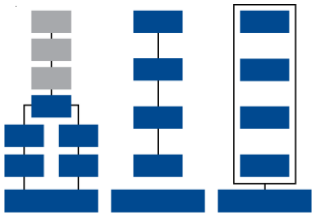
SPRENKELS & VERSCHUREN
ACTUARISSEN CONSULTANTS



RiskTransparant, deel 7

Hoe implementeert u als pensioenfonds de Algemene Verordening Gegevensbescherming (AVG)?

In deze editie van onze RiskTransparant besteden wij aandacht aan de Algemene Verordening Gegevensbescherming (AVG). De AVG gaat verder dan u wellicht op het eerste gezicht zou denken. Wij geven u graag inzicht hoe u de AVG kunt implementeren: het wat én hoe van deze nieuwe wetgeving.

1. Grootste wijziging privacywetgeving in 20 jaar

Per 25 mei 2018 wordt de Wet bescherming persoonsgegevens vervangen door de Algemene Verordening Gegevensbescherming (AVG). Dit is de grootste wijziging in de privacywetgeving in 20 jaar. De verordening zal gaan gelden in de gehele Europese Unie (EU) voor elke onderneming en instelling, die persoonsgegevens verwerkt van EU burgers, ongeacht of zij binnen of buiten de EU gevestigd zijn.

In het Engels wordt de AVG *'General Data Protection Regulation (GDPR)'* genoemd. Omdat binnen de EU steeds meer digitale uitwisseling van persoonsgegevens plaatsvindt, wordt de huidige wet- en regelgeving aangepast en de handhaving aangescherpt. In Nederland zal de Autoriteit Persoonsgegevens (AP) toezien op de handhaving. De AVG geldt ook voor pensioenfondsen. Pensioenfondsen krijgen dus naast DNB en AFM op het gebied van de privacy te maken met een nieuwe toezichthouder: AP.

2. Wat verandert er voor pensioenfondsen?

De AVG versterkt de privacy-rechten van alle EU burgers en daarmee ook van pensioen- en aanspraakgerechtigden evenals leden van besturen en organen van Nederlandse pensioenfondsen. Dit betekent concreet, dat elke betrokkene het recht verkrijgt om zijn persoonsgegevens op te vragen bij het fonds, te corrigeren of te verwijderen, het recht heeft om zijn persoonsgegevens elektronisch over te laten dragen (data portabiliteit) en het recht heeft om een klacht in te dienen bij de AP. De AVG schrijft voor pensioenfondsen de volgende verplichtingen voor:

1. Opstellen privacy beleid.
2. Opstellen verwerkingsregister.
3. Zorgdragen voor dekkend systeem verwerkersovereenkomsten.
4. Opstellen gegevensbeschermingseffectbeoordeling (DPIA).
5. Aanwijzen Functionaris Gegevensbescherming (FG).
6. Melding datalekken.
7. Naleving AVG.

Wij lichten deze AVG-verplichtingen hierna nader toe.

3. De AVG-verplichtingen nader toegelicht

Ad 1) Opstellen privacy beleid
Een pensioenfonds moet beleid opstellen waarbij de bescherming van persoonsgegevens centraal staat (*Data Security Policy*). Persoonsgegevens zijn alle gegevens over identificeerbare personen. Als identificeerbaar wordt beschouwd een persoon, die direct of indirect kan worden geïdentificeerd aan de hand van een 'identificator', zoals een naam, een BSN-nummer of één of meer andere elementen, die kenmerkend zijn voor de identiteit van die persoon. Een pensioenfonds moet ook een *privacyverklaring* opstellen, waarmee het fonds aantoont, dat het ook daadwerkelijk uitvoering geeft aan het privacy beleid.

Er moet een goed en gedegen proces worden doorlopen van opzet, bestaan en werking van het privacy beleid met aandacht voor passende organisatorische én technische maatregelen voor geautomatiseerde systemen. Hierbij gelden als principes *'privacy by design'* en *'privacy by default'.* '*Privacy by design'* houdt in, dat er al bij het ontwerpen van producten en diensten voor wordt gezorgd, dat persoonsgegevens niet kunnen worden teruggevoerd op identificeerbare personen. Dit kan bijvoorbeeld door het anonimiseren van gegevens. '*Privacy by default'* houdt in, dat technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat bij het inrichten van standaardinstellingen de privacy wordt beschermd (geen vooraf aangevinkte instellingen).

Persoonsgegevens moeten niet alleen snel opvraagbaar zijn voor betrokkenen, maar moeten ook rechtmatig worden verwerkt. Onder 'rechtmatige' verwerking wordt verstaan een verwerking, die plaatsvindt met toestemming van betrokkene of een verwerking die noodzakelijk is voor:

a. Het uitvoeren van een overeenkomst, waarbij de betrokkene zelf partij is.
b. Het voldoen aan een wettelijke verplichting.
c. Het beschermen van vitale belangen van betrokkene.
d. Het vervullen van een taak van algemeen belang.
e. Het behartigen van gerechtvaardigde belangen van de verwerkingsverantwoordelijke.

Bij een ondernemingspensioenfonds, een APF of een vrijwillig bedrijfstakpensioenfonds vindt de verwerking van persoonsgegevens van een deelnemer plaats, omdat dit noodzakelijk is voor de uitvoering van de pensioenovereenkomst (zie sub a), waarbij de betrokkene partij is (geweest). Bij een verplichtgesteld bedrijfstakpensioenfonds of beroepspensioenfonds is verwerking noodzakelijk op grond van het nakomen van een verplichting, die voortvloeit uit de pensioenwetgeving (zie sub b). Het verkrijgen van toestemming is in deze situaties dus niet aan de orde.

Verwerking van *bijzondere persoonsgegevens*, zoals medische gegevens, politieke en religieuze overtuiging of het lidmaatschap van een vakbond, is toegestaan als de betrokkene daarvoor uitdrukkelijk toestemming geeft of als de verwerking van deze gegevens noodzakelijk is met het oog op sociaal- of arbeidsrechtelijke verplichtingen. De uitvoering van een pensioenregeling voor arbeidsongeschikte deelnemers, zoals premievrijstelling (PVI) en toekenning van een arbeidsongeschiktheidspensioen (AOP) is terug te voeren op arbeidsrechtelijke verplichtingen, die voortvloeien uit de pensioenwetgeving. Ook bij de verwerking van *bijzondere persoonsgegevens* is het dus niet nodig om toestemming te verkrijgen van betrokkenen. Verwerking op basis van toestemming is ook minder geschikt voor collectieve verwerking, omdat dit altijd door een betrokkene kan worden ingetrokken. Alleen in het geval een pensioenfonds andere *bijzondere persoonsgegevens* zou verwerken, die niet nodig zijn voor de uitvoering van een pensioenregeling, zoals bijvoorbeeld het lidmaatschap van een vakbond, dan is uiteraard wél de uitdrukkelijke toestemming nodig van betrokkenen.

Direct bij de start van de gegevensverwerking moet een pensioenfonds aan deelnemers de volgende informatie verstrekken:

- Contactgegevens van het fonds en de Functionaris Gegevensbescherming (zie ook Ad 5).
- Rechtsgrond en doelstelling van de verwerking van persoonsgegevens.
- Ontvangers van de persoonsgegevens.
- Bewaartermijn van persoonsgegevens.
- Rechten van betrokkenen (recht op inzage, rectificatie, beperking, verwijdering, bezwaar, overdraagbaarheid, vergetelheid, recht om geen onderwerp van geautomatiseerde besluitvorming te zijn en het recht om een klacht in te dienen bij de AP).
- Grondslag van de verplichting om gegevens te verstrekken en wat de gevolgen zijn als de gegevens niet verstrekt worden.
- Informatie over automatische besluitvorming[1].

Deze informatieverstrekking kan onderdeel zijn van de *privacyverklaring*, die wordt opgenomen in het **Pensioen 1-2-3** op de website van het fonds. Dit veronderstelt dat deze informatie direct bij aanvang van deelname aan de pensioenregeling (= start gegevensverwerking) beschikbaar is.

Ad 2) Opstellen verwerkingsregister

Vanuit zijn verantwoordelijkheid voor de verwerking van persoonsgegevens moet een pensioenfonds een verwerkingsregister opstellen, als er sprake is van een hoog privacy risico[2]. Hiervan is bijvoorbeeld sprake bij grootschalige verwerking van *bijzondere* persoonsgegevens, zoals gegevens die verband houden met de fysieke of mentale gezondheid van natuurlijke personen (mate van arbeidsgeschiktheid). Een verwerkingsregister van een pensioenfonds moet de volgende informatie bevatten:

- Contactgegevens van het fonds en de Functionaris Gegevensbescherming (zie Ad 5).
- Verwerkingsdoelen.
- Categorie betrokkenen en categorieën persoonsgegevens.
- Categorieën van ontvangers.
- Beoogde bewaartermijnen, indien mogelijk.
- Algemene beschrijving van technische en organisatorische beveiligingsmaatregelen.

Het is mogelijk dat meerdere verwerkingsregisters (voor verschillende verwerkingsdoelen) naast elkaar moeten worden aangehouden. Daarnaast dient ook een pensioenuitvoeringsorganisatie als feitelijke verwerker van persoonsgegevens een eigen verwerkingsregister aan te houden.

Ad 3) Zorgdragen voor dekkend systeem verwerkersovereenkomsten

De AVG schrijft voor dat bij de uitvoering van een pensioenregeling sprake moet zijn van een sluitend systeem van verwerkersovereenkomsten[3] tussen een ‘verwerkingsverantwoordelijke’ (*data controller*) en een ‘verwerker’ van persoonsgegevens (*data processor*). Een ‘verwerker’ verwerkt persoonsgegevens voor de ‘verwerkingsverantwoordelijke’. Deze laatste is degene, die bevoegd is om het doel en de middelen voor de verwerking vast te stellen. In theorie zijn deze rollen (verwerkingsverantwoordelijke en verwerker) wel te onderscheiden, maar in de praktijk niet altijd te scheiden: een partij kan beide rollen vervullen.

Ook bij de uitvoering van een pensioenregeling kan daarvan sprake zijn. Een werkgever sluit immers een pensioenovereenkomst met een werknemer en vraagt daarvoor persoonsgegevens

[1] Inclusief ‘profiling’.
[2] Dit geldt altijd voor grote werkgevers met 250 of meer werknemers.
[3] Onder de Wet bescherming persoonsgegevens worden dit ‘bewerkersovereenkomsten’ genoemd.

uit bij de werknemer. Voor de uitvoering van deze pensioenovereenkomst sluit de werkgever een uitvoeringsovereenkomst met een pensioenuitvoerder, zoals een ondernemings-pensioenfonds[4]. Daartoe meldt de werkgever de werknemer aan bij het fonds en verstrekt de werkgever de voor de uitvoering noodzakelijke gegevens. In die situatie is de werkgever aan te merken als verwerkingsverantwoordelijke en het fonds als verwerker. Mogelijk verloopt de aanmelding via een derde partij: een administratie- of accountantskantoor. Dan is ook deze derde in principe aan te merken als een verwerker. Wordt er gebruik gemaakt van een digitale applicatie, die wordt beheerd door een derde partij (met inzagerechten), dan is deze derde partij eveneens aan te merken als een verwerker. In dat geval dient zowel tussen de werkgever en de pensioenuitvoerder als tussen de werkgever en genoemde derde partijen een verwerkersovereenkomsten te worden gesloten.

Een pensioenfonds heeft de administratie van de pensioenregeling meestal uitbesteed aan een pensioenuitvoeringsorganisatie, waardoor de via de werkgever ontvangen persoonsgegevens nogmaals worden doorgegeven. In die relatie is het pensioenfonds aan te merken als verwerkingsverantwoordelijke en de pensioenuitvoeringsorganisatie als verwerker. Deze laatste kan op zijn beurt onderdelen van de pensioenadministratie waarbij persoonsgegevens worden verwerkt, zoals bijvoorbeeld het opstellen van UPO's, hebben uitbesteed aan 'subcontractors'. Dan is de pensioenuitvoeringsorganisatie aan te merken als verwerkingsverantwoordelijke en de 'subcontractor' als verwerker. Ook dan dient zowel tussen het pensioenfonds en de pensioenuitvoeringsorganisatie als tussen de pensioenuitvoeringsorganisatie en de 'subcontractor' een verwerkersovereenkomst te worden gesloten. Daarbij moet er voor worden gewaakt, dat de contractuele verplichtingen van de 'subcontractor' jegens de pensioenuitvoeringsorganisatie (met name de technische en organisatorische beschermings-maatregelen) niet afwijken van de contractuele verplichtingen van de uitvoeringsorganisatie jegens het pensioenfonds.

De AVG verplicht verwerkers tot het sluiten van een verwerkersovereenkomst met een bepaalde (minimale) inhoud. Een verwerkingsverantwoordelijke is verantwoordelijk voor het afsluiten van deze overeenkomst. Dit betekent, dat in elke relatie tussen partijen, waarbij persoonsgegevens worden uitgewisseld ten behoeve van de uitvoering van een pensioenregeling een verwerkersovereenkomst moet worden gesloten. Dat is alleen anders, als de uitvoering plaatsvindt op basis van een wettelijk voorschrift. Dit is bijvoorbeeld het geval bij een verplicht gesteld bedrijfstakpensioenfonds of beroepspensioenfonds. In die situatie is verwerking noodzakelijk op grond van een wettelijke verplichting en hoeft de werkgever geen verwerkersovereenkomst te sluiten met het fonds.

Ad 4) Opstellen gegevensbeschermingseffectbeoordeling (DPIA)

Bij een hoog privacy risico moet de verwerking van persoonsgegevens worden beoordeeld met behulp van een 'gegevensbeschermingseffectbeoordeling' (*'data privacy impact assessment; DPIA'*)[5]. Dit is een instrument om vooraf de privacy risico's van de gegevensverwerking in kaart te brengen om vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een *DPIA* is ook voorgeschreven bij '*profiling'*, ofwel bij het samenstellen van profielen bijvoorbeeld ten behoeve van het communiceren met doelgroepen.

[4] Bij onderbrenging bij een verplicht bedrijfstakpensioenfonds wordt geen uitvoeringsovereenkomst gesloten.
[5] Geldt altijd voor grote werkgevers met 250 of meer werknemers.

Voor een pensioenfonds moet een gegevensbeschermingseffectbeoordeling (*DPIA*) ten minste de volgende onderdelen bevatten:

- Systematische beschrijving beoogde verwerkingen en verwerkingsdoelen.
- Beoordeling noodzaak en evenredigheid van de verwerkingen.
- Beoordeling rechten en risico's en vrijheden betrokkenen, gelet op aard, omvang, context en doeleinden verwerking.
- Beoogde maatregelen om risico's aan te pakken.

Als uit een gegevensbeschermingseffectbeoordeling een hoog privacy risico blijkt dat niet met redelijke maatregelen kan worden beperkt, moet vooraf (voor de eerste verwerking) met de AP worden overlegd.

Ad 5) Aanwijzen Functionaris Gegevensbescherming (FG)
Het aanwijzen van een Functionaris Gegevensbescherming (*Data Protection Officer*) is onder meer verplicht bij de grootschalige verwerking van *bijzondere* persoonsgegevens, zoals gegevens over gezondheid en bij '*profiling'*. Bij pensioenfondsen zal hiervan al snel sprake kunnen zijn. Volgens de AP doen pensioenfondsen er daarom verstandig aan om een Functionaris Gegevensbescherming (FG) aan te wijzen, die intern toeziet op integrale naleving van de AVG.

Aan de aanwijzing zelf zijn geen voorwaarden verbonden, behalve dat de FG gemakkelijk toegankelijk moet zijn voor het fonds, de betrokkenen en de AP. Een pensioenfonds kan samen met de uitvoeringsorganisatie een FG aanstellen. Er mag ook een lid van het bestuur of van het intern toezicht worden aangewezen. De functie mag ook extern belegd worden. Eerder hebben wij gemeld, dat hier ook een rol kan liggen voor de '*Risk- en compliance officer'* van het pensioenfonds[6]. Het is zelfs mogelijk gebruik te maken van iemand, die deze rol voor meerdere pensioenfondsen tegelijk op zich neemt.

Wij krijgen in de praktijk vragen over het verschil tussen een FG en een 'privacy officer'. Het verschil zit vooral in het feit, dat een FG niet ontslagen kan worden bij de uitvoering van zijn taken onder de AVG. Dit is niet (wettelijk) geregeld voor een privacy officer[7].

Ad 6) Melding datalekken
De meldplicht voor datalekken blijft onder de AVG gehandhaafd. Een pensioenfonds moet als verwerkingsverantwoordelijke elke ongeoorloofde verwerking van persoonsgegevens melden bij de AP binnen 72 uur nadat deze er kennis van heeft genomen, tenzij niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van betrokkene(n). In de praktijk zal een pensioenfonds deze melding pas kunnen doen, nadat de pensioenuitvoeringsorganisatie als verwerker de melding aan het pensioenfonds heeft gedaan. De AVG bepaalt hierover, dat een verwerker de verwerkingsverantwoordelijke moet informeren 'zonder onredelijke vertraging', zodra hij kennis heeft genomen van een inbreuk.

De AVG stelt daarbij strengere eisen aan de eigen registratie van de datalekken. Elk datalek moet worden gedocumenteerd. Met deze documentatie moet de AP kunnen controleren of aan de meldplicht is voldaan. Dit gaat verder dan de huidige protocolplicht uit de Wbp, die alleen betrekking heeft op de gemelde datalekken. Bij een hoog risico moet de inbreuk worden gemeld bij de betrokkene(n).

[6] Zie RiskTransparant, Deel 5: Compliancy.
[7] Zie artikel 38 lid 3 AVG en paragraaf 3.4 van de Guidelines on DPO's.

Ad 7) Naleving AVG
Bij overtreding van de AVG kunnen boetes worden opgelegd van maximaal € 20 miljoen of tot maximaal 4% van de totale premielast per jaar. Het is dus zaak de AVG-verplichtingen tijdig en correct na te komen.

4. Implementatie begint bij bewustwording

Zoals gezegd vormt de AVG na 20 jaar de grootste verandering in de privacywetgeving. Als bestuur van een pensioenfonds kunt u nu alvast stappen ondernemen om op 25 mei 2018 klaar te zijn voor de AVG. Om u hierbij te helpen, heeft de AP op de website een stappenplan opgenomen[8]. De eerste stap is bewustwording. Bestuur en beleidsbepalers bij pensioenfondsen moeten op de hoogte zijn van de nieuwe regelgeving. Zij moeten kunnen inschatten wat de impact van de AVG is op hun processen en diensten en welke aanpassingen nodig zijn om aan de AVG te voldoen.

Aangezien de datum van 25 mei 2018 snel nadert is het belangrijk om snel te handelen. Wij zetten daarom de acties, voor u als pensioenfonds, op een rij in onderstaand stappenplan:

Stappenplan naleving AVG

Stap	Actie	Toelichting	Deadline
0	Bepalen risicohouding en risicobereidheid (nulmeting).	Na in kaart brengen van huidige verwerking van persoonsgegevens (ketenanalyse aan de hand van vragen: Welke data wordt verwerkt? Van wie? Door wie (extern)? Waarom? Rechtsgrond?) bepaalt bestuur risicohouding en risicobereidheid met oog op opstellen en uitvoeren van privacy beleid.	**Ultimo 2017**
1	Opstellen privacy beleid.	Aandacht voor 'privacy by default' en 'privacy by design'. Onderdeel van beleid kan zijn opstellen van een privacy verklaring en protocol melding datalekken.	**Januari 2018**
2	Opstellen verwerkingsregister.	Inhoud: • Contactgegevens fonds. • Contactgegevens FG. • Verwerkingsdoelen. • Categorieën betrokkenen, persoonsgegevens en ontvangers. • Bewaartermijnen. • Technische en organisatorische beveiligingsmaatregelen.	**Januari 2018**
3	Zorgdragen voor dekkend systeem van verwerkersovereenkomsten.	Opstellen nieuwe overeenkomsten of wijzigen bestaande (bewerkers)overeenkomsten tussen verwerkingsverant-woordelijken en verwerkers.	**Februari 2018**
4	Opstellen gegevensbeschermings-effectbeoordeling (DPIA).	Inhoud: • Systematische beschrijving beoogde verwerkingen en verwerkingsdoelen. • Beoordeling noodzaak en evenredigheid verwerkingen. • Beoordeling rechten en risico's en vrijheden betrokkenen, gelet op aard, omvang, context en doelen verwerking. • Beoogde maatregelen om risico's aan te pakken.	**Februari 2018**
5	Aanwijzen FG.	Mag samen met pensioenuitvoeringsorganisatie en/of extern worden belegd.	**April 2018**
6	Aanpassen systemen en procedures.	Volgt uit privacy beleid.	**Mei 2018**
7	Naleving AVG	Mogelijkheid toepassen Code Verwerking Persoonsgegevens Pensioenfondsen'[9]	**Mei 2018**

[8] Zie: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/in_10_stappen_voorbereid_op_de_avg.pdf
[9] De Pensioenfederatie heeft aangekondigd pensioenfondsen te helpen om de AVG na te leven middels het opstellen van een *'Gedragscode Verwerking Persoonsgegevens Pensioenfondsen'.* Pensioenfondsen die deze gedragscode onderschrijven en naleven houden zich dan aantoonbaar aan de AVG. Deze code is thans nog niet beschikbaar.

Heeft u de AVG al geagendeerd en welke acties heeft u uitgezet? 25 mei 2018 is al heel snel en dit is niet het enige dossier op uw bureau….

Bij het uitvoeren van dit stappenplan helpen wij graag. Wij beschikken daartoe over de vereiste expertise op alle relevante gebieden: IT, Riskmanagement en de juridische voorschriften.

Meer informatie óf meer kennis delen?

Download:

- *RiskTransparant deel 1: Het IT dossier is een must voor elke bestuurder, uitgave mei 2016*
- *RiskTransparant deel 2: Welke waarde heeft een ISAE voor het bestuur: in control of een illusie van control, uitgave juni 2016*
- *RiskTransparant deel 3: Wat is uw risico identiteit? Bent u al een integrale bestuurder? uitgave september 2016*
- *RiskTransparant deel 4: Wat is uw risicohouding en risicobereidheid op het gebied van beleggingsbeleid? uitgave oktober 2016*
- *RiskTransparant deel 5: Wat is uw compliance bereidheid? uitgave februari 2017*
- *RiskTransparant deel 6: Wat is het bestaansrecht van ons fonds? Uitgave juni 2017*
- *S&V Reflector, "….op basis van een gestructureerde aanpak komen tot een doelmatig en uitlegbaar integraal risicomanagement bij pensioenfondsen….". Praktische handvatten voor borging van risicomanagement binnen uw fonds, uitgave november 2016*

Bekijk ook onze andere artikelen op http://www.sprenkelsenverschuren.nl of neem contact op met uw vaste contactpersoon bij Sprenkels & Verschuren.

Over Sprenkels & Verschuren

Wij zijn onafhankelijke adviseurs. Wij geven wij niet alleen advies, maar wij implementeren ook. Wij zijn denkers én doeners, die kennis graag in co-creatie ontwikkelen. Waarom? Omdat elk antwoord een vraag is geweest én geen enkele vraag hetzelfde is.