Persoonsgegevens van een overleden persoon vallen niet onder de AVG

Praktijkervaring leert ons dat er veel verwarring is over wat wel of niet onder persoonsgegevens wordt verstaan. De eerste gedachtegang is dat een overleden persoon onder de Algemene Verordening Gegevensbescherming (AVG) valt en dat zijn/haar persoonsgegevens middels de AVG beschermd moeten worden.

De AVG zegt hierover het volgende: *"een persoonsgegeven is alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene)"* (Artikel 4, AVG). Onder een natuurlijk persoon wordt verstaan iemand die nog leeft, een overleden persoon valt niet onder een natuurlijk persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Gegevens van een overleden persoon of van een rechtspersoon vallen hier niet onder.

AP ontvangt bijna 21.000 datalekken in 2018

In 2018 zijn er 20.881 datalekken gemeld bij de Autoriteit Persoonsgegevens (AP). Het aantal meldingen is meer dan verdubbeld ten opzichte van 2017. De meeste datalekken werden gemeld door organisaties uit de sectoren zorg en welzijn, openbaar bestuur en financiële dienstverlening. Het aantal meldingen overstijgt het eerder geschatte aantal fors. De AP breidt daarom haar capaciteit uit om meer actie te kunnen ondernemen. Deze acties kunnen leiden tot meer handhavende maatregelen.

In ruim tweederde (63%) van de datalekken die in 2018 zijn gemeld, gaat het om persoonsgegevens die aan een verkeerde ontvanger zijn gestuurd. De overige 37% bestaat uit onder meer kwijtgeraakte persoonsgegevens door bijvoorbeeld een verloren of gestolen laptop of usb-stick, hacking, phishing of malware. Het gaat in de meeste gevallen om NAW-gegevens,

DPIA – Data Protection Impact Assessment

Wat is een Data Protection Impact Assessment (DPIA) precies? Wanneer is een DPIA verplicht? Wanneer moet ik een DPIA uitvoeren? Dit zijn vragen die leven bij veel ondernemers. In dit artikel trachten wij hieromtrent duidelijkheid te scheppen.

Wat is een Data Protection Impact Assessment (DPIA)?
Onder de Algemene Verordening Gegevensbescherming (AVG) kunnen organisaties verplicht zijn een DPIA, in het Nederlands een ‘gegevensbeschermingseffectbeoordeling’ genoemd, uit te voeren. Dit is een instrument om vooraf de privacy risico’s van een gegevensverwerking in kaart te brengen. Op basis hiervan kunnen maatregelen worden getroffen om deze risico’s te verkleinen.

Wanneer moet een organisatie een DPIA uitvoeren?
De AVG geeft aan dat u als organisatie in ieder geval een DPIA moet uitvoeren, als uw organisatie:

gegevens over geslacht, medische gegevens en BSN.

Phishing

Uit de meldingen valt op dat datalekken door hacking en phishing met name voorkomen in de zorg. Bij phishing kan het gaan om nep e-mails die afkomstig lijken van een betrouwbare partij. Wanneer op de link wordt geklikt of een bijlage wordt geopend kan een virus, bijvoorbeeld ransomware, worden geïnstalleerd. Dit is een type malware dat gegevens versleutelt en ervoor zorgt dat deze niet meer toegankelijk zijn.

Sectoren met de meeste meldingen

In 2018 kwamen de meeste meldingen van datalekken van organisaties uit de volgende sectoren:

- gezondheid en welzijn 29%
- financiële dienstverlening 26%
- openbaar bestuur 17%

Acties 2018

De AP heeft een palet aan verschillende instrumenten om actie mee te ondernemen. In 2018 heeft de AP in veel gevallen uitleg

- systematisch en uitgebreid persoonlijke aspecten evalueert gebaseerd op geautomatiseerde verwerking, waaronder profilering, en daarop besluiten baseert die gevolgen hebben voor mensen;
- op grote schaal bijzondere persoonsgegevens verwerkt of strafrechtelijke gegevens verwerkt;
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

De verplichting om een DPIA uit te voeren geldt alleen voor nieuwe verwerkingen. Dit geldt dus voor verwerkingen die na 25 mei 2018 zijn gestart, omdat vanaf dat moment de AVG van toepassing is. Een DPIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacy risico oplevert voor de mensen van wie de organisatie gegevens verwerkt. Als organisatie hoeft u geen DPIA uit te voeren voor bestaande verwerkingsactiviteiten, tenzij een bestaande verwerking of het risico van deze verwerking veranderd, dan kan een DPIA alsnog verplicht zijn.

gegeven aan organisaties over te nemen beveiligingsmaatregelen, heeft de AP gevraagd om aanvullende informatie over het datalek, zijn brieven met normuitleg verstuurd en normoverdragende gesprekken gevoerd met organisaties.

In 2018 heeft de AP bij 298 datalekmeldingen actie ondernomen richting organisaties die een datalek gemeld hebben. Een deel van deze interventies loopt nog. Over het algemeen leidden deze acties tot een waarschuwing en beëindiging van de overtreding. Hieronder vielen ook interventies naar mogelijke datalekken bij organisaties die dit níet hebben gemeld bij de AP. Het komende jaar gaat de AP daar meer aandacht aan besteden.

In november 2018 heeft de AP vervoersdienst Uber een boete van 600.000 euro opgelegd voor het te laat melden van een datalek. Het ging om het te laat melden aan zowel de AP als aan de betrokkenen.

Meldplicht datalekken onder de AVG

Een bestaande gegevensverwerking kan bijvoorbeeld veranderen als uw organisatie een nieuwe technologie gaat gebruiken of wanneer u als organisatie de persoonsgegevens van een verwerking voor een ander doel gaat gebruiken dan waarvoor het voorheen werd verzameld. In deze situaties moet u, net als bij een nieuwe gegevensverwerking, vaststellen of de gewijzigde verwerking een waarschijnlijk hoog privacy risico oplevert. Wanneer dit het geval is, bent u alsnog verplicht om een DPIA uit te voeren.

Indien uw organisatie nieuwe verwerkingsactiviteiten gaat uitvoeren kunt u het beste in een zo vroeg mogelijk stadium de DPIA betrekken bij de ontwikkeling. Er kan dan namelijk vanaf het begin van het project/de activiteit rekening gehouden worden met de privacy risico’s. Ondanks dat de privacy risico’s na een uitgevoerde DPIA in kaart zijn gebracht is het belangrijk continu te controleren of de risico’s wijzigen en of de DPIA derhalve moet worden aangepast.

Vanaf 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). De meldplicht datalekken is onder de AVG grotendeels hetzelfde gebleven als in de jaren daarvoor. De AVG stelt wel strengere eisen aan de registratie van datalekken. Een organisatie moet voortaan alle datalekken documenteren en niet meer alleen de gemelde datalekken. Daarnaast zijn de boetes vanaf 25 mei hoger.

Vanaf 25 mei 2018 geldt de meldplicht datalekken in alle EU-landen. In Nederland geldt deze meldplicht al sinds 1 januari 2016.

Bron: Autoriteit Persoonsgegevens