TriView

Compliance Nieuwsbrief

Klokkenluidersregeling en bescherming van persoonsgegevens

Verder in deze nieuwsbrief:

- Uitbesteding en in control zijn over gedragsnormen
- Vervallen Privacyshield

februari 2021

De Klokkenluidersregeling en bescherming van persoonsgegevens

Meldingen van klokkenluiders van pensioenfondsen bevatten veel persoonlijke gegevens die anoniem worden verwerkt. Een effectieve werking van een klokkenluidersregeling vraagt in veel gevallen om niet anonieme gegevensverwerking. Tot hoever strekt de bescherming van de anonimiteit van de melder?

Met de komst van de Algemene Verordening Gegevensbescherming (AVG) in 2018 hebben organisaties meer verantwoordelijkheden gekregen en moeten zij zelf aantonen dat hun verwerkingen in overeenstemming zijn met de vereisten voor gegevensverwerking. Het vinden van een passende balans tussen de anonimiteit van de klokkenluidersregeling en de AVG is specifiek van belang in het kader van de DPIA op grond van de AVG.

Wanneer de verwerking van persoonsgegevens een hoog risico oplevert voor de rechten van de betrokkene, dient het pensioenfonds op grond van de AVG een gegevensbeschermingseffect-beoordeling (Engelse afkorting: DPIA) uit te voeren. Een DPIA is een tool om vooraf de privacy-risico's van gegevensverwerking in kaart te brengen en wordt beschouwd als een belangrijk instrument voor verantwoording omdat het aantoont dat er passende maatregelen zijn getroffen om de naleving van de AVG te waarborgen.

Wanneer is er sprake van een hoog privacy risico? De AVG vereist niet dat een DPIA wordt uitgevoerd voor elke verwerking die risico's voor de rechten en vrijheden van natuurlijke personen kan inhouden. Een DPIA is alleen verplicht als de verwerking "waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen". Het Europees adviesorgaan Groep Gegevensbescherming Artikel 29 geeft enkele voorbeelden wanneer een verwerking "waarschijnlijk een hoog risico inhoudt". Zo worden grootschalige verwerkingen van bijzondere categorieën van persoonsgegevens genoemd of systematische en uitgebreide beoordelingen van persoonlijke aspecten van natuurlijke personen. Een dergelijke verwerking van persoonsgegeven kan aan de orde zijn voor pensioenfondsen; werk aan de winkel dus.

Wat moet een pensioenfonds doen? Code 21 van de Code Pensioenfondsen schrijft een klokkenluidersregeling voor een pensioenfonds voor. De Model Klokkenluidersregeling 2020 van de Pensioenfederatie geeft daar een generieke invulling aan. Dit model moet worden afgestemd op uw pensioenfonds. De verwerking van persoonsgegevens kan bij de klokkenluiders-regeling een hoog risico opleveren omdat niet in alle gevallen de anonimiteit van de klokkenluider kan worden gegarandeerd.

Een voorbeeld hoe de AVG hierop inspeelt is het feit dat de AVG klokkenluiders een sterkere positie geeft ten aanzien van zeggenschap over hun eigen gegevens. De Model Klokkenluidersregeling van de pensioenfederatie regeling haakt hier op in. Zo biedt deze modelregeling niet alleen bescherming over inzage van persoonlijke gegevens van de melder maar schrijft bijvoorbeeld ook regels voor betreffende mogelijke interne en externe publicaties. Voor pensioenfondsen is het zaak om te beoordelen of de positie van klokkenluiders binnen het fonds conform de AVG voldoende beschermd wordt.

Uitbesteding en in control zijn over gedragsnormen

Voor pensioenfondsen is het van belang om 'in control' te zijn over de uitbestede werkzaamheden en de verdere keten van uitbesteding. Dit geldt ook voor compliance gerelateerde onderwerpen. Bij DNB ligt hier ook de focus op in het kader van het toezicht. De volgende onderwerpen zijn in dit kader specifiek van belang:

- Naleving van de gedragsnormen uit de gedragscode van het pensioenfonds;
- Incidenten- en klokkenluidersregeling en klachtenregeling alsmede melding incidenten/ misstanden/ klachten;
- Naleving sanctiewetgeving en wetgeving terrorismefinanciering;
- Beloningsbeleid;
- AVG beleid en melding datalekken.

Enerzijds is van belang dat voor de genoemde onderwerpen adequaat beleid en processen zijn geformuleerd en vastgelegd. Dit zal bij aanvang van de werkzaamheden veelal onderdeel zijn van het selectieproces. Echter een periodieke, bij voorkeur jaarlijkse, toets of dit beleid en de processen actueel zijn, is naar onze mening ook van belang. Verder dient het pensioenfonds te controleren op de naleving van dit beleid en processen. Denk in dit kader aan de naleving van de gedragscode door betrokken medewerkers, zijn er incidenten of datalekken geweest en vindt adequate screening op de naleving van sanctiewetgeving plaats. Dit zowel bij de uitbestedingspartij zelf, als bij eventuele onderuitbestedingen. Wat hierbij helpt zijn periodieke verantwoordingsrapportages van uitbestedingspartijen waarin zij zelf proactief rapporteren over deze onderwerpen. Zo blijft het pensioenfonds door het jaar heen in control. Het alternatief is een periodieke, bij voorkeur jaarlijkse, uitvraag door (de compliance officer van het) pensioenfonds om de naleving te toetsen.

Vervallen Privacyshield

In het kader van de AVG is het niet toegestaan om persoonsgegevens door te geven naar een land buiten de Europese Economische Ruimte ("EER") als dat land een ontoereikend beschermingsniveau biedt ten aanzien van persoonsgegevens. De Verenigde Staten ("VS") is een van die landen waar sprake is van een ontoereikend beschermingsniveau van persoonsgegevens. Om de doorgifte van persoonsgegevens vanuit de EER naar de VS toch mogelijk te maken is in 2016 het EU-US Privacyshield overeengekomen tussen de Europese Commissie en de VS. Het Europese Hof heeft 16 juli 2020 (Schrems II/ Facebook zaak) het Privacyshield beoordeeld en heeft geconcludeerd dat onvoldoende bescherming met betrekking tot persoonsgegevens wordt geboden door het Privacyshield. Deze uitspraak heeft tot gevolg dat de afspraken uit het Privacyshield per direct ongeldig zijn verklaard. Om voldoende bescherming van persoonsgegevens in de VS te waarborgen kan worden gewerkt met modelcontracten met bedrijven in de VS (zogenaamde 'standard contractual clauses'), of kan gebruik worden gemaakt van de aanbevelingen die de European Data Protection Board (EDPB) heeft gepubliceerd.

Voor pensioenfondsen is het van belang om te analyseren in hoeverre zaken wordt gedaan met partijen die zelf of via onderuitbestedingen persoonsgegevens doorgeven of door kunnen geven aan de VS. Indien dit het geval is dienen nadere afspraken te worden vastgelegd om de privacy voldoende te waarborgen.