ravc ©

Nieuwsflits Nieuwe Privacywetgeving:

Top 10 meest gestelde vragen: deel 1 van 3

In onze RiskTransparant (deel 7) van eind 2017 hebben wij stilgestaan bij het wat én hoe van de nieuwe privacywetgeving (AVG). Wij hebben hierop veel reacties gehad. Om u als pensioenfondsbestuurder verder te ondersteunen bij dit dossier, 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 eerste Nieuwsflits aan. De volgende staat gepland voor volgende maand. 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.

1. Wij hebben nu toch ook al de Wbp? Wat is er nieuw aan de AVG?

De Wet bescherming persoonsgegevens (Wbp) vervalt zodra de AVG in werking treedt. Dit is per 25 mei 2018. Het bijzondere van de AVG is dat deze rechtstreeks werkt en er toe leidt dat overal in de Europese Unie dezelfde regelgeving gaat gelden. Nieuw is ook dat het pensioenfonds (actief) moet aantonen dat het voldoet aan de AVG. Dat kan bijvoorbeeld door:

a) opstellen van privacybeleid;
b) opstellen van verwerkingsregister;
c) zorgen voor sluitend systeem van verwerkersovereenkomsten;
d) opstellen van gegevensbeschermingseffectbeoordeling (Privacy Impact Assessment of PIA);
e) aanwijzen van een Functionaris Gegevensbescherming (FG);
f) opstellen van een privacyverklaring.

Als een pensioenfonds dit niet kan aantonen, is er sprake van een boetewaardige overtreding van de AVG. Daarnaast is het protocol voor het melden van datalekken aangescherpt.

2. Wat is de samenhang met het Integraal Risico Management (IRM)?

Binnen IRM kun je verschillende domeinen onderscheiden zoals bijvoorbeeld integriteit en IT. Privacy is ook zo'n domein. Het gaat dan specifiek om privacy risico's en de beheersing van datalekken. De IRM-aanpak biedt een goede kapstok voor het in kaart brengen van deze risico's, het vaststellen van risicohouding & risicobereidheid en het treffen van beheersingsmaatregelen. Het opstellen van een PIA past als instrument in deze aanpak. Onze tip hierbij is om geen nieuw proces op te starten, maar aansluiting te zoeken bij het huidige IRM-wegingsproces van risico's.

3. Wat zijn onze verantwoordelijkheden als pensioenfondsbestuur en wat zijn de verantwoordelijkheden van onze uitvoeringsorganisatie?

U bent en blijft als bestuur altijd verantwoordelijk. Onder de AVG is het pensioenfonds 'verwerkingsverantwoordelijke' (*data controller*). Uw uitvoeringsorganisatie treedt op als 'verwerker' (*data processor*) voor het pensioenfonds. Dit betekent dat de uitvoeringsorganisatie zich moet richten op het niveau van gegevensbeveiliging dat u als bestuur op basis van uw privacybeleid hebt vastgesteld. U dient derhalve uw eigen beleid te hebben en kunt niet (zomaar) afgaan op (het beleid van) uw uitvoeringsorganisatie.

4. **Onze uitvoeringsorganisatie levert alle AVG-documenten aan. Zijn wij dan AVG-proof?**
Nee, dat is zeker niet automatisch het geval! Uw uitvoeringsorganisatie heeft zoals in vraag 3 gezegd een eigen rol. Als verwerkingsverantwoordelijke moet u zelf het doel en de middelen van de gegevensverwerking vaststellen. Uw AVG-documenten moeten daarop aansluiten. Er zal dus een toetsing nodig zijn van de aangeleverde documenten op de AVG-verplichtingen voor u als verwerkingsverantwoordelijke en aan uw privacybeleid. Het dient ook te passen binnen uw uitbestedingsbeleid, communicatiebeleid en IRM-beleid. Daarbij dient u als fonds alle processen van gegevensverwerking in beeld te hebben; ook eventuele processen die niet via uw uitvoeringsorganisatie lopen. Te denken valt aan de persoonsgegevens die u deelt met uw vermogensbeheerder (zie vraag 6).

5. **Wij hebben dit jaar onze pensioenadministratie bij een andere uitvoeringsorganisatie ondergebracht (transitie). Moeten wij nog letten op bijzondere AVG-verplichtingen?**
Ja, denkt u met name aan de archivering van alle (oude) gegevens. Meestal is met de overgang ook het fysieke en/of digitale archief mee overgegaan naar de nieuwe uitvoeringsorganisatie. Of mogelijk is het archief bij een externe partij ondergebracht. Omdat ook het 'bewaren' van gegevens onder de werking van de AVG valt, dient het archief ook AVG-proof te zijn. De externe partij bij wie het archief is ondergebracht, treedt dan op als verwerker van het pensioenfonds. De nieuwe uitvoeringsorganisatie zal (in overleg met u) al maatregelen hebben getroffen. Als dit niet het geval is, dan is spoedige actie vereist. Let erop dat als de overgang (inclusief de overdracht van het archief) nog niet is afgerond op 25 mei 2018 uw oude uitvoeringsorganisatie ook nog optreedt als verwerker van het pensioenfonds.

6. **Moeten wij ook onze vermogensbeheerovereenkomst aanpassen?**
Ja, in principe wel. Sinds begin dit jaar is ook MIFID II (Markets In Financial Instruments Directive) van kracht geworden. Deze Europese regels schrijven onder meer voor dat vermogens-beheerders (telefoon)gesprekken van (professionele) cliënten moeten opnemen en bewaren inclusief elektronische communicatie, die verband houden met het ontvangen, doorgeven en uitvoeren van cliëntorders. Op basis van de AVG zullen vermogensbeheerders zich willen beperken zich tot de contactpersonen van het pensioenfonds. Daartoe worden dan gegevens van die personen bewaard. Hierover dienen in een verwerkersovereenkomst nadere afspraken te worden gemaakt. Het gaat dan om een expliciet doel. Uw beleggingscommissie of IRM commissie (afhankelijk hoe u dit heeft ingericht) zal in contact moeten treden met de vermogensbeheerder. Wij adviseren in dat geval om een verwerkersovereenkomst op te nemen als bijlage bij uw (bestaande) vermogensbeheerovereenkomst.

7. **Is de aanwijzing van een FG voor pensioenfondsen verplicht?**
Er geldt geen 'harde' verplichting tot aanwijzing van een FG voor pensioenfondsen. Dat moet elk pensioenfonds zelf beoordelen op basis van de criteria van de AVG. Een belangrijk criterium is of het fonds op grote schaal '*bijzondere persoonsgegevens*' verwerkt, zoals gegevens over de fysieke en geestelijke gezondheid. Bij de uitvoering van een arbeidsongeschiktheidspensioen of premievrije voortzetting bij invaliditeit kan hiervan sprake zijn. Het ligt daarom in de rede om een FG aan te wijzen. Aleid Wolfsen, de voorzitter van de Autoriteit Persoonsgegevens, acht het ook wenselijk dat pensioenfondsen een FG aanwijzen gelet op de grote hoeveelheid gevoelige gegevens die zij verwerken.

8. **Wat is het verschil tussen de FG en een Privacy Officer?**
De rol en de taken van de FG zijn specifiek omschreven in de AVG. Bij de uitvoering van deze taken geniet de FG bovendien wettelijke ontslagbescherming. Een Privacy Officer heeft geen wettelijke status. Uiteraard kunt u wel een Privacy Officer aanwijzen als FG. Het is ook mogelijk om een bestaande Privacy Officer op termijn als FG aan te wijzen, zodra de toepassing van de criteria van de AVG voor de pensioensector 100% duidelijk is. U dient zich voor uw besluit wel steeds te kunnen verantwoorden jegens de Autoriteit Persoonsgegevens.

9. **Wie mag persoonsgegevens opvragen? Mag een partner van de deelnemer dit ook (bijvoorbeeld bij echtscheiding)?**
Alleen de betrokkene (deelnemer, gewezen deelnemer of pensioengerechtigde) mag zijn eigen persoonsgegevens opvragen. Dit inzagerecht is verankerd in de AVG en is bovendien nodig om het recht op rectificatie, bezwaar en vergetelheid te kunnen effectueren. Een (ex) partner of kind van de (gewezen) deelnemer mag dus niet zonder toestemming of machtiging van de betrokkene zelf diens persoonsgegevens opvragen. Hiervoor dienen pensioenfondsen een protocol aan te houden. Wanneer de betrokkene overlijdt, dan geldt niet langer de bescherming van de AVG. Niettemin zal het protocol erin moeten voorzien de voor het nabestaandenpensioen relevante persoonsgegevens met de nabestaanden van de betrokkene te kunnen delen. Deze instructie zal duidelijk belegd moeten worden in de klantcontactafdelingen van uw uitvoerder.

10. **Hoe lang moet een pensioenfonds op grond van de AVG persoonsgegevens bewaren?**
De AVG schrijft geen concrete bewaartermijnen voor. Pensioenfondsen moeten als regel zelf bepalen hoe lang zij (categorieën van) persoonsgegevens bewaren. Daarbij moeten zij beoordelen hoe lang de gegevens nodig zijn voor het doel waarvoor deze zijn verzameld of worden gebruikt. Onder de AVG dienen zij zich jegens de Autoriteit Persoonsgegevens steeds te kunnen verantwoorden voor de gehanteerde bewaartermijn. Er bestaan wel bewaartermijnen voor specifieke persoonsgegevens op basis van fiscale wetgeving en het arbeidsrecht. Met inachtneming van deze termijnen is het van belang om voor elke verwerking van gegevens, die is te herleiden naar natuurlijke personen, vast te leggen hoe lang deze (categorieën van) gegevens worden bewaard en op basis van welk doel. De AVG gaat er vanuit dat de gegevens in ieder geval niet langer worden bewaard dan noodzakelijk is. Het pensioenfonds moet dit kunnen aantonen en daar dus beleid op maken.

Volgende nieuwsflits over de AVG is gepland eind maart 2018.

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.

Meer weten over de AVG? Neem dan contact op met uw vaste contactpersoon binnen Sprenkels & Verschuren of download onze RiskTransparant Deel 7 vanaf de site.