig laat interpreteren is, zijn wij bij KYOCERA van mening dat de implementatie van (een) technische oplossing(en) de naleving van de AVG eenvoudiger en efficiënter maakt ten opzichte van handmatige verwerking. Bovendien is het waarschijnlijk ook de meest rendabele optie als we de volgende AVG-vereisten in aanmerking nemen:

- juistheid van gegevens (zie artikel 5 - actuele gegevens),
- onmiddellijke toegang (zie artikel 15 - het vermogen van een bedrijf om te voldoen aan een verzoek tot inzage van een betrokkene), en
- het bewaren en wissen van gegevens (ook wel het recht op vergetelheid genoemd) (zie artikel 16 en 17).

Veel bedrijven weten niet waar ze moeten beginnen bij het classificeren van gegevens die mogelijk op een groot aantal IT-systemen zijn opgeslagen. Tegenwoordig zijn er veel geautomatiseerde technologieën voor gegevensclassificering en -verwerking beschikbaar, zoals de technologieën van KYOCERA. Deze kunnen een oplossing voor het gegevensbeheer zijn.

Versleuteling van gegevens is een belangrijke technologie voor gegevensbescherming als vermeld in de AVG. Artikel 32 noemt: "de pseudonimisering en versleuteling van persoonsgegevens; het vermogen om de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht te garanderen; het vermogen om gegevens na een incident te herstellen; en een proces voor het testen, beoordelen en evalueren van de doeltreffendheid van de beveiliging".

Uiteindelijk moet u als organisatie en in een rechtbank de maatregelen die u hebt genomen en de processen die u hebt ingesteld om AVG te implementeren, kunnen verdedigen. Op die manier beperkt u de aansprakelijkheid voor een boete. In andere woorden: heeft uw organisatie de relevante verantwoordelijkheden met betrekking tot gegevensbescherming geëvalueerd en op basis daarvan uw conclusie getrokken?

TOP 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 gegevensbescherming (artikel 35) indien uw kernactiviteiten ínhouden:

- stelselmatige en grootschalige monitoring van personen;
- grootschalige verwerking van gevoelige gegevens; of
- overheidsinstanties.

De functionaris hoeft niet voltijds in dienst van de organisatie te zijn. Deze functie kan indien nodig worden uitbesteed. Als een/uw 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 gegevensbescherming. 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 contentmanagemensysteem (ECM) en gebruik van een geschikt documentmanagementsysteem. Bijvoorbeeld informatie over wie de verwerker is? Wie is de

verwerkingsverantwoordelijke? 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 DOCUMENTMANAGEMENT-/CONTENTMANAGEMENTSYSTEEM 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/was ten tijde van een mogelijke inbreuk op gegevens.

Hoewel de vage regelgeving op dit gebied zich lastig laat interpreteren is, zijn wij bij KYOCERA van mening dat de implementatie van (een) technische oplossing(en) 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 contentmanagementsysteem 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.

WOORDENLIJST

Archiefsysteem - elke specifieke set persoonsgegevens die toegankelijk is volgens bepaalde criteria, of die kan worden opgevraagd
AVG / GDPR - De Algemene Verordening Gegevensbescherming (AVG) / General Data Protection Regulation (GDPR) (Regelgeving (EU) 2016/679) is een wet waarmee het Europees Parlement, de Europese Raad en de Europese Commissie gegevensbescherming voor personen binnen de Europese Unie (EU) willen verbeteren en uniform willen maken. De AVG/GDPR betreft de beveiliging van persoonsgegevens van of met betrekking tot inwoners van de EU
Betrokkene - een natuurlijke persoon wiens persoonsgegevens worden verwerkt door een verwerkingsverantwoordelijke of een verwerker
Functionaris gegevensbescherming - een expert op het gebied van gegevensprivacy die op onafhankelijke basis werkt om ervoor te zorgen dat een entiteit zich houdt aan het beleid en de procedures van de AVG
Gegevensverwerker - de entiteit die de gegevens namens de verwerkingsverantwoordelijke verwerkt
Gegevens wissen - ook het recht op vergetelheid genoemd. De betrokkene heeft het recht om de gegevensverwerker te vragen zijn/haar persoonsgegevens te wissen, te stoppen met verdere verspreiding van de gegevens en eventuele derde partijen te vragen om te stoppen met het verwerken van de gegevens
Inbreuk in verband met persoonsgegevens - een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, misbruik, enz. van persoonsgegevens
Onderneming/organisatie - elke entiteit die deelneemt aan economische activiteiten, ongeacht de juridische vorm, waaronder personen, partnerschappen, verenigingen, enz.
Ontvanger – een entiteit waaraan de persoonsgegevens worden verstrekt
Persoonsgegevens - ‘Alle informatie met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon’. Identificatie kan direct of indirect zijn, en bevat identificatoren zoals ‘een naam, identificatienummer, locatiegegevens, online-identiteit, een of meer factoren met betrekking tot de fysieke, psychologische, genetische, mentale, culturele of sociale identiteit van die persoon’ (zie artikel 4 [1]). Profileren maakt hier ook deel van uit, en hieronder valt ‘het beoordelen van de beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen van een persoon’ (zie AVG, artikel 4 [4]). In dit document kan ook met de term ‘persoonlijke informatie’ worden verwezen naar persoonsgegevens (zie onderstaand).
Persoonlijke informatie - informatie die afzonderlijk of samen met andere informatie kan worden gebruikt om een persoon te identificeren, contact met de persoon op te nemen of de persoon te vinden, of om een persoon op basis van context te identificeren
Privacy by design - een principe dat ervan uitgaat dat al bij het ontwerp van systemen aandacht wordt besteed aan gegevensbescherming, in plaats van het later toe te voegen

Privacy Impact Assessment - een tool voor het vaststellen en verlagen van de privacy-risico's van entiteiten door middel van analyse van de persoonsgegevens die worden verwerkt, en het geldende beleid inzake de bescherming van de gegevens
Pseudonimisering van gegevens - een procedure waarmee de meeste identificerende velden binnen een gegevensdossier worden vervangen door een of meer kunstmatige identificatoren of pseudoniemen. Er kan sprake zijn van een enkel pseudoniem voor een verzameling vervangen velden zijn of een pseudoniem per vervangen veld. (Bron - Wikipedia)
Recht op toegang - ook toegangsrecht voor betrokkene genoemd; de betrokkene heeft het recht om de persoonsgegevens te bekijken die de verwerkingsverantwoordelijke van hem of haar heeft
Recht op vergetelheid - ook het wissen van gegevens genoemd; de betrokkene heeft het recht om de gegevensverwerker te vragen zijn/haar persoonsgegevens te wissen, te stoppen met verdere verspreiding van de gegevens en eventuele derde partijen te vragen om te stoppen met het verwerken van de gegevens
Richtlijn - wetgeving waarin een doel wordt beschreven dat alle Europese-landen moeten bereiken aan de hand van hun eigen nationale wetten
Toegangsrecht voor betrokkene - ook recht op toegang genoemd; de betrokkene heeft het recht om de persoonsgegevens te bekijken die de verwerkingsverantwoordelijke van hem of haar heeft
Toestemming - elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;
Toezichthoudende autoriteit - een nationale instantie die de taak heeft om gegevens en privacy te beschermen, en de regelgevingen inzake persoonsgegevens binnen de Unie te monitoren. Voor Nederland is dit de Autoriteit Persoonsgegevens (AP) https://autoriteitpersoonsgegevens.nl, in overeenstemming met artikel 46.
Verordening - bindende wetgeving die in zijn geheel moet worden toegepast in de gehele Europese Unie.
Versleutelde gegevens - persoonsgegevens die worden beschermd met behulp van technologische maatregelen zodat de gegevens alleen toegankelijk/leesbaar zijn voor personen met de juiste bevoegdheden.
Vertegenwoordiger - elke persoon in de Unie die expliciet is aangewezen door de verwerkingsverantwoordelijke waarmee de toezichthoudende autoriteiten contact kunnen opnemen.
Verwerking - een bewerking met betrekking tot persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, gebruiken, registreren, enz.
Verwerkingsverantwoordelijke - de entiteit die het doel van, de voorwaarden van en de middelen voor de verwerking van persoonsgegevens vaststelt.

(Bron - EU GDPR-woordenlijst, tenzij anders aangegeven, bijv. Wikipedia)

KYOCERA Document Solutions Nederland
Beechavenue 25 | 1119 RA Schiphol-Rijk | Tel.: +31 (0)20 587 72 00
www.kyoceradocumentsolutions.nl | bps@dnl.kyocera.com

KYOCERA
Document Solutions