Eén jaar na de AVG: Wat is er veranderd en wat moet er nog gebeuren?

“Er moet nog een verdiepingsslag plaatsvinden. Op 25 mei 2018 trad de AVG na veel publiciteit in werking en op 26 mei ontdekten we gelukkig dat de wereld niet was veranderd en gewoon doordraaide. Wat was er nu anders voor de deelnemers? Pensioenfondsen hadden een privacyverklaring op hun website geplaatst en in hun startbrieven wezen ze op bescherming van de privacy. Er was voldoende aandacht voor de AVG, maar binnen de pensioenorganisaties moest de wet nog een plekje krijgen.”

Stefan van de Giessen is binnen Montae een specialist die pensioenfondsbesturen adviseert over het beheren en verwerken van persoonsgegevens. Precies een jaar na de invoering van de Algemene verordening gegevensbescherming (AVG) zoeken wij hem op om te vragen hoe hij terugkijkt op 1 jaar AVG. Wat is er veranderd en wat moet er nog gebeuren? Is de indruk correct dat veel fondsbesturen destijds hijgend naar de datum 25 mei toewerkten om te voldoen aan de zoveelste nieuwe wetgeving voor pensioenfondsen? “Je moet bedenken dat de AVG weliswaar al twee jaar eerder was aangekondigd, maar dat de impact van de wet en regelgeving nog niet altijd even concreet was voor de pensioenfondsen” zegt Stefan. “Besturen hadden dus een flinke uitdaging. Daarnaast betekende de implementatie van de AVG een extra belasting voor hun toch al niet geringe takenpakket.”

Ontdekkingsreis

De AVG was in bepaalde opzichten een ontdekkingsreis voor pensioenfondsen. Het vertalen van de AVG naar praktische oplossingen was soms een uitdaging. “Fondsen leunden bijvoorbeeld vaak op de pensioenadministrateur, die een kritische uitbestedingsrelatie is en tevens verwerker voor het pensioenfonds. Het steunen op de administrateur om de AVG geïmplementeerd te krijgen, is niet voldoende omdat de verwerkingsverantwoordelijkheid bij het bestuur ligt en de

pensioenadministrateur slechts één van de verwerkers is. Omdat pensioenfondsen de verwerkingsverantwoordelijke zijn, bepalen fondsbesturen de doelen waarvoor persoonsgegevens worden verwerkt en de middelen waarmee dit gebeurt. Pensioenfondsen verwerken grote hoeveelheden privacygevoelige gegevens en zij hebben er dus belang bij dat dit veilig en zorgvuldig gebeurt.

Besturen hebben altijd al het belang en de waarde van duidelijke privacyregels en adequate bescherming van persoonsgegevens gezien. Met de digitalisering die plaatsvindt in de sector en de komst van de AVG beseften zij dat voor een goede implementatie van de AVG meer nodig was dan wachten op het groene licht van de pensioenadministrateur. Naarmate de acties voor de implementatie van de AVG concreter werden, zijn fondsen druk bezig geweest met onder meer het ontwikkelen en het aanscherpen van hun informatiebeveiligingskaders, het stellen van bewaartermijnen, het implementeren van procedures hoe datalekken af te handelen en het toetsen van de volwassenheid van de informatiebeveiligingsmaatregelen bij hun verwerkers.

Hulp op verschillende gebieden

Stefan vertelt dat Montae fondsen op verschillende gebieden heeft geholpen om te voldoen aan de nieuwe privacywetgeving. “We hebben quick scans gemaakt om in kaart te brengen wat er moest gebeuren. We hebben overeenkomsten met verwerkers en documenten voor het IT- beleid, het uitbestedingsbeleid en het integraal risicomanagementbeleid opgesteld of aangepast. En we hebben advies gegeven over vragen als: wat gebeurt er als er een datalek optreedt? Wie komt er dan in de lucht en wat moet je doen? We hebben ook voor fondsen het intern toezicht houden op de gegevensverwerking, de gegevensbescherming en de naleving van de AVG ingevuld door te zorgen voor een functionaris gegevensbescherming of data protection officer.”

Centraal aanspreekpunt

Fondsen zijn in bepaalde situaties verplicht om een functionaris gegevensbescherming aan te stellen of kunnen besluiten een data protection officer aan te wijzen, die toeziet op de naleving van de AVG. Dit is een soort ‘light’ versie van de functionaris gegevensbescherming. “Wij vullen die rollen overigens wel op een vergelijkbare manier in op basis van best practices die wij steeds

verder doorontwikkelen”, zegt Stefan. “Je ziet bij veel fondsen dat de functionaris gegevensbescherming vooral vanuit de juridische invalshoek opereert. Wij hebben gekozen voor een andere aanpak. Als wij een functionaris gegevensbescherming leveren aan een fonds dan is die het centrale aanspreekpunt voor alle aspecten die bij de verwerking en bescherming van gegevens een rol spelen. Of het nu gaat om toetsen en adviseren over IT en informatiebeveiliging, het aanpassen van juridische documenten of het integraal onderbrengen van de AVG binnen de risicobeheersing binnen het fonds. Onze functionaris zorgt ervoor dat er specialisten worden aangehaakt uit verschillende disciplines binnen een team dat hier specifiek voor is samengesteld. Wij beschikken over een multidisciplinair team, dat klaar is voor elk vraagstuk met betrekking tot privacybescherming en de bijhorende technische en organisatorische maatregelen. Met die aanpak onderscheiden we ons in de markt.”

Nog veel te winnen

De meeste pensioenfondsen hebben inmiddels de verplichte zaken met betrekking tot de AVG zoals privacyverklaring, verwerkingsovereenkomsten en verwerkingsregister op orde. Maar volgens Stefan is er nog wel veel te winnen om te zorgen dat gegevensbescherming permanent aandacht krijgt binnen pensioenfondsen en wordt ingepast in bestuur cycli om de naleving van de regels te blijven volgen.

Ook moet er volgens hem nog een verdiepingsslag plaatsvinden. “Als voorbeeld: veel fondsen hebben de pensioenadministratie uitbesteed aan een pensioenadministrateur. Maar daarachter zit een hele wereld van verschillende partijen die zich met de verwerking van persoonsgegevens bezighouden. Het bestuur is verwerkingsverantwoordelijke en moet dus inzicht hebben in hoe al die partijen hun taak uitvoeren en bijdragen aan voldoende beheersingsmaatregelen om de privacy van de betrokkenen te beschermen. Hierbij denken we niet alleen aan de drukker die de brieven verstuurt, maar ook de datacenters en diverse hostingpartijen die persoonsgegevens verwerken. Wij kennen deze digitale wereld en zijn klaar om fondsen te ondersteunen om de juiste mate van besturing en beheersing te vinden. Wij helpen besturen te sturen op de bescherming van privacy en gevoelige informatie.

Gedragslijn

Onlangs heeft de Pensioenfederatie een concept Gedragslijn Verwerking Persoonsgegevens Pensioenfondsen gepubliceerd. “De Federatie doet daarmee een stap naar voren om zich te positioneren als het aanspreekpunt voor de pensioenbranche op het gebied van gegevensbescherming als verlengstuk van de Autoriteit Persoonsgegevens.” In dit lijvige document geeft de Pensioenfederatie richtlijnen voor sector-gerelateerde onderwerpen rond gegevensverwerking en –bescherming. “Voor fondsbesturen die de AVG-regelgeving goed hebben ingevoerd zou het document geen verrassingen moeten bevatten”, zegt Stefan. Ze kunnen het zien als een toetsmiddel om te bepalen of ze goed bezig zijn. Daar helpt deze gedragslijn bij.”