ravc ©

S&V

Nieuwsflits Nieuwe Privacywetgeving:

Top 10 meest gestelde vragen: derde en laatste deel

Op 25 mei 2018 heeft u de nieuwe privacywetgeving (AVG) geïmplementeerd. Staat het thema nog steeds op uw agenda? Na ruim vijf maanden zien wij in de praktijk nog een aantal vragen. Eerder brachten wij al de delen 1 en 2 uit, in een reeks van 3. Hierbij treft u onze derde en tevens laatste Nieuwsflits aan.

1. Verschijnt dit jaar nog een Code AVG vanuit de Pensioenfederatie?

Nee, voor zover nu bekend is, publiceert de Pensioenfederatie dit jaar geen 'Code Verwerking Persoonsgegevens Pensioenfondsen' meer. Wel werkt de Pensioenfederatie in overleg met de Autoriteit Persoonsgegevens (hierna: AP) aan nadere guidance voor de sector. De vormgeving van deze guidance (een Code in de zin van de AVG of alleen 'gedragsregels') en het moment van publicatie zijn nog niet bekend.

2. Wat is precies een 'bulkmelding'?

Een 'bulkmelding' is een melding bij de AP van meerdere min of meer gelijktijdig opgetreden datalekken bij grootschalige postverzendingen. Deze melding is bedoeld voor grote organisaties voor wie het melden van elk (afzonderlijk) geopend retour ontvangen of vermist poststuk een onredelijke administratieve last betekent. Ook de verzending van UPO's door pensioenfondsen kwalificeert als een grootschalige postverzending. Als een deel van de UPO's geopend geretourneerd wordt of niet aankomt, dan vallen deze incidenten onder de meldplicht datalekken en moeten zij worden gemeld aan de AP. Pensioenfondsen mogen deze datalekken 'in bulk' melden. De voorwaarden daarbij zijn:

- Het betreft poststukken, die inhoudelijk vergelijkbaar zijn, zodat gegevens zoals aard van de persoonsgegevens en mogelijke gevolgen voor de betrokkenen in de melding correct kunnen worden weergegeven.
- Het in bulk melden van datalekken gebeurt door een specifieke functionaris binnen het fonds (doorgaans de Privacy Officer of de Functionaris Gegevensbescherming).
- Deze functionaris beschikt over een overzicht van alle incidenten, die in bulk zijn gemeld.
- De incidenten waarom het gaat, worden uiterlijk op de overeenkomstige dag van de eerstvolgende kalendermaand na de dag van ontdekking gemeld aan de AP.
- De mogelijkheid om in bulk te melden geldt niet voor één complete zending poststukken, die door een derde wordt aangetroffen (in dat geval is sprake van één datalek).

De AP heeft een elektronisch formulier op haar website beschikbaar gesteld, waarmee pensioenfondsen een bulkmelding kunnen doen. De bulkmelding verschilt niet veel van de normale datalekmelding. Na een proefperiode zal de AP de opgedane ervaringen evalueren, en wordt deze mogelijkheid eventueel breder opengesteld.

3. Is het raadzaam om boetebedingen op te nemen in (nieuwe) verwerkersovereenkomsten?

Het is naar onze mening niet aan te bevelen voor pensioenfondsen om voor de AVG specifieke boetebedingen op te nemen in verwerkersovereenkomsten met verwerkers. Dergelijke bedingen zouden dan over en weer tussen partijen moeten gelden bij niet-nakoming van gemaakte afspraken. Onze ervaring is dat dit in de praktijk gaat wringen: partijen nemen elkaar per afspraak scherper de maat en kijken niet naar oplossingen om de ontstane problemen op te lossen. Het is wel aan te bevelen om een duidelijke aansprakelijkheidsbepaling op te nemen in de verwerkersovereenkomsten, voor het geval het fonds schade lijdt als gevolg van tekortkomingen of fouten van ingeschakelde verwerkers (en sub-verwerkers).

4. Wij hebben nog geen PIA opgesteld. Is dat echt nodig?

Een PIA is een afkorting voor 'Privacy Impact Analysis'. De volledige naam is 'Data Privacy Impact Analysis' (DPIA) of in het Nederlands 'gegevensbeschermingeffectbeoordeling'. Een PIA is een proces dat is bedoeld om de verwerking van persoonsgegevens te beschrijven, de noodzaak en evenredigheid van de verwerking te beoordelen en de daaraan verbonden privacy risico's te beheersen door deze risico's in te schatten en maatregelen te bepalen om ze aan te pakken.

Daarmee is het een proces voor het naleven van de normen van de AVG. 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. Deze negen criteria zijn:

1. Grootschalige gegevensverwerkingen
2. Gevoelige (bijzondere) persoonsgegevens
3. Gekoppelde databases
4. Gegevens over kwetsbare personen
5. Gebruik van nieuwe technologieën
6. Beoordelen van mensen op basis van persoonskenmerken
7. Geautomatiseerde beslissingen
8. Stelselmatige en grootschalige monitoring
9. Blokkering van een recht, dienst of contract.

Hierbij geldt de volgende toelichting:

1. Grootschalige gegevensverwerkingen
   De AVG geeft geen definitie van 'grootschalige gegevensverwerkingen'. De AP adviseert om op basis van de volgende criteria te bepalen of hiervan sprake is:
   - de hoeveelheid mensen van wie gegevens worden verwerkt;
   - de hoeveelheid gegevens en de verscheidenheid aan gegevens die worden verwerkt;
   - de tijdsduur van de gegevensverwerking;
   - de geografische reikwijdte van de gegevensverwerking.
2. Gevoelige (bijzondere) persoonsgegevens
   Het gaat hierbij om bijzondere categorieën van persoonsgegevens als genoemd in artikel 9 van de AVG, zoals informatie over iemands politieke voorkeuren. Het betreft hier ook gegevens die over het algemeen als privacygevoelig worden beschouwd, zoals gegevens over elektronische communicatie, locatiegegevens en financiële gegevens.
3. Gekoppelde databases
   Het gaat hierbij om gegevensverzamelingen die aan elkaar gekoppeld of met elkaar gecombineerd zijn. Bijvoorbeeld databases die voortkomen uit twee of meer verschillende gegevensverwerkingen met verschillende doelen en/of uitgevoerd door verschillende verantwoordelijken, op een manier die betrokkenen niet redelijkerwijs kunnen verwachten.
4. Gegevens over kwetsbare personen
   Bij het verwerken van dit type gegevens kan een PIA nodig zijn omdat er sprake is van een ongelijke machtsverhouding tussen de betrokkene en de verantwoordelijke. Dit heeft als gevolg dat betrokkenen niet in vrijheid toestemming kunnen geven of weigeren voor het verwerken van hun gegevens. Het kan hierbij om bijvoorbeeld werknemers, kinderen en patiënten gaan.
5. Gebruik van nieuwe technologieën
   De AVG is er duidelijk over dat een PIA nodig kan zijn bij het gebruik van een nieuwe technologie. De reden hiervoor is dat dit gebruik gepaard kan gaan met nieuwe manieren om gegevens te verzamelen en te gebruiken, met mogelijk grote privacyrisico's. De persoonlijke en maatschappelijke gevolgen van het gebruik van een nieuwe technologie kunnen zelfs nog onbekend zijn. Een PIA helpt dan om de risico's te begrijpen en te verhelpen.
6. Beoordelen van mensen op basis van persoonskenmerken
   Het gaat hierbij onder meer om profiling en het maken van prognoses, met name op basis van kenmerken als iemands beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen. Voorbeelden hiervan zijn een bank die de kredietwaardigheid van klanten bepaalt (creditscoring), een bedrijf dat DNA-testen aan consumenten levert om gezondheidsrisico's te testen en een bedrijf dat bezoekers van zijn website volgt en op basis daarvan profielen van deze mensen opstelt.
7. Geautomatiseerde beslissingen
   Het gaat hierbij om beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben. Zo'n gegevensverwerking kan er bijvoorbeeld toe leiden dat mensen worden uitgesloten of gediscrimineerd.

8. Stelselmatige en grootschalige monitoring
   Het gaat hierbij om monitoring van openbaar toegankelijke ruimten, bijvoorbeeld met cameratoezicht. Hierbij kunnen persoonsgegevens worden verzameld zonder dat betrokkenen weten wie hun gegevens verzamelt en wat daar vervolgens mee gebeurt.
9. Blokkering van een recht, dienst of contract
   Het gaat hierbij om gegevensverwerkingen die tot gevolg hebben dat betrokkenen:
   - een recht niet kunnen uitoefenen of;
   - een dienst niet kunnen gebruiken of;
   - een contract niet kunnen afsluiten.

   Bijvoorbeeld een bank die persoonsgegevens verwerkt om te bepalen of zij een lening aan iemand willen verstrekken.

Deze criteria zijn een handreiking om in te schatten of een PIA moet worden uitgevoerd. Ook als een pensioenfonds aan slechts één of geen van deze criteria voldoet, moet goed 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 (ten minste 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 jaarlijks rapporteren of en, zo ja, welke aanpassingen er zijn geweest voor uw pensioenfonds. Dit kan de vorm krijgen van een jaarlijks privacy auditrapport.

5. Wie of wat is een 'CISO'?

'CISO' is de afkorting voor 'Chief Information Security Officer'. Het is op grond van de AVG niet noodzakelijk voor pensioenfondsen om een CISO aan te stellen. Een CISO wordt doorgaans aangesteld door organisaties, die op grote schaal gevoelige persoonsgegevens verwerken. Het kan ook concurrentiegevoelige bedrijfsinformatie betreffen. De CISO heeft met name een taak bij het beveiligen van systemen en mobiele devices, zoals laptops en usb-sticks. Ook kan de CISO passende beveiligingsniveaus bepalen en implementeren bij een PIA. Daarbij kan gebruik worden gemaakt van tools om files met persoonsgegevens of financiële data automatisch te classificeren als 'vertrouwelijk'.

6. 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.

7. 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' (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').

[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).

8. Hoe kunnen wij bewaartermijnen handhaven?

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.

Tot slot nog twee specifieke vragen voor beroepspensioenfondsen

9. Wat is de status van de beroepspensioenvereniging onder de AVG?

Wanneer een beroepspensioenfonds persoonsgegevens van deelnemers, slapers en/of pensioengerechtigden verstrekt aan de gelieerde beroepspensioenvereniging, geldt zowel de Wet verplichte beroepspensioenregeling (hierna: Wvb) als de AVG. Als partijen gezamenlijk doelen en middelen voor de verwerking van de persoonsgegevens vaststellen, moeten zij hun verplichtingen als verwerkingsverantwoordelijken vastleggen in een onderlinge regeling als bedoeld in artikel 26 lid 1 AVG. De manier waarop is niet voorgeschreven. In het geval van een beroepspensioenfonds en de gelieerde beroepspensioenvereniging kan dit aanvullend worden opgenomen bij de opdrachtaanvaarding of in de uitvoeringsovereenkomst (bijvoorbeeld in een aparte bijlage bij deze overeenkomst).

10. Welke persoonsgegevens mogen wij doorgeven aan de beroepspensioenvereniging?

In artikel 46 lid 2 van de Wvb is geregeld dat een beroepspensioenfonds alleen naam-, adres- en woonplaatsgegevens (NAW-gegevens) van deelnemers, slapers en pensioengerechtigden mag verstrekken aan de gelieerde beroepspensioenvereniging. Voorts is gegevensverstrekking aan derden (zoals de beroepspensioenvereniging) alleen mogelijk als dit noodzakelijk is voor de uitvoering van de pensioenregeling.

Mogelijk is voor de uitvoering van de beroepspensioenregeling door het fonds en voor het vervullen van de statutaire taken van de beroepspensioenvereniging nodig dat de beroeps-pensioenvereniging beschikt over de status van de deelnemer (actief, slapend of gepensioneerd). Ook die gegevens kunnen in dat geval worden verstrekt. Er is geen wettelijke grondslag om andere persoonsgegevens aan de beroepspensioenvereniging te verstrekken, zoals gegevens over het pensioengevend salaris, het deeltijd percentage of de mate van arbeidsgeschiktheid. Als dat toch wenselijk is, dan dient het fonds hiervoor de uitdrukkelijke toestemming te verkrijgen van de betrokkenen.

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