Onderstaand artikel is in verkorte vorm als opiniestuk gepubliceerd op de website van Pensioen Pro (www.pensioenpro.nl) op 16 februari 2018. Het artikel is geschreven door Ad Meeuwesen van KoutersVanderMeer in samenwerking met Niels Romijn van Willis Towers Watson.

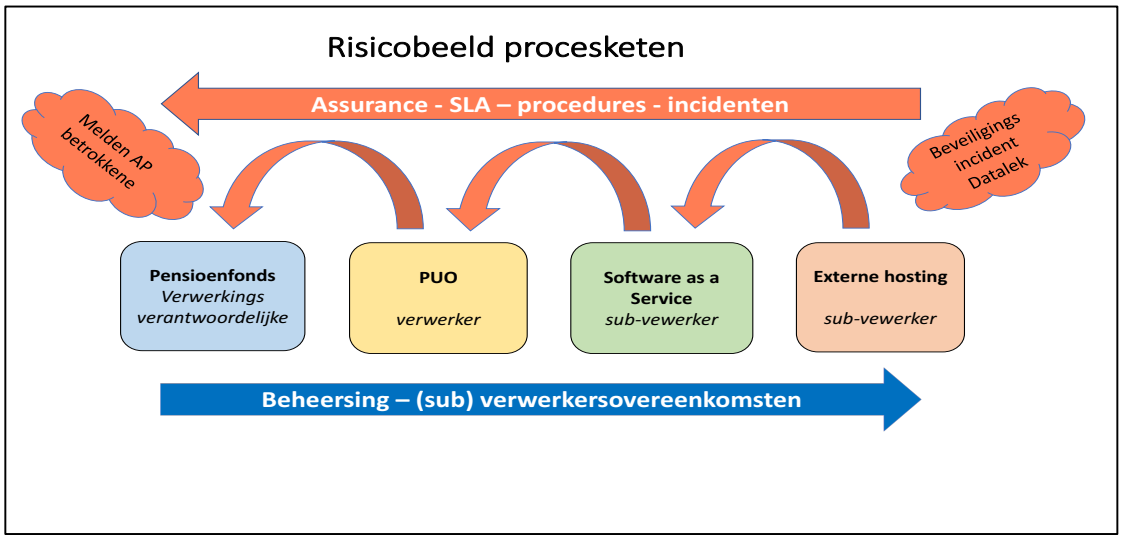
Het implementeren van de EU-AVG: geen hogere wiskunde!

Vanaf mei 2016 is de EU-AVG van kracht geworden en hebben organisaties 2 jaar de tijd om aan de verplichtingen uit deze Europese verordening te gaan voldoen. De afgelopen periode zijn we overspoeld met artikelen over op welke wijze organisaties, waaronder pensioenfondsen, dit moeten doen. Toch blijkt het zetten van een eerste stap lastig. Maar waarom? Het implementeren van de EU-AVG is geen hogere wiskunde. *Je gaat het pas zien als je het doorhebt,* zie een bekend persoon ooit. En dat is precies waar het om draait bij het implementeren van de EU-AVG. Uiteindelijk zie je welke stappen je moet zetten, omdat je de achterliggende gedachte en de logische opzet van de EU-AVG begrijpt. Dit artikel beschrijft enkele van deze stappen. Advies is, ga stappen zetten, want mei 2018 is het zo.

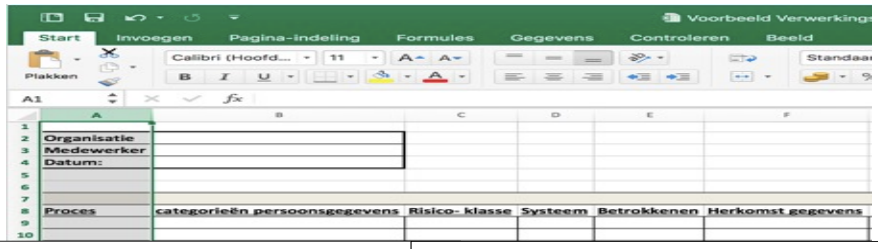
Wat is al geregeld?
Bekijk wat je als pensioenfonds, mogelijk onbewust, al hebt geregeld in het kader van de Wet Bescherming Persoonsgegevens. Dat is de basis van waaruit het pensioenfonds de verplichtingen uit de EU-AVG gaat oppakken. De EU-AVG is veelal een aanvulling cq. aanscherping van de WBP. In het Servicedocument Gegevensbescherming van de Pensioenfederatie is overzichtelijk weergegeven welke aanvullingen en aanscherpingen er zijn. Als je weet wat je al hebt en je legt dat naast wat er aanvullend moet, dan heb je de gap-analyse gedaan.

Nieuw uitgangspunt
Belangrijk nieuw uitgangspunt van de EU-AVG is de verantwoordingsplicht van pensioenfondsen en de verplichting de naleving van de EU-AVG aan te kunnen tonen. Dit betekent dat je als pensioenfonds besluiten in het kader van EU-AVG moet motiveren, zaken moet beschrijven en op tijd alles geïmplementeerd moet hebben.

Procesplaat
Bepaal aan de hand van een procesplaat je speelveld waarvoor je als pensioenfonds verantwoordelijk bent. Zie bijvoorbeeld onderstaande afbeelding, die ziet op een pensioenadministratie. Beschrijf welke (sub)partijen de administratie voor je voeren, welke (bijzondere) persoonsgegevens betrokken zijn, wat doelstellingen en grondslagen van de gegevensverwerking zijn en welke afspraken gelden met deze (sub)partijen. Op basis van deze procesplaat kun je partijen tevens kwalificeren als (sub)verwerker of als verwerkingsverantwoordelijke.



Verwerkingsgregister
Met de informatie uit de procesplaat maak je een eerste opzet van het verwerkingsregister, je gegevensbeschermingsbeleid en privacyverklaring. Je kunt ook gebruik maken van het op basis van de WBP verplichte meldformulier bij de Autoriteit Persoonsgegevens ten behoeve van het meldingenregister. Zie bijgaande afbeelding van een eenvoudig verwerkingsregister in Excel. Later kun je het verwerkingsregister, het gegevensbeschermingsbeleid en de privacyverklaring aanvullen.



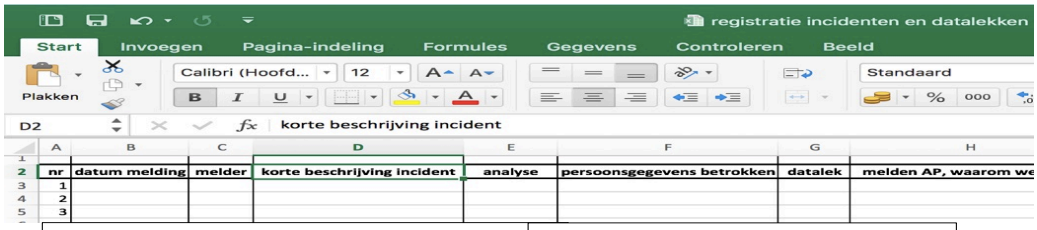
- Proces
- Categorieën Persoonsgegevens
- Risico-klasse
- Systeem
- Betrokkenen
- Herkomst Gegevens

- Ontvangers
- (sub) verwerkers
- Doelstelling
- Rechtmatige grondslag
- Bewaartermijn
- Beveiligingsmaatregelen

Verwerkersovereenkomsten
Check je verwerkersovereenkomsten met je verwerkers. Vul deze aan of als er nog geen overeenkomsten zijn, sluit deze dan af. Zorg dat met sub-verwerkers dezelfde afspraken worden gemaakt. Zet je verwerkers aan de slag en laat ze ook een verwerkingsregister opmaken.

Beleid en rechten betrokkenen
Denk zelf na over (aanpassing van) je eigen gegevensbeschermingsbeleid en privacybeleid en integreer dit met je Integraal Risico Management methodiek. Dit gegevensbeschermingsbeleid vormt onder andere ook de basis voor je technische en organisatorische (beveiligings)maatregelen die je treft (of al hebt getroffen). Neem hierin een verbetercyclus op om periodiek de effectiviteit van de genomen maatregelen te toetsen. Het privacybeleid dient voor transparantie richting deelnemers/betrokkenen. Vul de procedures met betrekking tot de rechten van betrokkenen aan. Het gaat om inzage, rectificatie, verwijdering, beperking, overdraagbaarheid en bezwaar.

Datalekken
Alle incidenten (datelekken) met betrekking tot de verwerking van persoonsgegevens moeten geregistreerd worden. Neem in dit incidentenregister ook de analyse op waarom een incident wel of niet kwalificeert als een datalek. En in het geval sprake is van een datalek of deze gemeld is bij de Autoriteit Persoonsgegevens en betrokkenen. Richt een verbetercyclus in om na te gaan of je zaken anders/beter kunt doen. Beschrijf de stappen en verantwoordelijkheden in een procedure. Werk ook aan het risicobewustzijn van je medewerkers.



- Nummer
- Datum melding
- Melder
- Korte beschrijving
- Analyse
- Persoonsgegevens betrokkenen
- Datalek

- Melden AP – Wel/Niet
- Melden betrokkenen – Wel/Niet
- Maatregelen
- Evaluatie
- Mogelijke verbeteringen

PIA en FG

Twee onderdelen waarvan het nog niet duidelijk is of dit te allen tijde een verplichting is, zijn het privacy impact assessment (PIA) en de aanstelling van een functionaris gegevensbescherming (FG). Ons advies is om bij nieuwe werkwijze of applicatiekeuze altijd te bepalen wat de privacy risico's zijn en of deze risico's afdoende worden beheerst. Ten aanzien van de FG gaat het wat ons betreft niet zozeer om de vraag of je een functionaris formeel aanstelt maar meer of je de noodzakelijke expertise – intern of extern – hebt geborgd.

Alles overziend concluderen wij dat het implementeren van de EU-AVG weliswaar best bewerkelijk is, maar zeker geen hogere wiskunde. Bewustwording van de EU-AVG is al een eerste stap naar verandering. Nu is het tijd om de vervolgstappen te zetten. Ga dus aan de slag. Succes met de voorbereidingen en implementatie!