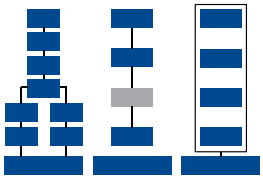
SPRENKELS & VERSCHUREN
ACTUARISSEN CONSULTANTS



ravc ©

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 vertellen u graag hoe u de AVG kunt implementeren: het wat én hoe van deze nieuwe wetgeving.

1. Grootste wijziging in 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. Dit is volgens de EU noodzakelijk voor het vertrouwen dat nodig is om de digitale economie verder te kunnen laten ontwikkelen.

De AVG geldt ook voor werkgevers en pensioenfondsen. In Nederland zal de Autoriteit Persoonsgegevens (AP) toezien op de handhaving.

2. Wat verandert er voor pensioenfondsen?

De AVG versterkt de privacy-rechten van alle EU-burgers en daarmee ook van pensioen- en aanspraakgerechtigden evenals van leden van besturen en organen van pensioenfondsen in Nederland. Elke betrokkene krijgt het recht om zijn persoonsgegevens op te vragen bij het fonds, te corrigeren of te laten verwijderen, het recht om zijn persoonsgegevens elektronisch over te laten dragen (data portabiliteit) en het recht om een klacht in te dienen bij de AP. Uit de AVG volgen voor pensioenfondsen de volgende verplichtingen:

1. Opstellen privacy beleid
2. Opstellen verwerkingsregister
3. Zorgen voor sluitend 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 op basis waarvan natuurlijke personen zouden kunnen worden geïdentificeerd aan de hand van een unieke 'identificator', zoals een naam of een BSN-nummer (direct) of door één of meer andere persoonselementen te combineren en deze combinatie van elementen kenmerkend is voor de identiteit van die persoon (indirect). In het kader van het privacy beleid zijn pensioenfondsen weliswaar niet verplicht om een *privacyverklaring* te hebben, maar het is in de digitale wereld vrijwel ondenkbaar dat een pensioenfonds zonder privacyverklaring aan de wettelijke verplichtingen zal kunnen voldoen.

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 zoveel mogelijk rekening wordt gehouden met de privacy en de eisen uit de AVG. Dit kan bijvoorbeeld door het anonimiseren, pseudonimiseren en versleutelen van gegevens. '*Privacy by default'* houdt in, dat technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat bij keuzemogelijkheden de standaardinstellingen (*default*) zo gekozen worden, dat de privacy het meest gewaarborgd is.

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 en een vrijwillig bedrijfstakpensioenfonds vindt de verwerking van persoonsgegevens van een deelnemer plaats, omdat dit noodzakelijk is voor de uitvoering van een 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 of religieuze overtuiging of het lidmaatschap van een vakbond, is in de AVG met extra waarborgen omkleed. Dit is toegestaan als de betrokkene daarvoor uitdrukkelijk toestemming geeft of als aan specifiek in de AVG opgenomen voorwaarden wordt voldaan. Het verwerken van medische gegevens voor de uitvoering van een pensioenregeling voor arbeidsongeschikte deelnemers, zoals premievrijstelling (PVI) en de toekenning van een arbeidsongeschiktheidspensioen (AOP), is wel uitdrukkelijk toegestaan voor pensioenfondsen. 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 de betrokkenen.

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

- Contactgegevens van het fonds en van de Functionaris Gegevensbescherming (zie Ad 5).
- Rechtsgrond en doelstelling van de verwerking van persoonsgegevens.
- Ontvangers van de persoonsgegevens (bijvoorbeeld uitvoeringsorganisaties bij uitbesteding).
- 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. De AVG schrijft bovendien voor dat deze informatie beknopt, transparant en begrijpelijk moet zijn. Er mag dus geen technisch of juridisch jargon worden gebruikt.

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 van 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 uitvoeringsorganisatie als feitelijke verwerker van persoonsgegevens een eigen verwerkingsregister aan te houden.

Ad 3) Zorgen voor sluitend 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' (*data processor*) of van andere rechtshandelingen waardoor deze partijen gebonden worden. 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 (verwerkings-verantwoordelijke en verwerker) goed te onderscheiden, maar in de praktijk is het niet altijd duidelijk of een partij verwerkingsverantwoordelijke is of verwerker. Organisaties kunnen ook beide rollen vervullen.

[1] Inclusief 'profiling'.
[2] Dit geldt altijd voor grote werkgevers (inclusief fondsen/stichtingen) met 250 of meer werknemers.
[3] Onder de Wet bescherming persoonsgegevens worden dit 'bewerkersovereenkomsten' genoemd.

Ook bij de uitvoering van een pensioenregeling kan daarvan sprake zijn. Een werkgever sluit immers een pensioenovereenkomst met een werknemer en vraagt daarvoor persoonsgegevens uit bij de werknemer. Voor de uitvoering van deze pensioenovereenkomst sluit de werkgever een uitvoeringsovereenkomst met een pensioenuitvoerder, zoals een pensioenfonds. Daartoe meldt de werkgever de werknemer aan bij het pensioenfonds en verstrekt de werkgever de voor de uitvoering noodzakelijke gegevens aan het pensioenfonds. In die situatie is de werkgever aan te merken als verwerkingsverantwoordelijke en het pensioenfonds 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 mogelijk ook deze derde partij aan te merken als een verwerker. In dat geval zouden op grond van de AVG zowel tussen de werkgever en de pensioenuitvoerder als tussen de werkgever en deze derde partijen verwerkersovereenkomsten gesloten moeten worden.

Pensioenfondsen ontvangen bepaalde gegevens rechtstreeks van (gewezen) deelnemers. Een pensioenfonds heeft de administratie van de pensioenregeling verder meestal uitbesteed aan een uitvoeringsorganisatie, waaraan de rechtstreeks van de (gewezen) deelnemers ontvangen persoonsgegevens en de via de werkgever ontvangen persoonsgegevens worden doorgegeven. In die situatie is het pensioenfonds aan te merken als verwerkingsverantwoordelijke en de uitvoeringsorganisatie als verwerker. De uitvoeringsorganisatie kan op zijn beurt onderdelen van de pensioenadministratie waarbij persoonsgegevens worden verwerkt, zoals bijvoorbeeld het opstellen van UPO's, hebben uitbesteed aan subverwerkers. Een en ander dient wel goed vastgelegd te worden. Daarbij moet er voor worden gewaakt, dat de contractuele verplichtingen van de subverwerker (met name de technische en organisatorische beschermingsmaatregelen) niet afwijken van de contractuele verplichtingen van de uitvoeringsorganisatie jegens het pensioenfonds en de werkgever.

De AVG verplicht verwerkingsverantwoordelijken en verwerkers in beginsel tot het sluiten van verwerkersovereenkomsten of het treffen van andere bindende rechtshandelingen in elke situatie waarbij persoonsgegevens worden uitgewisseld. Dit geldt ook bij de uitvoering van pensioenregelingen. Deze verplichting zou mogelijk anders ingevuld kunnen worden als de verwerking plaatsvindt op basis van een wettelijk voorschrift zoals bij een verplichtgesteld bedrijfstakpensioenfonds of beroepspensioenfonds. Het lijkt immers niet praktisch dat tussen werkgevers en deze verplichtgestelde pensioenfondsen verwerkersovereenkomsten moeten worden opgesteld. De regelgeving biedt hierover op dit moment nog geen duidelijkheid.

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' of DPIA)*[4]. 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. Een DPIA moet ten minste de volgende onderdelen bevatten:

- Systematische beschrijving van de beoogde verwerkingen en verwerkingsdoelen.
- Beoordeling noodzaak en evenredigheid van de verwerkingen.
- Beoordeling rechten en risico's en vrijheden betrokkenen.
- Beoogde maatregelen om risico's aan te pakken.

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

[4] Geldt altijd voor grote werkgevers (inclusief fondsen/stichtingen) met 250 of meer.

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 als FG 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[5]. 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 ontslagbescherming geniet bij de uitvoering van zijn taken onder AVG. Dit is niet (wettelijk) geregeld voor een privacy officer[6].

Ad 6) Melding datalekken
De meldplicht voor datalekken blijft onder de AVG gehandhaafd. Een pensioenfonds moet als verwerkingsverantwoordelijke elke inbreuk in verband met persoonsgegevens binnen 72 uur nadat het pensioenfonds er kennis van heeft genomen melden bij de AP. De melding hoeft echter niet plaats te vinden als het 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 uitvoeringsorganisatie als verwerker de melding aan het fonds heeft gedaan. De AVG bepaalt hierover dat een verwerker de verwerkingsverantwoordelijke moet informeren 'zonder onredelijke vertraging', zodra hij kennis heeft genomen van een inbreuk. Als een inbreuk waarschijnlijk een groot risico inhoudt voor de rechten en vrijheden van betrokkene(n), moet de melding ook aan de betrokkene(n) zelf plaatsvinden. Andere pensioenuitvoerders (verzekeraars en ppi's) hoeven deze melding aan betrokkene(n) niet te doen; zoals het er nu naar uitziet, pensioenfondsen wel.

De AVG stelt strengere eisen aan de eigen registratie van 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.

Er blijft 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 (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.

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.

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

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 tijd klaar te zijn voor de AVG. Om u hierbij te helpen, heeft de AP op de website een stappenplan opgenomen. 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 nu actie te ondernemen. 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	Het bestuur bepaalt eerst zijn risicohouding en risicobereid-heid. Na deze essentiële stap is het van belang om een ketenanalyse te maken aan de hand van de volgende vragen: Welke data wordt waar verwerkt en door wie? Waarom verwerken we als fonds deze data (zowel aan de bestuurstafel als bij uitvoerders) en wat is de rechtsgrond?	**Ultimo 2017**
1	Opstellen privacy beleid	In het beleid worden de resultaten van stap 0 opgenomen. Aandacht voor 'privacy by default' en 'privacy by design'. Onderdeel van beleid kan zijn het opstellen van een privacy verklaring en een protocol melding datalekken.	**Januari 2018**
2	Opstellen verwerkingsregister	Inhoud: • Contactgegevens fonds en FG. • Verwerkingsdoelen. • Categorieën betrokkenen, gegevens en ontvangers. • Bewaartermijnen. • Technische en organisatorische beveiligingsmaatregelen.	**Januari 2018**
3	Zorgen voor sluitend systeem verwerkersovereenkomsten	Opstellen nieuwe overeenkomsten of wijzigen bestaande (bewerkers)overeenkomsten tussen verwerkingsverant-woordelijken en verwerkers (juridische stap).	**Februari 2018**
4	Opstellen gegevensbeschermings-effectbeoordeling (DPIA)	Inhoud: • Beschrijving beoogde verwerking en verwerkingsdoelen. • Beoordeling noodzaak en evenredigheid verwerking. • Beoordeling rechten en risico's en vrijheden betrokkenen, gelet op aard, omvang, context en doelen verwerking. • Beoogde maatregelen om risico's aan te pakken. • DPIA kan worden opgesteld na voorgaande stappen te hebben gezet.	**Februari 2018**
5	Aanwijzen FG	Mag samen met uitvoeringsorganisatie (extern) worden belegd.	**April 2018**
6	Aanpassen systemen en procedures	Volgt uit privacy beleid en kan zeer materieel zijn afhankelijk van uw geautomatiseerde systemen.	**Mei 2018**
7	Naleving AVG	Mogelijkheid toepassen Code Verwerking Persoonsgegevens Pensioenfondsen'[7] en het opzetten van een planning & control cyclus voor de AVG. Wij adviseren om dit op te nemen in de Risk & Compliance jaarcyclus en ISAE proces.	**Mei 2018**

[7] De Pensioenfederatie heeft aangekondigd pensioenfondsen te helpen om de AVG na te leven middels het opstellen van een *'Gedragscode Verwerking Persoonsgegevens Pensioenfondsen'.* Het aansluiten bij een goedgekeurde gedragscode kan worden gebruikt als element om aan te tonen dat de AVG-verplichtingen zijn nagekomen. Deze gedragscode is thans nog niet beschikbaar.

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

Bekijk ook onze andere artikelen op http://www.sprenkelsenverschuren.nl of neem contact op met uw vaste contactpersoon bij Sprenkels & Verschuren bij vragen over de AVG of andere elementen van het Risk & Compliance proces.

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.

Over Sprenkels & Verschuren

Wij zijn onafhankelijke adviseurs. Wij geven niet alleen advies, maar 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.