ravc ©

SPRENKELS & VERSCHUREN
STRATEGY • GOVERNANCE • RISK • COMPLIANCE

RiskTransparant nummer 10

AVG één jaar na invoering: Waar staat uw fonds?

Op 25 mei 2018 heeft u de nieuwe privacywetgeving (AVG) ingevoerd. Inmiddels zijn we een jaar verder. Pensioenfondsen hebben op meer dan gepaste wijze invulling gegeven aan de nieuwe privacy verplichtingen. Toch leven in de praktijk nog steeds vragen. Eerder brachten wij al een drietal Q&A's uit over de AVG. In deze RiskTransparant delen wij graag met u welke 10 vragen wij horen aan de bestuurstafel.

1. Hoe zit het met de Code AVG van de Pensioenfederatie? Komt die nog?

De Pensioenfederatie publiceert geen 'Code Verwerking Persoonsgegevens Pensioenfondsen', zoals eerder aangekondigd. Wel heeft zij inmiddels een consultatieversie gepubliceerd voor een nieuwe '**gedragslijn**'. De vormgeving van deze 'gedragslijn' en het moment van publicatie zijn nog niet bekend. Deze gedragslijn is weliswaar geen gedragscode in de zin van de AVG, maar gaat net zoals de Code Pensioenfondsen waarschijnlijk wel een bindend karakter hebben ('comply or explain').

2. Wel of geen datalek melden bij AP?

Een datalek is een inbreuk op de beveiliging, die leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens. Als het waarschijnlijk is, dat een datalek een risico inhoudt voor de rechten en vrijheden van betrokkenen, dan dient dit datalek in beginsel uiterlijk binnen 72 uur na constatering te worden gemeld bij de AP. Er is sprake van een risico als de persoonsgegevens in handen (kunnen) komen van onbevoegde derden. De vraag of het waarschijnlijk is hangt af van de feiten en omstandigheden. Zo zal bij wijze van voorbeeld het verlies van een datastick met persoonsgegevens, die is beveiligd ('encrypted') volgens de laatste technische stand van zaken, in beginsel niet worden aangemerkt als een datalek, tenzij er geen kopie meer beschikbaar is van de bestanden met persoonsgegevens op de datastick.

3. Wel of geen datalek doormelden aan de betrokkene?

Niet elk datalek hoeft te worden gemeld aan de betrokkene. Dit hoeft alleen als er een 'hoog privacy risico' voor betrokkene is. Hiervan is sprake als het datalek kan leiden tot ernstige schade voor betrokkene, zoals bijvoorbeeld discriminatie, identiteitsfraude, financiële schade of reputatie schade of als een betrokkene zijn AVG-rechten niet meer kan uitoefenen. Het lekken van paspoortgegevens of Burger Service Nummer (BSN) kan bijvoorbeeld leiden tot identiteitsfraude. Het BSN mag overigens alleen verwerkt worden als dat op grond van de wet is toegestaan. Wij adviseren daarom om zo weinig mogelijk te corresponderen met BSN-gegevens.

4. Wel of geen datalek als 'incident' melden bij DNB?

Datalekken kunnen tevens kwalificeren als 'incidenten' volgens het Incidentenbeleid van het fonds. Er moet dan sprake zijn van een 'ernstig gevaar voor de integere uitoefening van het bedrijf van een fonds'. In dat geval is tevens een onverwijlde melding nodig bij DNB ingevolge artikel 19a lid 4 Besluit FTK. Hierbij kunt u denken aan een hack van het systeem, waarbij toegang tot een groot aantal persoonsgegevens is verkregen. Een incidenteel datalek van bijvoorbeeld twee brieven voor twee verschillende deelnemers, kan wel kwalificeren als een datalek, maar is geen incident dat aan DNB gemeld moet worden.

5. Moeten wij alle datalekken registreren?

Ja, u moet alle gemelde en niet-gemelde datalekken (beveiligingsincidenten) registreren. Daarbij moet u vastleggen in een 'datalekregister':

a) Omschrijving van het datalek
b) Wanneer het datalek heeft plaatsgevonden
c) Welke persoonsgegevens het betreft

d) Wat er met deze gegevens is gebeurd (verloren gegaan, door onbevoegde ingezien, gekopieerd of gewijzigd)
e) Van welke betrokkenen er gegevens gelekt zijn en om hoeveel personen het gaat
f) Gevolgen van het datalek
g) Maatregelen die zijn genomen naar aanleiding van het datalek.

Doel van deze registratie is om datalekken in de toekomst te kunnen voorkomen en om jegens de AP aan te tonen dat datalekken worden gemonitord en opgevolgd. Een pensioenfonds kan het datalekregister onderdeel laten zijn van het reeds bestaande incidentenregister.

6. Wij hoeven geen PIA op te stellen. Klopt dat nog steeds?

Een pensioenfonds moet een PIA opstellen als er bij de verwerking van persoonsgegevens sprake is van een 'hoog privacy risico' voor betrokkenen. Er bestaat een lijst met negen criteria om te beoordelen of er sprake is van een hoog privacy risico. Als vuistregel kan gehanteerd worden, dat als een verwerking aan twee hiervan voldoet een PIA moet worden uitgevoerd. De negen criteria zijn:

a) Grootschalige gegevensverwerkingen
b) Gevoelige (bijzondere) persoonsgegevens
c) Gekoppelde databases
d) Gegevens over kwetsbare personen
e) Gebruik van nieuwe technologieën
f) Beoordelen van mensen op basis van persoonskenmerken
g) Geautomatiseerde beslissingen
h) Stelselmatige en grootschalige monitoring
i) Blokkering van een recht, dienst of contract.

Deze criteria vormen een leidraad om in te schatten of een PIA moet worden uitgevoerd. Ook als een pensioenfonds aan slechts één of geen van deze criteria voldoet, moet kunnen worden onderbouwd waarom het fonds ervoor kiest om geen PIA uit te voeren. Dit maakt onderdeel uit van de verantwoordingsplicht.

De beoordeling moet worden uitgevoerd bij het aangaan van nieuwe verwerkingsactiviteiten en daarnaast periodiek (gemiddeld een keer in de drie jaar) bij bestaande activiteiten om vast te stellen of zich geen veranderingen hebben voorgedaan. Wij adviseren daarom om met de pensioenuitvoeringsorganisatie af te spreken, dat zij rapporteren of en, zo ja, welke aanpassingen er zijn geweest voor uw pensioenfonds. Wij adviseren om met de pensioenuitvoeringsorganisatie af te spreken om u op de hoogte te stellen van een voor uw fonds relevante PIA op een zodanig moment dat u als fonds nog invloed kan uitoefenen op de mogelijk te nemen maatregelen. Algemene PIA's, die niet specifiek voor uw fonds, zijn kunnen periodiek worden gerapporteerd in een privacy auditrapport.

7. Bestaat er voor pensioenfondsen een 'format' voor een PIA?

Nee, de vormgeving van een PIA is niet voorgeschreven. Er zijn uiteraard wel 'formats' of modellen in omloop om een PIA vorm te geven. Volgens de AP, moet in elke PIA in ieder geval verantwoording worden gegeven over de volgende onderdelen van het proces:

a) Systematische beschrijving: wat houdt de verwerking van persoonsgegevens in?
b) Noodzaak en evenredigheid: waarom wordt deze verwerking toegepast?
c) Risico's: wat kan er misgaan vanuit het perspectief van betrokkenen?
d) Maatregelen: hoe borgen we de compliance en hoe pakken we de risico's aan?
e) Documentatie: wat hebben we gedaan en wat heeft het opgeleverd?
f) Toezicht en evaluatie: is er aanvulling of herziening nodig?

De AP adviseert om een goedgekeurde Gedragscode en/of certificeringen bij de PIA te betrekken. Zodra de 'gedragslijn' van de Pensioenfederatie (zie hiervoor bij vraag 1) beschikbaar is, dan ligt het voor de hand om ook deze 'gedragslijn' bij de PIA van het fonds te betrekken.

8. Welke fondsdocumenten moeten worden aangepast in het kader van de AVG?

Elke (nieuwe) uitbesteding van bedrijfsprocessen moet het fonds toetsen aan de AVG-verplichtingen. Te denken valt aan de registerplicht, de PIA en het dekkende systeem van verwerkersovereenkomsten. Dit betreft als het ware een 'on going' ketenanalyse en moet tevens in de paragraaf uitbesteding van de ABTN worden opgenomen. In de paragraaf governance van de ABTN zal de rol van de Functionaris Gegevensbescherming of de Privacy Officer moeten worden beschreven. Daarnaast moet het privacybeleid consistent zijn met het IRM-, IT-, communicatie- en uitbestedingsbeleid van het fonds. Het kan dus goed zijn dat ook deze documenten moeten worden aangepast.

9. Wat is het verschil tussen 'zelfstandige' en 'gezamenlijke' verwerkingsverantwoordelijke?

Er is sprake van een zelfstandige verantwoordelijkheid voor het verwerken van persoonsgegevens als een partij zelf het doel en de middelen van de verwerking bepaalt. Dit omvat het zelfstandig bepalen van bewaartermijnen, melden van datalekken, het inschakelen van verwerkers en het informeren van betrokkenen. Deze partij is aan te merken als een 'zelfstandige' verwerkingsverantwoordelijke. Volgens artikel 26 van de AVG is sprake van twee 'gezamenlijke' verwerkingsverantwoordelijken als twee partijen gezamenlijk doel en middelen van de verwerking bepalen. De 'European Data Protection Board' ('EDP': dit is de nieuwe opvolger van de 'Working Party 29') heeft in het verleden in een 'Opinie' een toelichting gegeven[1]. Daarin staat, dat bij gezamenlijke verantwoordelijken de relatie van partijen verschillende vormen kan aannemen. Er is sprake van een gezamenlijke verantwoordelijkheid als er sprake is van het gezamenlijk bepalen van (gedeelten van) doelen of (gedeelten van) middelen van de gegevensverwerking ('sharing only purposes or means, or a part thereof').

Wij adviseren tenslotte om ook bij de uitwisseling van persoonsgegevens met andere partijen, zoals met een andere verwerkingsverantwoordelijke, afspraken te maken over privacy. Wij denken dan bijvoorbeeld aan afspraken over wie een betrokkene informeert bij een datalek.

10. Hoe handhaven wij onze bewaartermijnen?

In het privacybeleid en het verwerkingsregister van het fonds is vastgelegd wat de bewaartermijnen zijn voor de diverse typen gegevensverwerkingen. Middels de privacyverklaring of het 'privacy statement' zijn de betrokkenen hierover geïnformeerd. Het is aan het bestuur van het fonds om te borgen, dat de persoonsgegevens ook binnen de gestelde termijnen daadwerkelijk worden verwijderd. De Functionaris Gegevensbescherming of de Privacy Officer dient hierop toe te zien en aan het bestuur te rapporteren. Hierbij kunnen digitale tools, zoals Microsoft Exchange, SharePoint of OneDrive ondersteuning bieden. Deze tools controleren automatisch op vooraf ingestelde termijnen en 'deleten' files met persoonsgegevens, wanneer de termijnen zijn verstreken. Dit kunnen zeer lange termijnen zijn. Dit kan helpen voorkomen dat veel tijd wordt besteed aan het bijhouden van bewaartermijnen.

Voor een pensioenfonds zijn lange bewaartermijnen van persoonsgegevens van deelnemers, pensioengerechtigden en andere aanspraakgerechtigden in de pensioenadministratie van het fonds aan te bevelen. Deze termijnen starten bij aanvang van het (aspirant) deelnemerschap en eindigen, nadat de laatste gerechtigde (de partner en/of kinderen van de deelnemer) is overleden en geen aanspraak meer kan doen gelden op pensioen. Daar kunnen dan vervolgens nog de wettelijke bezwaartermijnen bij op worden geteld.

Meer weten over de AVG?
Neem dan contact op met uw vaste contactpersoon!

[1] Zie: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/med/med20100219_c.03_dc-dp_opinion_adopted.pdf (met name bladzijden 17 t/m 22).