Swalef
pensioenjuristen | academie

Nieuwsbericht

Datum: 28 september 2018
Van: Swalef pensioenjuristen en academie

Onderwerp: **De Algemene verordening gegevensbescherming en de pensioensector**

Inleiding

De Algemene verordening gegevensbescherming (hierna ook: AVG) is op 25 mei 2018 in werking getreden. Sinds 25 mei 2018 dient de hele Europese Unie te voldoen aan dezelfde privacywetgeving. Wij schreven er hier, op 8 februari 2018 al een nieuwsbericht over en in dit nieuwsbericht bekijken we wat de 'status' nu is en hoe de praktijk ermee omgaat. Maar eerst nog kort: wat regelt de AVG precies?

Begripsduiding

Persoonsgegevens = Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon

Verwerking = Een bewerking van persoonsgegevens zoals verzamelen, ordenen, gebruiken, doorzenden

Verwerkingsverantwoordelijke = Een (rechts)persoon, die het doel van de middelen voor de verwerking van persoonsgegevens vaststelt

Verwerker = Een (rechts)persoon, die ten behoeve de verwerkingsverantwoordelijke persoonsgegevens verwerkt

Wat regelt de AVG en toepassing pensioensector

Algemeen
De AVG regelt in algemene zin welke regels in acht moeten worden genomen bij het verwerken van persoonsgegevens door o.a. rechtspersonen.

Ook pensioenuitvoerders verwerken persoonsgegevens en moeten zich (dus) houden aan de AVG-voorschriften. Pensioenuitvoerders verwerken bijvoorbeeld persoonsgegevens van deelnemers als leeftijd, salaris, pensioengrondslag en parttime percentage.

Verantwoording
Inhoudelijk regelt de AVG het verwerken van persoonsgegevens. Met name op het gebied van *accountability* (verantwoordingsplicht) brengt de AVG vernieuwing. De AVG en de Uitvoeringswet AVG stellen algemene regels voor het verwerken van persoonsgegevens. Er zijn geen specifieke regels voor pensioenuitvoerders voor het verwerken van persoonsgegevens, zij zullen zich dan ook moeten houden aan het volledige spectrum van de AVG en de Uitvoeringswet AVG.

Pensioengerechtigden meer privacyrechten
Aanspraak- en pensioengerechtigden krijgen door de AVG meer en verbeterde privacyrechten. Pensioenuitvoerders zijn verplicht om hen te informeren over de verwerking van hun persoonsgegevens en ook op de website van de pensioenuitvoerder moet een zogenaamd privacy statement worden opgenomen. Hierin moet worden opgenomen hoe met persoonsgegevens wordt omgegaan.

Functionaris gegevensbescherming
De AVG noemt een aantal gevallen op grond waarvan het verplicht is een functionaris voor de gegevensbescherming (FG) aan te stellen. Zo is een FG *verplicht* als de verwerkingsverantwoordelijke of de verwerker *hoofdzakelijk* is belast met *grootschalige verwerking* van *bijzondere categorieën* van gegevens. De begrippen *hoofdzakelijk*, *grootschalig* en *bijzondere categorieën*[1] moeten in samenhang gelezen worden. Bij pensioenfondsen is er doorgaans geen sprake van hoofdzakelijk grootschalige verwerkingen van bijzondere categorieën van gegevens, zodat dan naar de letter van de AVG genomen de aanstelling van een FG niet verplicht is. De Pensioenfederatie raadt in haar Guidance pensioenfondsen en uitvoeringsorganisaties aan om een uitvoerige analyse te maken of een FG *verplicht* aangesteld moet worden.

Een FG kan ook *onverplicht* aangesteld worden. De in de AVG opgenomen voorwaarden voor aanwijzing, positie en taken van een FG gelden zowel bij een verplicht als vrijwillig aangewezen FG.

De werkzaamheden van de FG bestaan onder andere uit:

- Het informeren en adviseren over verplichtingen ten aanzien van het beschermen van gegevens
- Het toezien op naleving van de AVG of andere regels/beleid ten aanzien van de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het betrokken personeel en de betreffende audits
- Het samenwerken met en als contactpersoon dienen voor de Autoriteit Persoonsgegevens (AP)

Privacy Impact Assessment (PIA)
Een PIA moet gedaan worden om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. Voor verwerkingen die een *hoog risico* inhouden voor de rechten en vrijheden van natuurlijke personen moet een PIA worden uitgevoerd, om vervolgens maatregelen te kunnen nemen om risico's af te wenden of te verkleinen.
De werkgroep van Europese privacytoezichthouders (de zogenaamde Working Party 29) heeft in richtlijn Working Party 248 rev.01 negen criteria opgesteld om te toetsen of een PIA uitgevoerd moet worden. Wordt er aan ten minste twee van deze criteria voldaan dan is een PIA verplicht. Alle criteria kunnen voor pensioenuitvoerders van belang zijn.

Verwerkingsregister
Ook moeten pensioenuitvoerders een verwerkingsregister bij gaan houden, waarin staat welke verwerking met welke persoonsgegevens van toepassing is, wie dat doet, op basis van wat en ook het doel van de verwerking moet duidelijk zijn.

Verwerkersovereenkomst
Als een pensioenuitvoerder als verwerkingsverantwoordelijke gebruik maakt van een externe verwerker moet deze een verwerkersovereenkomst opstellen. Met een verwerkersovereenkomst sluit de pensioenuitvoerder uit dat de andere partij de persoonsgegevens voor eigen doelen mag verwerken. Een pensioenuitvoerder mag alleen verwerkers inschakelen die voldoende garanties bieden dat zij aan de wettelijke vereisten

[1] Onder bijzondere categorieën wordt verstaan: ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid

voldoen. Uiteraard geldt dat als de gegevensverwerking door een verwerker wordt uitgevoerd de pensioenuitvoerder nog steeds verantwoordelijk is voor de naleving van de AVG.

Belangrijk is om als pensioenuitvoerder het eigen beveiliging op orde te hebben, maar ook om de verwerkers hierop te attenderen mochten zij dit niet zo geregeld hebben. Neem daarom verschillende beveiligingsmaatregelen op in de verwerkersovereenkomst.

Nieuwe begrippen
Begrippen die ook samen met de AVG zijn geïntroduceerd zijn '*privacy by design*' (de bij de verwerking gehanteerde mechanismen en systemen zijn zo ontworpen dat zoveel als mogelijk rekening wordt gehouden met de privacy van de deelnemers en de AVG) en '*privacy by default*' (het zodanig instellen van standaardinstellingen dat de privacy zoveel als mogelijk wordt gewaarborgd).

Informatie
Een pensioenuitvoerder moet, zoals reeds vermeld, aan de betrokkene van wie de persoonsgegevens worden verwerkt duidelijk maken dat de persoonsgegevens verwerkt worden. Daartoe moet de pensioenuitvoeder bepaalde informatie mededelen.

Deze informatie moet in een 'beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm' gegoten zijn.

Toezichthouder
De Nederlandse toezichthouder voor de AVG - en andere gegevensbeschermings- en privacywetgeving - is de AP. Op de website van de AP is veel informatie te vinden over de implementatie.

Boete
De bevoegdheid van toezichthouders om administratieve geldboetes op te leggen bij inbreuk op de AVG is bedoeld ter afschrikking. De sancties moeten onder EU-recht namelijk doeltreffend, evenredig én afschrikkend zijn. De hoogte van de boete is maximaal € 20.000.000,00 of 4% van de (wereldwijde) omzet.

Servicedocumenten Pensioenfederatie
In april 2017 heeft de Pensioenfederatie het 'Servicedocument Gegevensbescherming' gepubliceerd en in september 2017 de 'Guidance Verwerking Persoonsgegevens'. Pensioenuitvoerders zullen stappen moeten zetten in het *privacyproof* maken van persoonsgegevensbestanden (in onder andere IT-systemen).

Handleiding Rijksoverheid
De Rijksoverheid heeft ook een handleiding gepubliceerd. In die handleiding zijn de belangrijkste bepalingen uit de verordening en uit de Nederlandse Uitvoeringswet Algemene verordening gegevensbescherming toegelicht.