ravc ©

SPRENKELS & VERSCHUREN
ACTUARISSEN CONSULTANTS

Nieuwsflits Nieuwe Privacywetgeving:

Top 10 meest gestelde vragen: deel 2 van 3

Om u als pensioenfondsbestuurder te ondersteunen bij de implementatie van de nieuwe privacywetgeving (AVG) zullen wij in een reeks van drie Nieuwsflitsen antwoorden geven op de meest gestelde vragen aan de bestuurstafel, die wij in de praktijk horen. Hierbij treft u onze tweede Nieuwsflits aan. Op 26 april 2018 zullen wij een interactieve sessie organiseren voor pensioenfondsbestuurders om de ervaringen met de implementatie van de AVG met elkaar te delen. Deel 1 van deze editie was vorige maand.

1. Komt er nog een Code AVG vanuit de Pensioenfederatie?

Volgens onze informatie is de Pensioenfederatie voornemens om in het derde kwartaal van dit jaar *een Gedragscode Verwerking Persoonsgegevens Pensioenfondsen* te publiceren. Dit vergt nog nader overleg met de Autoriteit Persoonsgegevens (AP). Het onderschrijven en daadwerkelijk toepassen van deze gedragscode is een belangrijk element om aan te tonen, dat een pensioenfonds (als verwerkingsverantwoordelijke) voldoet aan de AVG-verplichtingen.

2. Moeten wij ook met onze adviseurs een verwerkersovereenkomst sluiten?

Ja, zodra u met uw adviseurs (actuaris, accountant, bestuursadviseur, etc.) persoonsgegevens uitwisselt, dan dient u als verwerkingsverantwoordelijke met de rechtspersoon voor wie zij werken een verwerkersovereenkomst af te spreken. Hiervan is al sprake als een adviseur (bijvoorbeeld voor de uitvoering van de Wft) een kopie van een paspoort van u als bestuurder bewaart.

3. Onder welke voorwaarden mag ik aan profilering (‘profiling’) doen?

Profilering (‘profiling’) is een speciale vorm van gegevensverwerking: een geautomatiseerde verwerking van persoonsgegevens, waarbij een bepaald beeld wordt gevormd over de persoonlijke aspecten van iemand. Er wordt dan een profiel opgesteld. Aan de hand van dat profiel worden vervolgens voorspellingen gedaan, analyses gedaan of informatie verstrekt. Profilering en geautomatiseerde besluitvorming kunnen nuttig zijn voor pensioenfondsen en betrokkenen. Pensioenfondsen kunnen profilering bijvoorbeeld gebruiken om doelgroepgericht te communiceren. Profilering kan ook gebruikt worden om bijvoorbeeld de risicohouding vast te stellen of om premies en/of voorzieningen nauwkeuriger vast te stellen. Profilering wordt door de AVG niet verboden. Als een pensioenfonds dit goed vastlegt in de AVG-documenten, dan is profileren door pensioenfondsen mogelijk:

1. **Op grond van de wet: *toegestaan***
   Voor profilering moet net als bij andere verwerkingen van persoonsgegevens een rechtsgrond bestaan. Profilering is echter niet noodzakelijk voor de uitvoering van een pensioenregeling. Profilering door pensioenfondsen kan echter wel plaatsvinden op basis van de wet. Aan actieve deelnemers moet bijvoorbeeld in UPO’s op grond van de wet andere informatie worden verstrekt dan aan gewezen deelnemers. En aan gewezen deelnemers weer andere informatie dan aan pensioengerechtigden. Voor deze vorm van profilering verandert er niets. Deze profilering wordt gebaseerd op de wet en blijft gewoon toegestaan.

2. **Op grond van gerechtvaardigde belangen: *toegestaan, mits het pensioenfonds kan onderbouwen dat het een voldoende gerechtvaardigd belang heeft***
   De Pensioenwet geeft aan pensioenfondsen de opdracht om bij de communicatie te bevorderen dat persoonlijke informatie aansluit bij de informatiebehoefte en kenmerken van de (gewezen) deelnemer, gewezen partner en pensioengerechtigde. Ook dienen pensioenfondsen op grond van de wet bijvoorbeeld hun voorzieningen, premies en risicohouding zo nauwkeurig mogelijk vast te stellen. Voor zover een pensioenfondsen kan aantonen dat het een gerechtvaardigd belang heeft bij profilering, is profilering ook toegestaan.
   Wel eist de AVG dat de betrokkenen hierover actief worden geïnformeerd. Deze informatie moet duidelijk zijn en specifiek aandacht geven aan profilering, met daarbij toegelicht de onderliggende logica en het belang en de verwachte gevolgen voor de betrokkenen.

De betrokkenen kunnen bezwaar maken tegen deze profilering en eisen dat deze wordt stopgezet als de belangen, rechten en vrijheden van de betrokkenen zwaarder wegen dan de belangen die het pensioenfonds heeft bij profilering. Er moet dan bij de betreffende betrokkene(n) wel sprake zijn van bezwaren die te maken hebben met de specifieke omstandigheden van de betrokkene. Dus algemene principiële bezwaren tegen profileren zijn onvoldoende om dit te kunnen stopzetten. Naar onze mening geeft dit aan pensioenfondsen voldoende mogelijkheden tot profilering. Als dit overigens voor marketingdoelen wordt gebruikt, kan de betrokkene de profilering wel altijd via het indienen van bezwaren stopzetten. De verplichte informatieverstrekking over profilering kan bij een separate informatiebrief plaatsvinden, maar kan ook als apart onderdeel in de privacyverklaring (op de website) en het privacybeleid worden opgenomen.

3. **Op grond van toestemming betrokkene:**
   Als de profilering niet op basis van de wet of een voldoende gerechtvaardigd belang kan plaatsvinden, moet het pensioenfonds hiervoor uitdrukkelijk om toestemming vragen. In dat geval kan de betrokkene de profilering altijd stopzetten door de toestemming in te trekken.

NB: Voor één bepaalde vorm van profilering geldt wel een wettelijk verbod, namelijk als op basis van profilering automatische besluitvorming plaatsvindt, geheel zonder menselijke tussenkomst, en hieraan individuele rechtsgevolgen verbonden zijn voor de betrokkenen of het automatische besluit de betrokkenen op andere wijze aanmerkelijk treft. Dat speelt bijvoorbeeld als op basis van profilering bij een sollicitatieprocedure bepaald wordt met wie wel of geen sollicitatiegesprekken gevoerd worden. Bij pensioenfondsen zal er niet snel sprake zijn van deze verboden vorm van profilering.

4. Op welk onderdeel wijkt S&V af van de Guidance van de Pensioenfederatie?

In deel 7 van onze RiskTransparant *'Hoe implementeert u als pensioenfonds de AVG?'* hebben wij de rol van de werkgever bij de uitvoering van de pensioenregeling beschreven, omdat deze rol in de 'Guidance' van de Pensioenfederatie tot nu toe onderbelicht is gebleven. Zoals bekend verplicht de AVG elke verwerkingsverantwoordelijke tot het sluiten van een verwerkers-overeenkomst met een verwerker of tot het treffen van een andere bindende rechtshandeling wanneer zij met elkaar persoonsgegevens delen. Dit is vastgelegd in artikel 28 lid 3 AVG. Tussen twee verwerkingsverantwoordelijken, die samen het doel en de middelen voor de verwerking bepalen, moeten de verantwoordelijkheden onderling op transparante wijze worden vastgelegd. Dit is bepaald in artikel 26 lid 1 AVG.

Wanneer een werkgever persoonsgegevens van zijn werknemers aanlevert bij een pensioenfonds geldt onverkort de AVG. Als een werkgever samen met een pensioenfonds doel en middelen voor de verwerking vaststelt, moeten zij onderling de verantwoordelijkheden vastleggen. De manier waarop is niet voorgeschreven. In het geval een pensioenfonds persoonsgegevens verwerkt ten dienste van een werkgever dus zonder dat het pensioenfonds doel en middelen (mede) vaststelt, is er in beginsel een verwerkersovereenkomst of een andere bindende rechtshandeling vereist. Het is daarom van belang voor de pensioenpraktijk, dat er duidelijkheid komt over de rol van de werkgever bij de uitvoering van een pensioenregeling. Zolang dit niet het geval is, zal elk fonds zelf moeten beoordelen welke rol de werkgever heeft onder de AVG en op basis daarvan de verwerkingsafspraken moeten vastleggen.

5. Hoe kan een pensioenfonds verwerkingsafspraken met een werkgever vormgeven?

Afhankelijk van de vraag hoe het fonds de rol van de werkgever ziet, kan dit op verschillende manieren gebeuren. Bij een niet-verplichte deelname aan een pensioenfonds (OPF, APF of BPF) kunnen de verwerkingsafspraken (gebaseerd op artikel 28 lid 3, dan wel op artikel 26 lid1 AVG) worden opgenomen in de uitvoeringsovereenkomst (bijvoorbeeld in een aparte bijlage). Bij een verplichtgesteld pensioenfonds (BPF of beroepspensioenfonds) is dat niet mogelijk. In dat geval kunnen de verwerkingsafspraken bijvoorbeeld worden opgenomen in het uitvoeringsreglement.

6. Wat is een gegevensbeschermingseffectbeoordeling?

Een gegevensbeschermingseffectbeoordeling wordt ook wel een ‘data privacy impact analyse’ (DPIA) of kortweg een ‘PIA’ genoemd. Een PIA is een proces dat is bedoeld om de verwerking van persoonsgegevens te beschrijven, de noodzaak en evenredigheid van de verwerking te beoordelen en de daaraan verbonden privacy risico's te helpen beheren door deze risico's in te schatten en maatregelen te bepalen om ze aan te pakken. Daarmee is het een proces voor het verwezenlijken en aantonen van de naleving van de AVG.

De PIA bestaat ten minste uit de volgende onderdelen:

- een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoelen, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkings-verantwoordelijke worden behartigd;
- een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doelen;
- een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen; en
- de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.
- De PIA is niet verplicht voor elke verwerking. Een PIA is alleen verplicht als een verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Deze "rechten en vrijheden" hebben voornamelijk betrekking op de rechten op gegevensbescherming en privacy, maar kunnen ook andere grondrechten betreffen, zoals vrijheid van meningsuiting, discriminatieverbod en vrijheid van geweten en godsdienst.

Een verwerkingsverantwoordelijke moet telkens beoordelen of de risico’s die door de verwerkings-activiteiten ontstaan mogelijk een hoog risico inhouden. Dat betekent dat de beoordeling moet worden uitgevoerd bij het aangaan van nieuwe verwerkingsactiviteiten. Het is ook raadzaam om deze beoordeling periodiek bij bestaande activiteiten uit te voeren om vast te stellen om zich geen veranderingen hebben voorgedaan.

Een PIA is ten minste verplicht, indien een organisatie:

- systematisch en uitvoerig persoonlijke gegevens evalueert, waaronder profilering;
- op grote schaal bijzondere persoonsgegevens verwerkt;
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied.

Er bestaat een aanvullende lijst met criteria om te beoordelen of er sprake is van een hoog privacy risico. Als vuistregel kan gehanteerd worden, dat als een verwerking aan twee hiervan voldoet een PIA moet worden uitgevoerd:

- geautomatiseerde beslissingen die voor betrokkenen wezenlijke (rechts)gevolgen kunnen hebben;
- grootschalige gegevensverwerkingen (hoeveelheid, verscheidenheid, geografische reikwijdte);
- gekoppelde databases;
- gegevens over kwetsbare personen;
- gebruik van nieuwe technologieën;
- doorgifte van persoonsgegevens buiten de EU;
- gegevensverwerkingen die tot gevolg kunnen hebben, dat betrokkenen een recht niet kunnen uitoefenen, een dienst niet kunnen gebruiken of dat zij een contract niet kunnen afsluiten.

Wij adviseren daarom om met uw pensioenuitvoeringsorganisatie af te spreken, dat zij jaarlijks rapporteren of en, zo ja, welke aanpassingen er zijn geweest voor uw pensioenfonds. Dit kan de vorm krijgen van een jaarlijks privacy auditrapport.

7. Wat is de samenhang tussen privacybeleid en IT-beleid?

Privacybeleid hangt op twee onderdelen samen met het IT-beleid van een pensioenfonds:

1. als onderdeel van de inrichting van de IT-omgeving (organisatorisch en technisch);
2. als onderdeel van een specifiek onderdeel van het IT-beleid: het informatiebeveiligingsbeleid.

Bij het inrichten van een geautomatiseerd systeem moet het uitgangspunt zijn dat dit systeem zodanig wordt ingericht, dat bij de verwerking van persoonsgegevens zoveel mogelijk rekening wordt gehouden met de bescherming van de privacy van betrokkenen. Dit wordt 'privacy by design' genoemd. Een voorbeeld hiervan is het minimaliseren van gegevens van de betrokkene, bijvoorbeeld door alleen die gegevens te registreren, die echt noodzakelijk zijn voor de uitvoering van de pensioenregeling. Ook kan pseudonimisering of versleuteling van gegevens worden toegepast, zodat de gegevens niet meer kunnen direct worden herleid tot een natuurlijk persoon.

Daarnaast maakt privacy deel uit van het Informatiebeveiligingsbeleid van het fonds. Uit de PIA en de risicohouding van het fonds volgt doorgaans een indeling van soorten persoonsgegevens en de mate waarop deze beschermd moeten worden: de dataclassificatie. Deze dataclassificatie ziet toe op Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). Het Informatiebeveiligingsbeleid van het fonds moet dus aansluiten op de dataclassificatie, die uit de PIA volgt.

8. Wat is het verschil tussen een datalek en een beveiligingslek?

Er blijft onder de AVG verschil bestaan tussen een datalek en een beveiligingslek. Als er alleen sprake is van een zwakke plek in de beveiliging, waarbij (nog) geen inbreuk is gemaakt in verband met persoonsgegevens (dus nog geen verlies of onrechtmatige verwerking), dan spreken we van een beveiligingslek en niet van een datalek. Een beveiligingslek sec (dus zonder datalek) hoeft nooit gemeld te worden. Een mogelijk beveiligingslek kan wel oorzaak worden voor een datalek.

9. Zijn er verschillen in AVG-verplichtingen tussen soorten pensioenuitvoerders?

Ja, maar er zijn geen grote verschillen in AVG-verplichtingen tussen de diverse soorten pensioenuitvoerders. Een pensioenfonds (OPF, APF, BPF en beroepspensioenfonds) is tevens gehouden om bij een datalek, dat mogelijk een groot risico inhoudt voor de rechten en vrijheden van een betrokkene, dit te melden aan de betrokkene zelf. Een verzekeraar of PPI hoeft deze melding aan een betrokkene niet uit te voeren. Alle pensioenuitvoerders moeten datalekken sowieso melden aan de Autoriteit Persoonsgegevens (AP), tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de betrokkenen.

10. Moet ik mijn aansprakelijkheidsverzekering aanpassen als gevolg van de AVG?

Het moet niet, maar het is wel aan te raden om nog eens goed naar de voorwaarden van uw aansprakelijkheidsverzekering te kijken. Door de AVG neemt (in theorie) het claimrisico toe. Mogelijk is het verstandig om de dekking van deze verzekering uit te breiden. Let u er wel op, dat een aansprakelijkheidsverzekering geen dekking biedt tegen boetes van de AP. Daartegen kunt u zich dus niet verzekeren. Reden te meer om scherp te letten op de aansprakelijkheidsbepalingen in de verwerkersovereenkomsten met uw verwerkers. Voorkom dat u als pensioenfonds opdraait voor boetes voor schendingen van de nieuwe privacyvoorschriften, die door uw verwerkers (ten aanzien van de persoonsgegevens van uw fonds) worden gepleegd.

Deel uw AVG-ervaringen met elkaar!

Op 26 april 2018 van 14.00 tot 16.00 uur zullen wij op ons S&V-kantoor in Amsterdam een interactieve sessie organiseren voor pensioenfondsbestuurders om de ervaringen met de implementatie van de AVG met elkaar te delen.

U kunt zich opgeven via: secretariaat@sprenkelsenverschuren.nl

Meer weten over de AVG? Neem dan contact op met uw vaste contactpersoon!

Q & A *Wat horen wij aan de bestuurstafel?*