PF

GVG

Guidance verwerking
persoonsgegevens
pensioenfondsen

PENSIOEN
FEDERATIE

Pensioenfederatie
De Pensioenfederatie is de overkoepelende belangenbehartiger van bijna alle Nederlandse pensioenfondsen.
Zij vertegenwoordigt namens ongeveer 215 pensioenfondsen de belangen van:

- 5,3 miljoen deelnemers
- 3 miljoen gepensioneerden
- 9,1 miljoen gewezen deelnemers.

Het overgrote deel van alle werkenden is aangesloten bij een collectief pensioenfonds.

De leden van de Pensioenfederatie beheren samen circa 1200 miljard euro.

Contactinformatie
Prinses Margrietplantsoen 90
2595 BR Den Haag

Postbus 93158
2509 AD Den Haag

T + 31 (0)70 76 20 220
info@pensioenfederatie.nl
www.pensioenfederatie.nl

Pensioenfederatie,
Den Haag, september 2017

Inhoudsopgave

Inleiding

De bescherming van personen bij de verwerking van persoonsgegevens is een grondrecht. Nu hebben alle lidstaten van de Europese Unie (EU) eigen wetgeving op dit terrein, gebaseerd op een verouderde EU-richtlijn uit 1995. Zo geldt bijvoorbeeld in Nederland de Wet bescherming persoonsgegevens (Wbp). Dat gaat veranderen. Op 25 mei 2018 wordt de Algemene verordening gegevensbescherming (AVG) van toepassing en moet deze worden nageleefd. Vanaf die datum geldt dezelfde privacywetgeving in de hele EU.[1] De Wbp geldt dan niet meer.[2]

De AVG versterkt de positie van mensen van wie gegevens worden verwerkt. Zij krijgen nieuwe privacyrechten en hun bestaande rechten worden versterkt. Organisaties die persoonsgegevens verwerken, zoals pensioenfondsen en hun pensioenuitvoeringsorganisaties (hierna: PUO), krijgen meer verplichtingen. De Pensioenfederatie heeft in april 2017 een eerste servicedocument voor haar leden beschikbaar gesteld, waarin de nieuwe regels worden toegelicht.

Deze nadere guidance is opgesteld naar huidige inzichten en is bedoeld om pensioenfondsen en hun uitvoerders te helpen bij het interpreteren van de nieuwe privacywetgeving en bij de implementatie daarvan in de bedrijfsvoering. De Pensioenfederatie adviseert haar leden om nu al aan de slag te gaan met de AVG door een aanpak van 'richten, inrichten en verrichten': zorg voor bewustwording en beleid, pas waar nodig processen en systemen aan, maak goede afspraken met PUO's, en zie erop toe dat de nieuwe regels worden nageleefd.

Deze informatie is afgestemd met de Autoriteit Persoonsgegevens (AP). Meer algemene informatie over de stappen die organisaties nu al kunnen nemen om straks klaar te zijn voor de nieuwe privacywetgeving is te vinden op de website van de AP: https://autoriteitpersoonsgegevens.nl.

De Pensioenfederatie streeft ernaar om, in aanvulling op deze guidance, een door de AP goedgekeurde gedragscode te publiceren: de Gedragscode Verwerking Persoonsgegevens Pensioenfondsen. Leden van de Pensioenfederatie die de gedragscode onderschrijven en naleven houden zich dan aantoonbaar aan de wet.

1 De territoriale scope van de AVG omvat de EU-lidstaten plus Liechtenstein, Noorwegen en IJsland (de zogenoemde Europese Economische Ruimte ofwel EER).

2 De AVG laat op sommige punten bewust ruimte aan de lidstaten om nadere regels te stellen, alsmede om de op- en inrichting van de nationale toezichthouder te regelen. In Nederland zal dat gebeuren via de nog te publiceren Uitvoeringswet Algemene verordening gegegevensbescherming. De Nederlandse overheid kiest daarbij voor een beleidsneutrale uitvoering van de AVG. Het bestaande recht uit de Wbp wordt zoveel mogelijk gehandhaafd, tenzij dit in verband met de AVG niet mogelijk is.

1 Persoonsgegevens

Het begrip persoonsgegevens (artikel 4 AVG) omvat alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Voor pensioenfondsen gaat het om:

- aanspraak- en pensioengerechtigden;
- (ex)leden van fondsgremia;
- (oud)werknemers van het pensioenfonds of bestuursbureau;
- namen van werkgevers, niet zijnde rechtspersonen zoals eenmanszaken of VOF's, die verwijzen naar een natuurlijk persoon.

Gegevens van overleden personen zijn geen persoonsgegevens in de zin van de AVG. Uiteraard moeten pensioenfondsen en uitvoerders wel zorgvuldig met deze gegevens omgaan.

2 De verwerkingsverantwoordelijke en de verwerker

De verwerkingsverantwoordelijke (artikelen 4 en 24 AVG) is de entiteit die het doel van en de middelen voor de verwerking van persoonsgegevens bepaalt. De verwerker (artikelen 4 en 28 AVG) is de partij die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. De verwerker heeft een uitvoerende taak en heeft geen zeggenschap over de wijze van verwerken. In de praktijk is dit onderscheid echter diffuus. Zo kiezen verwerkers vaak zelf bijvoorbeeld welke software zij gebruiken of de wijze van archiveren. In deze gevallen geeft de doorslag wie het doel van de verwerking bepaalt. Het kan voorkomen dat meerdere partijen gezamenlijk verwerkingsverantwoordelijk zijn. Indien de verwerker toch het doel en middelen van de verwerking bepaalt dan wordt hij aangemerkt als verwerkingsverantwoordelijke. Hij dient dan zelf ook alle verplichtingen uit de AVG na te komen. Over het algemeen is het pensioenfonds de verwerkingsverantwoordelijke en de PUO de verwerker.

Een veel voorkomend misverstand is dat het pensioenfonds verwerker is voor de werkgever. Dat is niet het geval, omdat het pensioenfonds zelf doel en middelen van de verwerking bepaalt. Vanaf het moment dat de persoonsgegevens door de werkgever aan het pensioenfonds worden geleverd, op basis van de uitvoeringsovereenkomst of het uitvoeringsreglement, is het pensioenfonds de verwerkingsverantwoordelijke.

Derde partij wel of geen verwerker

Pensioenfondsen onderhouden met veel externe partijen een zakelijke relatie. Er zijn ten aanzien van uitbestedingspartners die persoonsgegevens verwerken drie categorieën te onderscheiden:

- uitbestedingspartners waar persoonsgegevens naar toe gestuurd worden, oftewel dat persoonsgegevens buiten de context van het pensioenfonds of PUO komen. In zo'n geval is een verwerkersovereenkomst vereist;
- uitbestedingspartners c.q. leveranciers die bij het pensioenfonds of PUO programmatuur neerzetten en toegang hebben tot persoonsgegevens. Dit is een schemergebied. De Pensioenfederatie adviseert om van geval tot geval risicogebaseerd te beoordelen of een verwerkersovereenkomst nodig is (en bij twijfel het zekere voor het onzekere te nemen en een verwerkersovereenkomst af te sluiten).

Hierna wordt van enkele veel voorkomende dienstverleners in de pensioensector aangegeven of die doorgaans verwerker zijn, of juist niet (omdat zij zelf verwerkingsverantwoordelijke zijn). Dit betreft een indicatie. Er kunnen omstandigheden zijn die er voor zorgen dat een derde partij in tegenstelling tot onderstaand overzicht juist wel of geen verwerker is. De Pensioenfederatie adviseert pensioenfondsen om per externe dienstverlener te bepalen of die beschouwd moet worden als verwerker in de zin van de AVG.

Dienstverlener	*Wel/geen verwerker*
Extern bestuursbureau	Wel verwerker
Pensioenuitvoeringsorganisatie (PUO)	Wel verwerker
Vermogensbeheerder	Geen verwerker, tenzij (bij bijvoorbeeld een individuele beschikbare premieregeling) wordt gewerkt met een niet geanonimiseerd[3] deelnemersbestand
Herverzekeraar	Geen verwerker, tenzij wordt gewerkt met een niet geanonimiseerd deelnemersbestand
Jaarrekening accountant	Geen verwerker
Certificerend actuaris	Geen verwerker
Adviserend actuaris	Wel verwerker, tenzij wordt gewerkt met een geanonimiseerd deelnemersbestand
Software leverancier	Geen verwerker
Gedetacheerde bij het pensioenfonds	Geen verwerker (zelfde regime als werknemers van het pensioenfonds)

3 Anonimisering van persoonsgegevens houdt in dat die gegevens niet meer herleidbaar zijn tot individuele personen, ook niet door koppeling met een ander (deel)bestand.

3 Garanties bij (onder)uitbesteding

Het pensioenfonds mag alleen een PUO (verwerker) inschakelen als het fonds afdoende garanties heeft dat de verwerker in staat is de verplichtingen uit de AVG na te komen (artikel 28 AVG). Dit om te voorkomen dat door het inschakelen van een derde de privacy van de aanspraak- en pensioengerechtigden (in de AVG: betrokkenen) onvoldoende worden gewaarborgd. De garanties moeten met name betrekking hebben op het gebied van deskundigheid, betrouwbaarheid en middelen zoals passende technische en organisatorische maatregelen op het gebied van gegevensbeveiliging. Om aan te tonen dat aan de gevraagde garanties wordt voldaan, kan de uitvoerder gebruik maken van een door de AP goedgekeurde gedragscode of certificeringsregeling. Op dit moment zijn deze nog niet bekend, maar gedacht kan worden aan bijvoorbeeld een ISAE-verklaring of ISO-certificering. Uiteraard moeten pensioenfondsen altijd controleren of dergelijke verklaringen en certificeringen in voldoende mate de dienstverlening dekken.

De verwerking door de PUO moet worden vastgelegd in een verwerkersovereenkomst (voorheen: bewerkersovereenkomst), die inhoudelijk moet voldoen aan de eisen van de AVG. De verwerkersovereenkomst hoeft geen afzonderlijk document te zijn, maar mag onderdeel uitmaken van de uitbestedingsovereenkomst tussen het pensioenfonds en de PUO.

De Europese Commissie en de AP kunnen standaardcontractbepalingen voor de verwerking opstellen. Die zijn er nog niet. Mochten die er wel komen, dan kunnen pensioenfondsen en PUO's zelf bepalen of zij daarvan gebruik willen maken.

In de praktijk maken PUO's vaak gebruik van andere dienstverleners die persoonsgegevens van het pensioenfonds verwerken, zoals bijvoorbeeld communicatieadviesbureaus of post verzendhuizen. Dergelijke onderuitbesteding door de PUO is alleen toegestaan als de verwerkingsbepalingen uit de verwerkersovereenkomst worden doorgegeven aan de subverwerker. Bovendien mag een PUO niet een subverwerker inschakelen zonder voorafgaande specifieke of algemene schriftelijke toestemming van het pensioenfonds. Als het pensioenfonds in de verwerkersovereenkomst een algemene toestemming voor de inschakeling van subverwerkers heeft gegeven, moet de PUO het pensioenfonds inlichten over een voorgenomen (wijzigingen in de) aanstelling van subverwerkers en het pensioenfonds de mogelijkheid bieden om daartegen bezwaar te maken. Zo wordt gewaarborgd dat het pensioenfonds als verwerkingsverantwoordelijke steeds overzicht houdt over de gehele keten van de verwerking van persoonsgegevens.

Meer informatie over de verwerkersovereenkomst is opgenomen in paragraaf 13.

4 Bewustwording

Het eerste dat het pensioenfonds (inclusief een eventueel bestuursbureau) en de PUO moeten organiseren is het vergroten van het bewustzijn over de nieuwe regels van de AVG bij beleidsmakers en medewerkers die persoonsgegevens verwerken. Gegeven het toenemende belang van data privacy is het raadzaam om dit onderwerp een afzonderlijk onderdeel te maken van de permanente educatie. Getrainde beleidsmakers en pensioenadministrateurs kunnen vervolgens de impact van de AVG op de gehele administratieve keten bepalen en aangeven waar aanpassingen nodig zijn. Implementatie van de AVG kan een groot beslag leggen op de organisatie in termen van beschikbaarheid van mensen en middelen. Om tijdig te voldoen aan de AVG is het zaak om samen met de PUO (s) de implementatie zo snel mogelijk projectmatig ter hand te nemen. PUO's zullen doorgaans uit een oogpunt van standaardisatie maatregelen voor alle pensioenfondsklanten op een uniforme manier willen inregelen.

5 Beginselen voor verwerking

De artikelen 5 en 6 van de AVG bevatten diverse algemene beginselen voor de verwerking van persoonsgegevens, dat wil zeggen het verzamelen en vervolgens bewerken, archiveren en vernietigen van persoonsgegevens.

Rechtmatigheid, behoorlijkheid en transparantie

De AVG schrijft voor dat persoonsgegevens moeten worden verwerkt op een wijze die rechtmatig, behoorlijk en transparant is. Voor aanspraak- en pensioengerechtigden moet inzichtelijk zijn waarom en op welke manier persoonsgegevens worden verwerkt. Het pensioenfonds moet hier helder en toegankelijk over communiceren in een zogenoemde privacyverklaring. Deze verklaring moet in duidelijke en eenvoudige taal worden opgesteld en mag dus niet lezen als een juridische disclaimer.

Verwerking van persoonsgegevens is alleen rechtmatig als aan een van de volgende grondslagen wordt voldaan:

a de aanspraak- of pensioengerechtigde heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens (zie ook paragraaf 13); een voorbeeld hiervan is toestemming voor het gebruik van tracking cookies op de website van het pensioenfonds;

b de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is (inclusief precontractuele maatregelen), zoals de pensioenovereenkomst tussen de werkgever en de werknemers;

c het pensioenfonds is wettelijk verplicht de verwerking uit te voeren; denk hierbij aan alle voorschriften uit de Pensioenwet, de Wet verplichte beroepspensioenregeling of fiscaal verplichte administratieve taken, en voor verplichtgestelde bedrijfstakpensioenfondsen aan de Wet BPF in combinatie met de verplichtstelling;

d de verwerking is noodzakelijk om de vitale belangen (lees: het leven) van de aanspraak- en pensioengerechtigden of andere personen te beschermen; deze grondslag zal bij pensioenfondsen niet snel voorkomen;

e verwerking is noodzakelijk voor een taak van algemeen belang of een publieke taak; deze grondslag zal bij pensioenfondsen niet snel voorkomen;

f een eigen gerechtvaardigd belang van het pensioenfonds of een derde, dat zwaarder weegt dan de grondrechten van de aanspraak- en pensioengerechtigden, zoals bijvoorbeeld fraudepreventie; er moet sprake zijn van een belangenafweging op basis van alle omstandigheden van het geval.

Een beroep op de gronden genoemd onder c en e moet terug te voeren zijn tot een specifieke wettelijke regeling in het Unierecht of het recht van een lidstaat dat op het pensioenfonds van toepassing is. Lidstaten mogen bij deze grondslagen nadere regels stellen.

Doelbinding

Gegevensverwerking mag alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden gebeuren. Een pensioenfonds moet die doeleinden concreet vaststellen en omschrijven voordat de verwerking begint. Een omschrijving als "wij verwerken uw persoonsgegevens voor onze doeleinden als pensioenfonds" is te algemeen. Het pensioenfonds dient een gegevensbeschermingsbeleid op te stellen en ervoor te zorgen dat persoonsgegevens worden verwerkt in overeenstemming met dat beleid.

Verdere verwerking van persoonsgegevens, voor een ander doel dan waarvoor ze oorspronkelijk werden verzameld, moet separaat gerechtigvaardigd kunnen worden als de verdere verwerking niet berust op toestemming of een wettelijke verplichting. De verwerking moet in ieder geval noodzakelijk zijn voor het doel dat wordt nagestreefd. Is dat niet het geval, dan is verdere verwerking niet toegestaan. Ook hier geldt dat deelnemers niet verrast mogen worden over de omgang van het pensioenfonds met hun persoonsgegevens. Het pensioenfonds moet hen altijd informeren over verdere verwerkingen en de rechten die betrokkenen hebben, zoals het recht om daartegen bezwaar te maken (zie ook paragraaf 6).

Minimale gegevensverwerking

Er moet sprake zijn van minimale gegevensverwerking. Dataminimalisatie betekent dat verwerking moet worden beperkt tot wat noodzakelijk is om de vastgestelde doeleinden te bereiken. Hiermee hangt samen dat persoonsgegevens ook zo snel mogelijk moeten worden geaggregeerd (als daarmee ook het doel kan worden gerealiseerd), geanonimiseerd en gewist. De opslagperiode van de persoonsgegevens moet tot een strikt minimum worden beperkt en er dienen termijnen te zijn voor het wissen of periodiek toetsen van de persoonsgegevens.

Juistheid

Het pensioenfonds moet er actief voor zorgen dat de verwerkte gegevens juist en actueel zijn en neemt daar alle redelijke maatregelen voor. Het is onvoldoende als een pensioenfonds een afwachtende houding aanneemt, waarbij foutieve gegevens alleen worden gecorrigeerd na klachten van deelnemers.

Opslagbeperking

Het beginsel van opslagbeperking betekent dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het bereiken van de gestelde doeleinden. Uiteraard moeten pensioenfondsen gegevens bewaren als daar een (andere) wettelijke verplichting voor is uit hoofde van bijvoorbeeld het Burgerlijk Wetboek, de Pensioenwet, de Wet verplichte beroepspensioenregeling of fiscale wetgeving.

Langere opslag van gegevens voor (louter) archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden mag, als voor passende waarborgen wordt gezorgd om de privacy van deelnemers te beschermen.

Integriteit en vertrouwelijkheid

Het beginsel van integriteit en vertrouwelijkheid brengt met zich mee dat het pensioenfonds ervoor zorgt dat door middel van passende technische en organisatorische beveiligingsmaatregelen ongeoorloofde toegang tot c.q. ongeoorloofd gebruik van persoonsgegevens wordt voorkomen.

Verantwoordingsplicht

Het pensioenfonds is verantwoordelijk voor de naleving van deze beginselen en moet dat ook kunnen aantonen (de zogenoemde verantwoordingsplicht). Dit betekent een omgekeerde bewijslast; als het pensioenfonds niet kan aantonen dat aan de beginselen uit de AVG wordt voldaan, dan kan de AP een boete opleggen.

Samengevat moet een pensioenfonds actief zorgdragen voor een transparant privacybeleid, adequate implementatie, monitoring, evaluatie en registratie, en indien nodig actualisatie van het beleid en de uitvoering daarvan.

6 Rechten van betrokkenen

Aanspraak- en pensioengerechtigden (in de AVG: de betrokkenen) krijgen meer en verbeterde privacyrechten, die hierna worden toegelicht (artikelen 12 tot en met 23 AVG).

Recht van inzage

Dit recht bestaat al onder de Wbp. De betrokkene heeft het recht om te vragen of zijn persoonsgegevens worden verwerkt. Als zijn persoonsgegevens worden verwerkt dan heeft hij recht om te weten welke gegevens dat zijn en heeft hij het recht een kopie van deze persoonsgegevens op te vragen. Het pensioenfonds moet bij een dergelijk verzoek de volgende zaken melden:

- welke persoonsgegevens worden verwerkt, bijv. de daadwerkelijke naam, adres, geslacht, geboortedatum, burgerservicenummer (BSN) etc. zoals die in de administratie staan;
- de verwerkingsdoeleinden en grondslag; waarom worden de gegevens verwerkt en op basis van welke grondslag. Bij pensioenfondsen zal dat vaak zijn omdat verwerking noodzakelijk is om de pensioenregeling die arbeidsrechtelijk geldt tussen de werkgever en de werknemers, uit te voeren;
- welke categorieën van persoonsgegevens worden verwerkt; bijv. salarisgegevens;
- hoe lang de gegevens worden verwerkt; bijvoorbeeld zo lang het nodig is om de pensioenregeling goed uit te voeren of om vast te stellen of het pensioenfonds nog verplichtingen heeft;
- welke rechten de betrokkene heeft ten aanzien van zijn persoonsgegevens; er moet expliciet worden gewezen op het recht op inzage, het recht op rectificatie, het recht op wissen, het recht op beperking, het recht op bezwaar en het recht op dataportabiliteit;
- het recht om (na het doorlopen van de interne klachtenprocedure) een klacht in te dienen bij de AP;
- als de gegevens niet van de betrokkene zelf zijn verkregen moet gemeld worden van wie de gegevens zijn verkregen; denk aan de werkgever, de Basisregistratie Personen (BRP) of het Uitvoeringsinstituut werknemersverzekeringen (UWV);
- als er sprake is van geautomatiseerde besluitvorming, dat wil zeggen geautomatiseerde verwerking van persoonsgegevens zonder menselijke interventie, dan moet worden gemeld om welke besluitvorming (computeranalyse) het gaat en welke gevolgen dit kan hebben;
- als er sprake is van doorgifte buiten de EU, dan moet worden aangegeven welke waarborgen er zijn genomen om de privacy van de betrokkene te beschermen.

De gegevens moeten in een gangbare elektronische vorm worden verstrekt, tenzij het verzoek op papier is gedaan of er expliciet om een papieren kopie

wordt gevraagd. De inzage is kosteloos, tenzij er meerdere kopieën worden opgevraagd. Dan mogen redelijke administratiekosten in rekening worden gebracht.

Bij het geven van inzage moet goed rekening gehouden worden met de rechten van anderen dan de betrokkene. De persoonsgegevens van derden, zoals bijvoorbeeld de partner of de ex-partner, mogen (behoudens expliciete toestemming daartoe) niet worden verstrekt.

Pensioenfondsen zullen dus een procedure moeten hebben om te voldoen aan dit recht van inzage.

Recht op rectificatie

Dit recht bestaat al onder de Wbp. Als de persoonsgegevens niet juist zijn dan heeft de betrokkene het recht om deze te wijzigen of aan te vullen. Als de betrokkene terecht een beroep doet op dit recht dan moet het pensioenfonds volgens de AVG iedere ontvanger van de gegevens, zoals bijvoorbeeld de belastingdienst, het UWV en subverwerkers, hiervan op de hoogte stellen.

Recht op wissen

Dit is een nieuw recht onder de AVG. De betrokkene heeft het recht om de gegevens te laten wissen als:

- de persoonsgegevens niet meer nodig zijn voor de doelen waarvoor deze zijn verzameld of verwerkt (in welk geval het pensioenfonds – behoudens wettelijke bewaartermijnen – ook al zelf verplicht is om de gegevens te vernietigen);
- de betrokkene zijn eerder verstrekte toestemming voor de verwerking intrekt of tegen de verwerking op terechte gronden bezwaar aantekent (en er geen andere rechtsgrond voor de verwerking is);
- de persoonsgegevens onrechtmatig zijn verwerkt;
- de persoonsgegevens dienen te worden gewist op basis van Europese of nationale wetgeving;
- de persoonsgegevens zijn verwerkt in het kader van leveren van diensten aan kinderen die jonger dan 16 jaar zijn.

Dit recht zal voor pensioenfondsen niet vaak van toepassing zijn, behalve wanneer de gegevens ten onrechte in de pensioenadministratie zijn opgenomen of profilering zoals bedoeld in de AVG (zie ook paragraaf 16) plaatsvindt. Het wissen moet kosteloos en zo snel mogelijk, doch in ieder geval binnen een maand, plaatsvinden. Als gegevens gewist worden dan moet het pensioenfonds dat doorgeven aan derden die de gegevens hebben verkregen van het pensioenfonds.

Recht op beperking

Dit is een nieuw recht onder de AVG. De betrokkene heeft het recht de verwerking te beperken in vier situaties:

- de juistheid van de gegevens worden betwist en het pensioenfonds moet dat controleren;
- de verwerking is onrechtmatig en de betrokkene verzet zich tegen wissen, maar wenst een beperking. Dit kan bijvoorbeeld het geval zijn als iemand op een 'zwarte lijst' wil staan om toekomstige verwerkingen te voorkomen;
- het pensioenfonds heeft de gegevens niet meer nodig, maar de betrokkene wel, bijvoorbeeld voor het voeren van een rechtszaak tegen het pensioenfonds of derden;
- als de betrokkene bezwaar heeft gemaakt tegen een verwerking waarop het pensioenfonds niet meteen beslist, dan kan de betrokkene een beperking verlangen.

Beperking houdt in dat de gegevens niet verwerkt mogen worden tenzij:

- er sprake is van louter opslag van gegevens;
- de betrokkene toestemming heeft gegeven;
- verwerking gebeurt ten behoeve van een rechtsvordering (bijvoorbeeld tegen de betrokkene), de bescherming van de rechten van andere personen of om gewichtige redenen van algemeen belang voor de Europese Unie of een lidstaat.

Als de beperking wordt opgeheven, moet de betrokkene hierover worden geïnformeerd. In de praktijk betekent beperking dat de betreffende gegevens separaat moeten worden opgeslagen of moeten worden geoormerkt als gegevens waarop een beperking ligt.

Recht op dataportabiliteit

Dit is een nieuw recht onder de AVG. Het recht op dataportabiliteit (overdraagbaarheid van gegevens) houdt in dat de betrokkene het recht heeft om zijn persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm te ontvangen en deze ongehinderd aan een andere verwerkingsverantwoordelijke over te dragen. Een pensioenfonds is niet verplicht om technisch compatibele systemen op te zetten of te gebruiken, maar als het technisch mogelijk is kan de betrokkene op grond van de AVG het pensioenfonds ook vragen om zijn persoonsgegevens rechtstreeks aan een andere verwerkingsverantwoordelijke over te dragen.

Het doel van dit nieuwe recht is om betrokkenen meer controle over hun gegevens te geven en het voor hen gemakkelijker te maken van dienstverlener te wisselen.

Het recht op dataportabiliteit is alleen van toepassing op verwerkingen die op basis van geautomatiseerde procedés worden verricht. Bovendien moet het gaan om persoonsgegevens die met toestemming van de betrokkene of op basis van een overeenkomst met de betrokkene, worden verwerkt. Als een pensioenfonds persoonsgegevens verwerkt op basis van een andere

grond, bijvoorbeeld een eigen gerechtvaardigd belang, bestaat geen recht op dataportabiliteit.

Dit nieuwe recht is nauw verbonden met het recht op inzage, maar verschilt hier ook van. Bij het recht op inzage kiest het pensioenfonds de vorm waarin de gevraagde informatie wordt geleverd. Bij het recht op dataportabiliteit is de verstrekkingsvorm wettelijk vastgelegd. Dataportabiliteit leidt niet automatisch tot de verwijdering van de gegevens uit de systemen van het pensioenfonds.

Afgeleide gegevens, dat wil zeggen gegevens die een pensioenfonds zelf genereert door bijvoorbeeld data-analyse hoeven bij dataportabiliteit niet te worden verstrekt. Bij het recht op inzage moeten wel alle persoonsgegevens worden verstrekt.

De vraag is in hoeverre het recht van dataportabiliteit van toepassing zal zijn in de relatie pensioenfonds – deelnemer gezien de verplichting om pensioen af te nemen bij het pensioenfonds. Bij vrijwillige producten van pensioenfondsen zou dit recht wel een rol kunnen spelen. De praktijk zal dit moeten uitwijzen.

Recht van bezwaar

De betrokkene heeft het recht om bezwaar te maken tegen het verwerken van zijn gegevens als er sprake is van verwerking op basis van de grondslag ‘taak van algemeen belang’ of ‘gerechtvaardigd belang’. In dit geval heeft het pensioenfonds een algemene belangenafweging gemaakt op basis waarvan het rechtmatig de gegevens verwerkt. Als de betrokkene van mening is dat in zijn specifieke situatie een andere belangenafweging nodig is dan heeft hij het recht dit aan te geven. In principe zal de verwerking dan gestaakt moeten worden, tenzij het pensioenfonds kan aantonen dat de belangen van het pensioenfonds boven die van de betrokkene gaan.

Bij pensioenfondsen zal van dit recht niet snel gebruik gemaakt kunnen worden, omdat die in beginsel niet de grondslag ‘taak van algemeen belang’ of ‘gerechtvaardigd belang’ gebruiken voor gegevensverwerking (zie ook paragraaf 4). Er zijn wel situaties denkbaar, bijvoorbeeld als belangrijke informatie vanuit de werkgever via het pensioenfonds naar gewezen deelnemers wordt verspreid (omdat die groep niet op een andere wijze dan via het pensioenfonds kan worden bereikt).

Het recht van bezwaar geldt niet bij de grondslag ‘toestemming’ omdat die altijd kan worden ingetrokken.

Algemene vereisten ten aanzien van de rechten van betrokkene

Er zijn algemene vereisten die gelden voor alle rechten van betrokkenen:

- een beroep op een recht moet in beginsel binnen een maand worden uitgevoerd. Indien dat niet lukt, dan moet in ieder geval binnen een maand worden gemeld waarom het niet lukt en kan de termijn met maximaal twee maanden worden verlengd;
- als een verzoek niet wordt gehonoreerd, dan wordt dit binnen een maand meegedeeld met de reden van weigering en informatie over de mogelijkheid om een klacht in te dienen bij de AP en beroep in te stellen bij de rechter;
- er zal moeten worden vastgesteld dat de betrokkene zelf het recht inroept, oftewel identificatie. Dit kan echter geen grond zijn om het verzoek af te wijzen. Het pensioenfonds zal dan aanvullende informatie moeten opvragen om de identiteit vast te stellen. Overigens hoeft de identificatie niet per se plaats te vinden met een identiteitsbewijs. Ook inloggen op een account in een digitaal portaal kan als identificeren dienen;
- het inroepen van alle rechten is in beginsel kosteloos;
- als een verzoek kennelijk ongegrond of buitensporig is mag het pensioenfonds hetzij redelijke kosten vragen voor het inwilligen van het verzoek of het verzoek weigeren.

7 Privacyverklaring

Pensioenfondsen zijn verplicht om aanspraak- en pensioengerechtigden te informeren over de verwerking van hun persoonsgegevens (artikel 12 AVG). In ieder geval moet op de website van het pensioenfonds een privacyverklaring (of privacy statement) worden opgenomen.

Onder de huidige Wbp worden maar minimale eisen aan een privacyverklaring gesteld. De zogenoemde artikel 29 Werkgroep, het Europese verband van privacytoezichthouders, heeft wel een aanbeveling gedaan op een aantal vaste onderwerpen die in ieder geval in een privacyverklaring opgenomen zouden moeten worden [4].

4 advies 5020/01/EN/Final; WP43, d.d. 17 mei 2001

In de AVG worden scherpere eisen gesteld aan de informatieplicht en daarmee aan de privacyverklaring. Deze worden hieronder toegelicht.

De privacyverklaring wordt gezien als een eenzijdige overeenkomst. Een pensioenfonds kan dus door deelnemers en pensioengerechtigden worden gehouden aan hetgeen in die verklaring wordt beloofd.

Transparantie

Met de AVG wordt als gevolg van versterking en vernieuwing van de rechten van betrokkenen het transparantiebeginsel in de wet geïntroduceerd. Dit nieuwe begrip komt in de plaats van het onder de Wbp gebruikte begrip 'zorgvuldig'. Het beginsel dat persoonsgegevens op een manier worden verwerkt die transparant is, houdt in dat deelnemers duidelijk geïnformeerd moeten worden over dat en hoe hun persoonsgegevens verzameld, gebruikt, geraadpleegd of op een andere manier verwerkt worden, waarom en door wie. Voor de privacyverklaring betekent dit:

- in heldere taal; de informatie aan deelnemers en daarmee de privacyverklaring moet beknopt, begrijpelijk, duidelijk, eenvoudig en gemakkelijk toegankelijk zijn (bijvoorbeeld via machineleesbare iconen);
- onderwerpen; in een privacyverklaring moet de volgende informatie staan:
  1. contactgegevens: wie ben jij (het pensioenfonds of de PUO) en hoe kunnen betrokkenen contact opnemen met het pensioenfonds of de PUO en (indien van toepassing) de functionaris voor de gegevensbescherming (FG)?;
  2. waarom worden persoonsgegevens verzameld en waarom mag dat (doel en rechtsgrond van de verwerking van de persoonsgegevens)?;
  3. wat zijn de gerechtvaardigde belangen van het pensioenfonds of de PUO (of door hen ingeschakelde derden) voor de gegevensverwerking, als dat de rechtsgrond van de verwerking is?;

4 aan wie worden de persoonsgegevens verder nog verstrekt (ontvangers of categorieën van ontvangers)?;
5 zijn betrokkenen verplicht om de gevraagde persoonsgegevens te verstrekken of niet? En wat zijn de gevolgen als een betrokkene de persoonsgegevens niet verstrekt (noodzaak)?;
6 waar en hoe kan de betrokkene vragen om inzage, rectificatie, wissen of overdracht van persoonsgegevens, klachten indienen, bezwaar maken of een verwerking beperken?;
7 hoe kan een betrokkene een verleende toestemming intrekken?;
8 hoe lang verwacht het pensioenfonds de persoonsgegevens te gaan bewaren?;
9 als persoonsgegevens buiten de EU verwerkt gaan worden, welke waarborgen zijn er getroffen dat de persoonsgegevens in dat derde land conform de AVG worden verwerkt en passend beveiligd zijn?;
10 doet het pensioenfonds aan geautomatiseerde besluitvorming (computergestuurde verwerking van persoonsgegevens zonder menselijke tussenkomst, bijvoorbeeld profilering)? En zo ja, welke logica wordt daarvoor gebruikt?;
11 maakt het pensioenfonds gebruik van zogenoemde cookies, welke persoonsgegevens worden dan verzameld, waarom en op welke wijze? Een pensioenfonds kan specifieke informatie hierover ook in een afzonderlijke cookieverklaring opnemen en enkel daarnaar verwijzen in de privacyverklaring.

Model privacyverklaring

Een pensioenfonds of PUO kan zelf een privacyverklaring opstellen of laten opstellen door een gespecialiseerde dienstverlener zoals bijvoorbeeld een ICT-recht advocaat of data privacy jurist. In de (online)markt zijn verschillende voorbeelden van privacyverklaringen beschikbaar. De Pensioenfederatie adviseert pensioenfondsen en PUO's wel om bij gebruik daarvan de uiteindelijke tekst altijd zelf te controleren en waar nodig aan te passen aan de eigen specifieke situatie.

8 Register verwerkingsactiviteiten

Pensioenfondsen moeten een register (artikel 30 AVG) aanhouden waarin in ieder geval wordt gedocumenteerd:

- naam en contactgegevens van het pensioenfonds, en van een eventueel aangestelde Functionaris Gegevensbescherming (FG). Als er een andere focal point voor de bescherming van persoonsgegevens in de organisatie is aangewezen, is het raadzaam om diens contactgegevens in het register op te nemen;
- de verwerkingsdoeleinden. Alhoewel het strikt genomen niet nodig is om de (juridische) grondslag voor de verwerking in het register te vermelden, is dat wel raadzaam. Grondslagen zijn in de AVG opgesomd (zie ook paragraaf 4);
- beschrijving van de categorieën van aanspraak- en pensioengerechtigden en van de persoonsgegevens;
- met welke partijen de gegevens (zowel binnen als buiten de EU) worden gedeeld;
- de termijnen waarbinnen de gegevens worden gewist;
- een korte beschrijving van de genomen technische en organisatorische beveiligingsmaatregelen.

Ook PUO's en hun subverwerkers moeten een soortgelijk register aanhouden, waarin per pensioenfonds inzichtelijk is welke categorieën verwerkingen voor het pensioenfonds worden uitgevoerd. Deze registers kunnen als input dienen voor één gezamenlijk overzicht van verwerkingen dat door het pensioenfonds wordt gehouden.

De registers moeten op verzoek aan de AP worden verstrekt. Dit betekent dat – anders dan onder de huidige Wbp – verwerkingen niet meer uit eigen beweging hoeven te worden gemeld.

De registers dienen als bewijs dat pensioenfondsen en PUO's de AVG naleven. Om die reden moeten de registers schriftelijk worden vastgelegd. Dat kan ook in elektronische vorm (database).

De registers zijn niet alleen verplicht op grond van de AVG, ze zijn ook handig om te kunnen voldoen aan andere verplichtingen uit de AVG, zoals het tijdig en volledig kunnen bedienen van aanspraak- en pensioengerechtigden die gebruik maken van hun rechten op inzage, correctie of verwijdering van hun persoonsgegevens.

9 Privacy impact assessment (PIA)

Artikel 35 AVG introduceert voor verwerkingsverantwoordelijken de nieuwe verplichting van een gegevensbeschermingseffectbeoordeling, ook wel Privacy Impact Assessment (PIA) genoemd. Een PIA is een instrument om vooraf de (bruto) privacyrisico's van een gegevensverwerking in kaart te brengen, om vervolgens maatregelen te kunnen nemen om die risico's te minimaliseren (waarna een netto risico overblijft).

Organisaties hoeven niet voor elke gegevensverwerking een PIA uit te voeren. Een PIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen. Dat is in ieder geval zo als een organisatie:

- systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profiling;
- op grote schaal bijzondere persoonsgegevens verwerkt;
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Buiten deze drie situaties geeft de AVG geen overzicht van verwerkingen met een hoog risico.

De werkgroep van Europese privacytoezichthouders (de zogenoemde WP 29) heeft voorschriften gepubliceerd over wanneer en hoe organisaties een PIA moeten uitvoeren. Daarbij zijn tien criteria opgesteld om het risico te bepalen. De AP zal een lijst van verwerkingen publiceren waarvoor een PIA verplicht is. Hierin kunnen ook verwerkingen vermeld worden waarvoor geen PIA vereist is.

Als verwerkingen niet voorkomen op de lijst van de AP, moet een organisatie zelf bepalen of een verwerking waarschijnlijk een hoog privacyrisico oplevert. Bij deze beoordeling kan gebruik gemaakt worden van de tien criteria die de WP 29 heeft opgesteld. Alle tien de criteria kunnen voor pensioenfondsen en PUO's van belang zijn. Als vuistregel kan gehanteerd worden dat als een verwerking aan ten minste twee criteria voldoet, een PIA uitgevoerd moet worden.

1 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. Een voorbeeld is het volgen van bezoekers van een website en op basis daarvan profielen van deze personen opstellen.

2 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 personen worden uitgesloten of achtergesteld, in welk geval de verwerking niet mag plaatsvinden.

3 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. Betrokkenen kunnen zich niet in openbare ruimten aan deze gegevensverwerking onttrekken.

4 Gevoelige gegevens
Het gaat hierbij in ieder geval om wat de AVG bijzondere categorieën van persoonsgegevens noemt, zoals informatie over iemands gezondheid (denk aan een arbeidsongeschiktheidspercentage), politieke voorkeuren of lidmaatschap van een vakbond. Ook strafrechtelijke gegevens vallen hieronder. Tot slot gaat het hier ook om gegevens die over het algemeen als privacygevoelig worden beschouwd, zoals iemands burgerservicenummer (BSN), gegevens over elektronische communicatie, locatiegegevens en financiële gegevens zoals een bankrekeningnummer.

5 Grootschalige gegevensverwerkingen
De AVG geeft geen definitie van 'grootschalige gegevensverwerkingen'.
WP 29 adviseert om met de volgende criteria te bepalen of hiervan sprake is:
- de hoeveelheid mensen van wie gegevens worden verwerkt;
- de hoeveelheid gegevens en/of de verscheidenheid aan gegevens die worden verwerkt;
- de tijdsduur van de gegevensverwerking;
- de geografische reikwijdte van de gegevensverwerking.

6 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.

7 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 gaan.

8 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 gebruiken, met mogelijk grote privacyrisico's. Een PIA helpt dan om de risico's te begrijpen en te verhelpen. Denk hierbij voor pensioenfondsen aan blockchain toepassingen in de pensioenadministratie of de introductie van nieuwe apps.

9 Doorgifte van persoonsgegevens buiten de EU

De bescherming van persoonsgegevens is niet in alle landen hetzelfde geregeld. Buiten de EU is het daarom niet zeker dat een land voldoende bescherming biedt.

10 Blokkering van een recht, dienst of contract

Het gaat hierbij om gegevensverwerkingen die tot gevolg hebben dat betrokkenen een recht niet kunnen uitoefenen, dat zij een dienst niet kunnen gebruiken of dat zij een contract niet kunnen afsluiten.

Een PIA hoeft niet uitgevoerd te worden als de gegevensverwerking:

- waarschijnlijk geen hoog privacyrisico oplevert;
- sterk lijkt op een andere gegevensverwerking waarvoor al een PIA is uitgevoerd;
- wordt geregeld door een andere Europese of nationale wet en er bij de totstandkoming van deze wet al een PIA is uitgevoerd, tenzij de privacytoezichthouder oordeelt dat er toch een PIA nodig is;
- op een lijst van de AP staat van verwerkingen waarvoor een PIA niet verplicht is.

Een PIA moet uitgevoerd worden voor nieuwe verwerkingen per 25 mei 2018. Als een bestaande gegevensverwerking na 25 mei 2018 hetzelfde blijft, hoeft geen PIA te worden uitgevoerd. Als het privacyrisico van een verwerking verandert, kan het verplicht zijn alsnog een PIA uit te voeren. Risico's kunnen bijvoorbeeld veranderen omdat een onderdeel van het verwerkingsproces wijzigt. Als een nieuwe technologie gebruikt gaat worden of als persoonsgegevens voor een ander doel worden gebruikt dan waarvoor ze oorspronkelijk zijn verwerkt, dan geldt de verplichting tot het uitvoeren van een PIA wel.

Een verplichting voor een PIA kan ook voortvloeien uit een verandering in de organisatie of als de maatschappelijke context verandert. Een voorbeeld hiervan is als gegevens worden doorgegeven aan een land dat de EU heeft verlaten. Stelregel is om na maximaal 3 jaar (vanaf 25 mei 2018) een nieuwe (of eerste) PIA uit te voeren (periodiek proces). Ook als het gaat om een bestaande gegevensverwerking van vóór 25 mei 2018 waarop ook nadien nooit een PIA is uitgevoerd, is het toch aan te raden om uiterlijk 3 jaar na deze datum alsnog een PIA uit te voeren.

Het is aan te bevelen om zo vroeg mogelijk, het beste al in de ontwerpfase, te starten met een PIA. Voordeel is dat daarmee tegelijk aan de wettelijk vereiste principes van privacy by design en privacy by default (zie ook paragraaf 8) kan worden voldaan. Het is verplicht om advies over een PIA in te winnen bij de Functionaris Gegevensbescherming (FG) als die aanwezig is. In het rapport over de PIA moet vermeld worden wat de FG heeft geadviseerd en wat met dat advies is gedaan. Als het pensioenfonds of de PUO niet formeel een FG heeft aangesteld, maar wel een 'gewone' privacy officer, dan is het raadzaam om de privacy officer ten aanzien van de PIA dezelfde rol als een FG te geven.

Als een PIA wordt gedaan, dan hoeft een pensioenfonds dat niet zelf te doen. De PIA kan ook worden gedaan door iemand binnen of buiten de organisatie. Het pensioenfonds blijft wel eindverantwoordelijk. De uitvoerder moet het pensioenfonds ondersteunen bij het uitvoeren van de PIA en de informatie verstrekken die het pensioenfonds nodig heeft.

Als het nodig is, moeten de aanspraak- en pensioengerechtigden om hun mening worden gevraagd. (Ter bepaling van de noodzaak hiervan doen fondsen die een functionaris gegevensbescherming of privacy officer hebben aangesteld er goed aan in deze diens advies te vragen.) De navraag kan plaatsvinden via de vertegenwoordigers van de aanspraak- en pensioengerchtigden in het VO/BO door middel van een vragenlijst of een intern of extern onderzoek. Als de uiteindelijke beslissing van het pensioenfonds over een bepaalde gegevensverwerking afwijkt van de mening van de betrokkenen moeten de redenen gedocumenteerd worden.

Er is geen standaardmethode voor een PIA. Een PIA moet in ieder geval het volgende bevatten:

- een systematische beschrijving van de beoogde gegevensverwerkingen en de doeleinden hiervan. Als de verwerkingsgrondslag die van 'gerechtvaardigd belang' is, moet dat ook worden vermeld;
- een beoordeling van de noodzaak (is het verwerken van persoonsgegevens op deze manier noodzakelijk om het doel te bereiken) en de proportionaliteit (is de inbreuk op de privacy niet onevenredig in verhouding tot het doel) van de verwerkingen;
- een beoordeling van de privacyrisico's voor de betrokkenen;
- de beoogde maatregelen om (1) de risico's aan te pakken (zoals waarborgen en veiligheidsmaatregelen) en (2) aan te tonen dat aan de AVG wordt voldaan.

Een handreiking voor de uitvoering van een PIA is te vinden op de website van de beroepsorganisatie van IT-auditors (NOREA). Het is niet verplicht de uitkomsten van een PIA te publiceren.

Op zich moet voor elke hoog risico gegevensverwerking vooraf een PIA plaatsvinden. Het is echter toegestaan om één PIA te doen op een administratie die de facto bestaat uit meerdere (specifieke) verwerkingen. Ook kunnen verschil-

lende generieke gegevensverwerkingen zo met elkaar verbonden zijn dat je die met één PIA kan afdoen. Zo volstaat één PIA voor bijvoorbeeld een deelnemersadministratie van een pensioenfonds met verschillende processen voor bijvoorbeeld pensioenopbouw, pensionering, afkoop, waardeoverdracht, gegevensverstrekking aan het Pensioenregister enzovoort.

Als het niet lukt om maatregelen te vinden voor het beperken van hoge privacyrisico's, dan moet voordat met de verwerking wordt gestart eerst de AP geraadpleegd worden.

10 Privacy by design & privacy by default

Privacy by design

Privacy by design (artikel 25 AVG) houdt in dat de bij de verwerking gehanteerde mechanismen en systemen zo zijn ontworpen dat zoveel als mogelijk rekening wordt gehouden met de privacy van de deelnemers en de AVG. De aandacht voor privacy blijft tijdens de gehele levensduur van het systeem bestaan. Onderdeel hiervan is het minimaliseren van gegevens van betrokkenen (alleen de gegevens verwerken die je nodig hebt voor de pensioenuitvoering) en het goed beveiligen van de gegevens. Dat kan bijvoorbeeld door autorisaties en het zo snel als mogelijk pseudonimiseren van gegevens.

Bij pseudonimisering wordt een gegevensbestand in tweeën gedeeld, waarbij bijvoorbeeld met het klantnummer van de deelnemer de koppeling tussen de bestanden kan worden gemaakt. Het eerste deelbestand bevat gegevens waarmee een deelnemer direct kan worden geïdentificeerd, zoals NAW-gegevens, telefoonnummer, e-mailadres of BSN-nummer. Het tweede deelbestand bevat gegevens die alleen indirect iets over de deelnemer zeggen, zoals voorkeuren of antwoorden op een enquête. Doel van deze 'bestandsknip' is dat de privacy van de deelnemer beter wordt beschermd in die gevallen waarin direct identificerende gegevens niet nodig zijn voor het doel dat met de verwerking wordt nagestreefd.

De PUO mag beide deelbestanden beheren, mits die maar afzonderlijk worden bewaard. Mocht de pseudonimisering ondanks passende technische en organisatorische waarborgen niet goed werken of onbevoegd ongedaan worden gemaakt, dan is sprake van een datalek dat bij de AP moet worden gemeld. Overigens kan een datalek als incident ook DNB meldingsplichtig zijn.

De Pensioenfederatie adviseert om in een testomgeving, bijvoorbeeld bij interne waardeoverdrachten en aanpassingen in systemen en applicaties, de persoonsgegevens zoveel als mogelijk te pseudonimiseren.

Let op! Pseudonimisering is wat anders dan anonimisering. Bij pseudonimisering is nog steeds sprake van persoonsgegevens in de zin van de AVG. Pas als geen koppeling meer gemaakt kan worden met direct identificerende gegevens, bijvoorbeeld door voor het tweede deelbestand het klantnummer van de deelnemer te verwijderen, zijn de gegevens echt geanonimiseerd. De AVG is dan niet meer van toepassing.

Privacy by default

Privacy by default (artikel 25 AVG) is het zodanig instellen van standaardinstellingen dat de privacy zoveel als mogelijk wordt gewaarborgd. Bij pensioenfondsen

is dit met name van belang bij online deelnemersportalen en bulk communicatie-activiteiten die verder gaan dan wat de Pensioenwet en de Wet verplichte beroepspensioenregeling voorschrijven. Insteek moet zijn geen opt-out regime, maar opt-in: pas als een deelnemer zich ergens voor heeft aangemeld ontvangt hij informatie (opt-in), in plaats van het automatisch ontvangen van informatie totdat het wordt stopgezet (opt-out). Enkele voorbeelden van wat niet conform privacy by default is:

- vooraf ingevulde velden bij (digitale) formulieren zoals "ik wil op de hoogte gehouden worden", waarbij de deelnemer een actieve handeling moet verrichten om de informatie niet (ongevraagd) te ontvangen;
- vragen om gegevens zoals geboortedatum en telefoonnummer als dat niet relevant is, bijvoorbeeld bij het abonneren op een nieuwsbrief van het pensioenfonds;
- in algemene voorwaarden of een privacy statement opnemen dat gegevens van deelnemers standaard met derden worden gedeeld;
- het automatisch via een deelnemersportaal inloggen op en koppelen met andere websites;
- app's die bij het installeren adresboeken kopiëren, en je overal volgen (locatie doorgeven) zonder dat de deelnemer hiervoor expliciet eerst toestemming heeft gegeven.

Er bestaat de mogelijkheid om aan te sluiten bij goedgekeurde certificeringsmechanismes, zoals bijvoorbeeld ISAE (COS) 3000 (assurance over niet-financiële informatie) en ISO/IEC (informatiebeveiligingsnormen), om aan te tonen dat wordt voldaan aan de principes privacy by design en privacy by default.

11 Functionaris voor gegevensbescherming

Algemeen

Pensioenfondsen moeten rondom de verwerking van persoonsgegevens een beheerste en integere bedrijfsvoering organiseren. Hoe dat gebeurt is afhankelijk van de doeleinden van de verwerking, het type van persoonsgegevens dat wordt verwerkt en de wijze waarop het pensioenfonds is georganiseerd. Onderdeel hiervan kan zijn het aanstellen van een zogenoemde functionaris voor de gegevensbescherming (FG). Op basis van de artikelen 37 tot en met 39 AVG is er strikt juridisch gezien geen eenduidige uitspraak mogelijk of pensioenfondsen en hun PUO's een FG moeten aanstellen. Het is echter raadzaam dat pensioenfondsen en PUO's iemand in de organisatie aanwijzen, die zich bekwaamt in het onderwerp, alles weet van privacyregels, toezicht houdt op de naleving daarvan, de organisatie adviseert over privacyvraagstukken en gedrag en cultuur bewaakt. Deze privacy officer (PO) kan desgewenst of indien dat in de gegeven omstandigheid wettelijk verplicht is, ook formeel als een FG in de zin van de AVG worden aangewezen. De rol van PO kan ook worden belegd binnen een team van privacyspecialisten (IT, Finance, Actuariaat enzovoort).

Pensioenfondsen verschillen nogal in de manier waarop zij zijn georganiseerd. Sommige fondsen doen de pensioenadministratie en de bestuursondersteuning in huis, terwijl andere fondsen geen werknemers in dienst hebben en alle taken hebben uitbesteed aan een externe dienstverlener. De AVG laat ruimte aan organisaties hoe de rol van FG (en daarmee dus ook die van 'gewone' PO) wordt vormgegeven. Grofweg kan een pensioenfonds zich langs de volgende lijnen organiseren:

1 aanstelling van een PO/FG in het eigen bestuursbureau (of contractueel ingehuurd). Dit format ligt in de rede als een belangrijk deel van de gegevensverwerking in huis gebeurt, dan wel dat er meerdere pensioenadministrateurs zijn aangesteld en een centrale 'line of sight' over de diverse gegevensverwerkingen vanuit het pensioenfonds onontbeerlijk is;
2 afspraak in de verwerkersovereenkomst met de PUO dat die een PO/FG-functie inricht met de taken conform de AVG. De PO/FG is in dienst van de PUO. Als er een FG is staat die als zodanig ingeschreven bij de AP;
3 afspraak in de verwerkersovereenkomst met de PUO over de aanstelling van een PA/FG zoals hierboven onder 2 aangeven, waarbij expliciet wordt overeengekomen dat de FG niet alleen als FG van de PUO maar ook als FG van het pensioenfonds wordt ingeschreven. In deze variant is het wel zaak om contractueel en organisatorisch goed te borgen dat de FG niet in een situatie van een belangenconflict tussen het pensioenfonds en de PUO terecht kan komen, want dat is volgens de AVG niet toegestaan.

Het is hoe dan ook raadzaam dat het pensioenfonds met de PUO(s) over dit

onderwerp in gesprek gaat en een opzet wordt gekozen die voor het pensioenfonds en de PUO werkt.

FG in de AVG

De FG is onder de AVG een zeer belangrijke functionaris die er voor moet zorgen dat organisaties de bepalingen van de AVG naleven. Let wel; de FG is niet (persoonlijk) verantwoordelijk wanneer de AVG niet nageleefd wordt. Het pensioenfonds of de PUO (afhankelijk van waar de FG is gepositioneerd) is verantwoordelijk en moet kunnen aantonen dat de verwerking aan de voorwaarden voldoet. Een FG moet voldoende autonomie en middelen hebben om zijn taken goed te kunnen uitvoeren. Het idee van een FG is niet nieuw. Al in de voorloper van de AVG, de Europese privacyrichtlijn, werd de FG genoemd. Sommige pensioenfondsen en PUO's hebben ook al onder de Wbp een FG aangesteld.

Verplichting tot aanstelling van een FG

In sommige gevallen is het verplicht om een FG aan te stellen. Dit is nieuw in vergelijking met de hiervoor genoemde richtlijn. Vanuit de WP 29 zijn nadere richtlijnen opgesteld [5]. Als het aanstellen van een FG niet verplicht is, kan het voor pensioenfondsen en PUO's toch zinvol zijn om vrijwillig een FG aan te wijzen.

5 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtlijnen_fg.pdf

Het aanwijzen van een FG is verplicht wanneer:

a de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan;
b de verantwoordelijke of de verwerker hoofdzakelijk verwerkingen uitvoert die vanwege hun aard, omvang en/of doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen; of
c de verantwoordelijke of de verwerker hoofdzakelijk grootschalige verwerkingen uitvoert van bijzondere categorieën van gegevens of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten.

Voor pensioenfondsen en PUO's geldt dat zij niet vallen onder sub a en b. Ten aanzien van de vraag of zij vallen onder sub c moet naar de betekenis van de begrippen hoofdzakelijk, grootschalig en bijzondere categorieën van gegevens gekeken worden.

I Hoofdzakelijk

De kerntaken zien op de verwerking van persoonsgegevens als hoofdactiviteit en niet als nevenactiviteit. Verwerking van gegevens die onlosmakelijk verbonden zijn met de hoofdactiviteit worden ook als kerntaak gekwalificeerd. De kerntaak van een pensioenfonds is het administreren van een pensioenregeling, het beheren van het vermogen en communiceren met belanghebbenden. Adequate uitvoering is niet mogelijk zonder de gegevens van deelnemers te verwerken. Daarom dient het verwerken van deze gegevens als een van de kerntaken van een pensioenfonds of verzekeraar gezien te worden. Verwerkingen die nood-

zakelijk ondersteunend zijn aan de kerntaak, zoals het betalen van medewerkers en het bieden van ICT-ondersteuning, worden als nevenactiviteit beschouwd. Aan dit criterium wordt derhalve voldaan.

II Grootschalig

De AVG verduidelijkt niet wat onder 'op grote schaal' verstaan moet worden. WP 29 is van plan een standaard te ontwikkelen voor het bepalen van objectieve en kwantitatieve criteria voor wat onder 'grootschalig' verstaan moet worden. Totdat hier meer duidelijkheid over bestaat, geldt het volgende.

Bij de bepaling of verwerking op grote schaal plaatsvindt, spelen in ieder geval de volgende factoren een rol:

- het aantal betrokkenen;
- de hoeveelheid gegevens en/of de hoeveelheid verschillende gegevens die wordt verwerkt;
- de duur of permanentie van de gegevensverwerking;
- de geografische reikwijdte van de verwerking.

Als voorbeeld van verwerking op grote schaal wordt de verwerking van klantgegevens als onderdeel van de gebruikelijke werkzaamheden van een verzekeringsmaatschappij of bank genoemd. Aangezien pensioenfondsen en hun PUO's qua gegevensverwerking vergelijkbaar zijn met verzekeringsmaatschappijen wordt aan dit criterium voldaan.

III Bijzondere categorieën van gegevens

Bijzonder categorieën persoonsgegevens zijn in de AVG beschreven. Voor pensioenfondsen en PUO's kan het bijvoorbeeld gaan om:

- lidmaatschap van een vakbond;
- gegevens over de gezondheid van deelnemers zoals een arbeidsongeschiktheidspercentage (SUAG) of verzuimgegevens van medewerkers;
- pasfoto's op identiteitsbewijzen; een good practice is dat betrokkenen wordt gevraagd om dergelijke foto's onherkenbaar te maken voordat zij deze insturen naar de pensioenadministratie.

Pensioenfondsen en PUO's kunnen uit de data waarover zij beschikken ook andere bijzondere categorieën van persoonsgegevens afleiden. Zo kan uit het geslacht van de partner van een deelnemer worden afgeleid wat zijn of haar seksuele geaardheid is. Dergelijke afgeleide gegevens die niet expliciet worden geregistreerd en verwerkt, zijn geen bijzondere persoonsgegevens in de zin van de AVG.

Wel/geen verplichte FG

De begrippen hoofdzakelijk, grootschalig en bijzondere categorieën moeten in samenhang gelezen worden. Bij pensioenfondsen en PUO's is er doorgaans geen sprake van hoofdzakelijk grootschalige verwerkingen van bijzondere categorieën van gegevens, zodat dan naar de letter van de AVG genomen de aanstelling van een FG niet verplicht is.

De WP 29 raadt aan om een uitvoerige interne analyse uit te voeren om te bepalen of een FG verplicht aangesteld moet worden. Op die manier kan worden aangetoond dat met alle relevante factoren rekening gehouden is. De Pensioenfederatie raadt pensioenfondsen en PUO's daarom aan om zelf vast te stellen of er sprake is van een verplichting om een FG aan te stellen.

Als er geen verplichting is om een FG aan te stellen, kan dat uiteraard wel op vrijwillige basis. De in de AVG opgenomen voorwaarden voor aanwijzing, positie en taken van een FG gelden zowel bij een verplicht als vrijwillig aangewezen FG.

Zoals hierboven al aangegeven kan in de plaats van een FG ook een andere medewerker in dienst worden genomen of een adviseur worden ingehuurd (bijvoorbeeld als PO) die zich bezighoudt met de bescherming van persoonsgegevens. Als deze persoon een andere functienaam, positie en takenpakket heeft, gelden de AVG-regels voor een FG niet voor deze persoon. Pensioenfondsen en PUO's moeten zowel naar binnen als naar buiten duidelijk maken dat de PO geen FG is.

Voor welke oplossing ook wordt gekozen, pensioenfondsen en uitvoerders moeten ervoor zorgen dat de implementatie en (het toezicht op) de naleving van de AVG adequaat in de organisatie is belegd.

Als zowel het pensioenfonds als de PUO een FG hebben aangesteld, dan moeten deze samenwerken. De Pensioenfederatie is van mening dat er geen stapeling van verantwoordelijkheden of werkzaamheden moet plaatsvinden, zeker niet in deze tijd waarin uitvoeringskosten onder druk staan. Uiteraard moet wel volledig worden voldaan aan de vereisten van de AVG.

PUO's met meerdere bedrijfsonderdelen, zoals bijvoorbeeld pensioenadministratie, bestuursondersteuning en verzekeringen, kunnen één FG aanwijzen als deze maar goed bereikbaar is vanuit elke afdeling en vestiging.

Profiel FG

Een FG wordt aangewezen op grond van zijn professionele kwaliteiten, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming, en zijn vermogen zijn taken te vervullen.

Het vereiste kennisniveau van de FG dient te passen bij de gevoeligheid, complexiteit en de hoeveelheid gegevens die de pensioenfondsen en PUO's verwerken. De FG dient voldoende inzicht te hebben in de uitgevoerde gegevensverwerkingen en de informatiesystemen en de behoeften van de pensioenfondsen en PUO's op het gebied van veiligheid van gegevens en gegevensbescherming.

De contactgegevens van de FG moeten worden gepubliceerd en aan de AP worden gecommuniceerd.

Waar het om gaat, is dat betrokkenen en toezichthouder gemakkelijk, direct en vertrouwelijk contact met de FG op kunnen nemen. De contactgegevens van de FG dienen informatie te bevatten die betrokkenen en toezichthouder in staat stellen de FG gemakkelijk te bereiken. Een good practice is de vermelding van naam, postadres, een speciaal telefoonnummer en een speciaal e-mailadres of contactformulier.

Anders dan bestuursleden, leden van een raad van toezicht of andere medebeleidsbepalers wordt een FG niet vooraf extern door DNB of de AP op geschiktheid (kennis, competenties en professioneel gedrag) getoetst. Gezien de rol van de FG als onafhankelijke functionaris die toegang heeft tot alle verwerkingen van persoonsgegevens, dient dit iemand van onbesproken gedrag te zijn. Het is dan ook raadzaam dat een FG voorafgaand aan de aanstelling uitgebreid wordt gescreend.

Positie FG

Het is van cruciaal belang dat een FG zo vroeg mogelijk betrokken wordt bij alle aangelegenheden die de bescherming van persoonsgegevens betreffen.

De pensioenfondsen en PUO's ondersteunen een FG door hem toegang te verschaffen tot alle persoonsgegevens en verwerkingen. Ook stellen zij een FG de middelen ter beschikking die nodig zijn voor het vervullen van zijn taken en het in stand houden van zijn deskundigheid.

In de AVG zijn basisgaranties vastgelegd die ervoor moeten zorgen dat een FG zijn taken met voldoende autonomie kan uitvoeren. Dit betekent met name dat:

- een FG geen instructies ontvangt met betrekking tot de uitvoering van taken;
- als het pensioenfonds en de PUO beslissingen nemen die afwijken van het advies van een FG, deze zijn afwijkende mening moet kunnen bespreken met degenen die de beslissingen nemen.

Het pensioenfonds of PUO blijft verantwoordelijk voor naleving van de AVG en moet kunnen aantonen dat deze nageleefd wordt.

Een FG mag niet ontslagen of gestraft worden voor de uitvoering van zijn taken. Er geldt een vergelijkbare ontslagbescherming als die voor leden van de ondernemingsraad en pensioenfondsbestuurders. Het is ook mogelijk om een externe FG in te huren onder een overeenkomst van opdracht (7:400 BW). De AVG stelt geen expliciete vereisten aan deze overeenkomst. De overeenkomst zal gezien de aard van de dienstverlening niet makkelijk opzegbaar moeten zijn (vergelijk artikel 7:408 lid 1 BW) en de bevoegdheid tot het geven van aanwijzingen (artikel 7:402 BW) zal zeer beperkt moeten zijn.

Een FG mag andere taken en plichten vervullen als deze taken of plichten maar niet tot een belangenconflict leiden. Een belangenconflict kan zich voordoen als

de FG een belang heeft bij beslissingen die ingaan tegen de rechten van aanspraak- en pensioengerechtigden. Bij directie- of bestuursfuncties zal naar alle waarschijnlijkheid al snel sprake kunnen zijn van belangenconflicten.

Taken FG

De werkzaamheden van de FG zijn:

- informeren en adviseren over verplichtingen ten aanzien van het beschermen van gegevens;
- toezien op naleving van de AVG of andere regels/beleid ten aanzien van de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het betrokken personeel en de betreffende audits;
- samenwerken met en als contactpersoon dienen voor de AP.

De FG dient erop toe te zien dat de AVG nageleefd wordt. Daartoe kan de FG:

- informatie verzamelen om verwerkingswerkzaamheden te identificeren;
- analyseren en controleren in hoeverre verwerkingswerkzaamheden aan de AVG voldoen; en
- het pensioenfonds of de PUO informeren, adviseren of aanbevelingen geven.

Het is de taak van de pensioenfondsen en PUO's om, waar nodig, een PIA uit te voeren. Dit is dus niet de taak van de FG, maar uiteraard kan een PIA wel in samenwerking met een FG worden uitgevoerd. Pensioenfondsen en PUO's zijn in ieder geval verplicht bij een PIA het advies van de FG in te winnen over de vragen:

- of er al of niet een PIA uitgevoerd moet worden;
- welke methodiek voor de PIA gebruikt moet worden;
- of de PIA intern uitgevoerd of uitbesteed moet worden;
- welke waarborgen (zoals technische en organisatorische maatregelen) ingebouwd moeten worden om eventuele risico's voor de rechten en belangen van de betrokkenen te beperken;
- of de PIA correct uitgevoerd is en de conclusies daaruit (de vraag of de verwerking door moet gaan en welke waarborgen er ingebouwd moeten worden) aan de AVG voldoen.

Als pensioenfondsen en PUO's het niet met het advies van de FG eens zijn, moet in de documentatie van de PIA specifiek schriftelijk aangegeven worden waarom het advies niet overgenomen is.

Een FG houdt bij de uitvoering van zijn taken rekening met het aan de verwerkingen verbonden risico en met de aard, de omvang, de context en de verwerkingsdoeleinden (risicogebaseerde benadering).

Het is aan te bevelen dat de FG het register op alle verwerkingen van persoonsgegevens die pensioenfondsen en PUO's uitvoeren, bijhoudt.

De FG is geen (verlengstuk van de) toezichthouder en heeft geen corrigerende bevoegdheden. Hij moet controleren en rapporteren aan de eindverantwoordelijken.

12 Meldplicht datalekken

Bij een datalek vindt er een inbreuk plaats op de beveiliging van persoonsgegevens. Voorbeelden hiervan zijn dat,

- er bij de PUO onbedoeld aan een te ruime kring van medewerkers toegang is gegeven tot het pensioenadministratiesysteem;
- persoonsgegevens onbedoeld zijn vrijgekomen (lekken), gewijzigd of vernietigd (denk aan een brand of lekkage in het datacenter);
- er is ingebroken in een databestand (hacken);
- er een USB-stick met persoonsgegevens is kwijtgeraakt;
- er een laptop met persoonsgegevens is achtergelaten in de trein of is gestolen;
- poststukken voor deelnemers geopend retour worden ontvangen, bij de verkeerde ontvanger zijn aangekomen (en geopend zijn), of nooit zijn aangekomen.

De nu al bestaande meldplicht datalekken blijft onder de artikelen 33 en 34 AVG grotendeels hetzelfde. De verwerkingsverantwoordelijke, dus het pensioenfonds, moet een geconstateerd datalek meteen doch in ieder geval binnen 72 uur melden aan de AP. Als dat niet tijdig lukt, dan moet het pensioenfonds hiervoor een verklaring kunnen geven. De PUO kan namens het pensioenfonds de melding bij de AP doen.

Er hoeft onder de AVG strikt genomen niet bij de AP te worden gemeld als het onwaarschijnlijk is dat het datalek redelijkerwijs een risico inhoudt voor de deelnemers. Echter in de praktijk is het raadzaam om bij twijfel het zekere voor het onzekere te nemen en toch te melden.

Als er wel een hoog risico is en het pensioenfonds achteraf geen maatregelen meer kan nemen om het risico te mitigeren, dan moeten naast de AP ook de deelnemers zelf worden geïnformeerd, zodat die eventueel voorzorgsmaatregelen kunnen treffen. De AP kan het pensioenfonds ook verplichten tot melding aan de deelnemers.

Als een melding aan deelnemers een onevenredige inspanning van het pensioenfonds zou vergen, dan kunnen de deelnemers ook op een andere manier worden geïnformeerd, bijvoorbeeld door een openbare mededeling.

Als er maatregelen zijn genomen waarmee het risico wel voldoende is verkleind, bijvoorbeeld doordat de gegevens gepseudonimiseerd zijn, is een melding aan de deelnemer niet nodig.

Er moet onder de AVG wel meer worden geregistreerd over de datalekken die zich hebben voorgedaan: feiten, gevolgen voor de deelnemers en genomen maatregelen. Alle datalekken, ook de niet aan de AP gemelde datalekken, moeten worden geregistreerd zodat de AP in staat is om de naleving van de AVG te controleren.

Thans staat de AP toe dat pensioenfondsen onder bepaalde voorwaarden datalekken bij grootschalige postverzending in bulk mogen melden. Het is onzeker of dat straks onder de AVG nog toegestaan is. De AP zal informatie hierover op haar website opnemen.

13 Verwerkersovereenkomst

Als een pensioenfonds (als verwerkingsverantwoordelijke) persoonsgegevens laat verwerken door een PUO (verwerker) dan moet over deze uitbesteding een schriftelijke verwerkersovereenkomst (of andere bindende rechtshandeling) tussen beide partijen gesloten worden (artikel 28 AVG).
Een PUO is in relatie tot een pensioenfonds bij de uitvoering van door het pensioenfonds aan de PUO uitbestede (pensioen)werkzaamheden altijd als verwerker te beschouwen.

Een verwerkersovereenkomst mag alleen gesloten worden met een verwerker die zelf ook afdoende technische en organisatorische maatregelen heeft getroffen om te waarborgen dat de verwerking voldoet aan de verplichtingen uit de verordening, in het bijzonder maatregelen om een passend beveiligingsniveau te waarborgen.

De verwerkersovereenkomst kan op maat opgesteld worden, maar evengoed kan gebruik worden gemaakt van standaardcontractbepalingen. Mogelijk dat de AP in de toekomst een dergelijke standaardcontractbepaling beschikbaar stelt.

In die verwerkersovereenkomst (op maat of standaard) moeten de volgende onderwerpen worden vastgelegd:

- Algemene beschrijving

Een omschrijving van het onderwerp, de duur, de aard en het doel van de verwerking, het soort persoonsgegevens, de categorieën van betrokkenen en de rechten en verplichtingen als verwerkingsverantwoordelijke.

- Instructies verwerking

De verwerking vindt uitsluitend plaats op basis van schriftelijke instructies van het pensioenfonds. De PUO mag de persoonsgegevens niet voor eigen doeleinden gebruiken. Als een instructie een inbreuk oplevert op de AVG stelt de PUO het pensioenfonds hier onmiddellijk van op de hoogte.

Iedere medewerker van het pensioenfonds, de PUO en eenieder die in dienst is van of werkzaam is voor de PUO verwerkt persoonsgegevens uitsluitend in opdracht van het pensioenfonds (behoudens andere wettelijke verplichtingen tot verwerking).

- Geheimhoudingsplicht

Personen in dienst van of werkzaam voor de PUO hebben een geheimhoudingsplicht.

- Beveiliging

De PUO treft passende technische en organisatorische maatregelen om de verwerking te beveiligen. Deze maatregelen moeten in ieder geval waarborgen: pseudonimisering en versleuteling van persoonsgegevens, permanente informatiebeveiliging, herstel van beschikbaarheid en toegang tot persoonsgegevens bij incidenten en regelmatige beveiligingstesten.

- Subverwerkers

De PUO schakelt geen subverwerker(s) in zonder voorafgaande schriftelijke toestemming van het pensioenfonds. De PUO legt aan een subverwerker in een subverwerkersovereenkomst dezelfde verplichtingen op als het pensioenfonds aan de PUO heeft gesteld. Met name de verplichting dat afdoende technische en organisatorische maatregelen zijn getroffen om te waarborgen dat de verwerking voldoet aan de verplichtingen uit de verordening.
Het is aan te bevelen om in de verwerkersovereenkomst direct vast te leggen dat, en onder welke voorwaarden, de verwerker subverwerkers mag inschakelen. Komt de subverwerker zijn verplichtingen niet na? Dan blijft de PUO volgens de AVG volledig aansprakelijk richting het pensioenfonds voor het nakomen van de verplichtingen van de subverwerker.

- Privacyrechten

De PUO helpt het pensioenfonds om te voldoen aan zijn plichten als aanspraak- en pensioengerechtigden hun privacyrechten uitoefenen (denk aan het recht op inzage, rectificatie, bezwaar, vergetelheid, beperking en dataportabiliteit).

- Andere verplichtingen

De PUO helpt het pensioenfonds ook om de overige verplichtingen na te komen, zoals het melden van datalekken, het uitvoeren van een privacy impact assessment (PIA) en het voorafgaand raadplegen van de AP ingeval van een hoog risicovolle PIA.

- Gegevens verwijderen

Na afloop van de verwerkingsdiensten verwijdert de PUO de persoonsgegevens. Als het pensioenfonds dit wil, kan de PUO de gegevens ook teruggeven aan het pensioenfonds. Ook verwijdert de PUO alle kopieën, tenzij er een wettelijke verplichting is om de gegevens te bewaren.

- Audits

De PUO werkt mee aan periodieke audits die door of namens het pensioenfonds worden uitgevoerd. De PUO stelt alle relevante informatie beschikbaar om te kunnen controleren of hij zich als verwerker houdt aan de aan hem als verwerker opgelegde verplichtingen.

De Pensioenfederatie adviseert om bestaande verwerkersovereenkomsten te toetsen aan bovenstaande criteria en waar nodig aan te passen.

14 Leidende toezichthouder en internationale aspecten

Artikel 56 AVG legt vast welke toezichthouder (van welk Europees land) de zogenoemde leidende toezichthoudende autoriteit is. Dit is alleen relevant voor pensioenfondsen met vestigingen buiten Nederland, want voor pensioenfondsen die zich uitsluitend binnen Nederland bevinden is de AP de aangewezen toezichthouder.

Een ander internationaal aspect is doorgifte van persoonsgegevens buiten Nederland, bijvoorbeeld bij uitbesteding van gegevensverwerking aan buitenlandse PUO-uitvoerders. Het is belangrijk om de afspraken hierover goed vast te leggen in de verwerkersovereenkomst. Bij doorgifte buiten de EU moet goed bekeken worden of doorgifte is toegestaan. Er zijn enkele mogelijkheden, zoals bijvoorbeeld het Privacy Shield tussen de EU en de VS, en Europese modelcontracten (Standard Contractual Clauses). Aan verwerking van persoonsgegevens via clouddiensten moet in dit verband ook extra aandacht worden geschonken; er moet benoemd worden waar de cloud – en dus de persoonsgegevens – zich bevindt/bevinden en doorgifte naar die locatie moet volgens de bestaande mogelijkheden gaan.

De AVG is van toepassing op pensioenfondsen die persoonsgegevens (doen) verwerken van betrokkenen in de Europese Unie, ongeacht of de verwerking plaatsvindt in de Europese Unie. Pensioenfondsen en hun uitvoerders moeten de nieuwe privacyregels dus ook toepassen als gegevens worden verwerkt buiten de Europese Unie, bijvoorbeeld via cloud computing. Contracten met IT-dienstverleners die niet in de Europese Unie gevestigd zijn zullen dus waar nodig moeten worden aangepast aan de AVG.

15 Toestemming

Vaak zal de gegevensverwerking van het pensioenfonds gebaseerd zijn op de grondslag 'uitvoeren van een overeenkomst' (Opf'en en APF'en) of het 'uitvoeren van een wettelijke verplichting' (Bpf'en en Bpr'en). In sommige gevallen kan er echter sprake zijn van gegevensverwerking op basis van toestemming van de deelnemer (artikel 7 AVG). Denk bijvoorbeeld aan het delen van pensioenberekeningen of andere persoonsgegevens met (de adviseur van) de werkgever of met een student in het kader van een afstudeerscriptie. De AVG stelt strengere eisen aan gegevensverwerking op basis van toestemming dan de Wbp:

- er moet duidelijk en in eenvoudige taal worden verteld waarvoor toestemming wordt gevraagd, voor welk specifiek doel het pensioenfonds de gegevens gaat gebruiken en de deelnemer moet erop worden gewezen dat de toestemming altijd ingetrokken mag worden;
- de gevraagde toestemming moet zo worden gepresenteerd dat er een duidelijk onderscheid is met andere zaken;
- de toestemming mag door de deelnemer worden geweigerd, zonder dat dat enig verder gevolg voor hem of haar heeft;
- de toestemming moet gegeven worden door een duidelijke, actieve handeling (opt-in). Een zogenoemd negatief piep-systeem (wie zwijgt stemt toe, ofwel opt-out) is niet toegestaan. Zo mogen bijvoorbeeld hokjes in een digitaal (web-based) formulier niet al vooraf zijn aangevinkt. Wel voldoende is bijvoorbeeld dat de deelnemer zijn e-mailadres invult op een inschrijfformulier voor een nieuwsbrief;
- het pensioenfonds moet in ieder geval zolang de gegevensverwerking duurt kunnen aantonen dat de toestemming is verkregen, bijvoorbeeld door logbestanden dat een vinkje is aangekruist, een kopie inschrijfformulier of een bevestiging bij de inschrijving op nieuwsbrieven;
- de toestemming moet makkelijk en op dezelfde wijze als dat hij gegeven is, ingetrokken kunnen worden. Na intrekking van de toestemming moet de verwerking uiteraard gestaakt worden.

Vanwege de strenge voorwaarden waaraan moet worden voldaan voor de verwerking van persoonsgegevens op basis van toestemming, en het feit dat de deelnemer de toestemming altijd kan intrekken, is het raadzaam om deze grondslag alleen te hanteren als er geen andere grondslag voor de gegevensverwerking mogelijk is.

16 Profilering

Een onder invloed van de digitale wereld in belang toenemend fenomeen betreft profilering. Onder profilering wordt in artikel 22 AVG verstaan: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen. Om de privacy van betrokkenen te beschermen, stelt de AVG voorwaarden aan deze wijze van dataverzameling.

Hoe wordt met profilering omgegaan

Profiling bestaat uit drie stappen:

1 het verzamelen van (persoons)gegevens over (een groep) mensen;
2 het analyseren en combineren van deze, en soms ook andere, gegevens om verbanden en patronen te ontdekken;
3 het toepassen van de verbanden en patronen (profielen) op (een groep) mensen om hen op grond van hun profiel in te delen in een bepaalde categorie en/of hun gedrag te voorspellen.

Een profiel kan bijvoorbeeld iets zeggen over iemands gezondheid, economische situatie, persoonlijke interesses en voorkeuren of hoe hij graag zijn vrije tijd doorbrengt. Ook voor pensioenfondsen en PUO's kan het profiel van hun deelnemers interessante en bruikbare informatie opleveren. Zo kan dit gebruikt worden voor segmentatie, bijvoorbeeld voor het toesturen van nieuwsbrieven of voor (aanvullende) productinformatie, of voor innovatie zoals de ontwikkeling van nieuwe diensten of producten zoals bijvoorbeeld online deelnemersportalen of apps.

De privacyrisico's van profilering

Profilering kan handig zijn voor zowel pensioenfondsen als betrokkenen. Hierdoor kan immers die informatie worden verstrekt die betrokkenen interessant vinden of waar zij zelfs behoefte aan hebben. Tegelijkertijd kan profilering gepaard gaan met privacyrisico's. Dat geldt zeker als bij profilering bijzondere categorieën van persoonsgegevens (bijvoorbeeld over gezondheid of strafrechtelijke gegevens) of andere gevoelige persoonsgegevens (zoals financiële gegevens, locatiegegevens of gegevens over surfgedrag) worden verwerkt.

Profilering kan de volgende risico's opleveren voor de privacy:

- verkeerd of niet actueel profiel; door het gebruik van onjuiste of verouderde gegevens kan een verkeerd beeld van iemand ontstaan;
- stigmatisering; door profilering kunnen individuen of groepen mensen in een bepaald hokje worden geplaatst en op basis daarvan anders worden behandeld of mogelijk zelfs worden achtergesteld of uitgesloten;
- geautomatiseerde besluitvorming; profilering gebeurt meestal geautomatiseerd. Ook de besluitvorming kan geautomatiseerd verlopen. De computer neemt dan een beslissing over iemand in plaats van een persoon. Hierin schuilt het gevaar dat iemand 'gevangen' zit in een (verkeerd of niet-actueel) profiel, omdat de menselijke tussenkomst ontbreekt;
- beïnvloeding, minder keuzevrijheid en in het ergste geval uitsluiting; websites die berichten of resultaten tonen waarvan wordt verwacht dat die het beste aansluiten bij iemands interesses. Dit beperkt in zekere mate de vrijheid van die persoon om informatie te krijgen;
- bovenmatige gegevensverwerking; dit houdt in dat er bij profilering meer gegevens over iemand worden verwerkt dan strikt noodzakelijk is voor het doel van de gegevensverwerking.

Voorwaarden voor toepassing van profilering

De belangrijkste privacyverplichtingen voor pensioenfondsen en PUO's zijn:

- toestemming vragen; als door middel van zogenoemde cookies het surfgedrag van een deelnemer op de website of in een online deelnemersportaal wordt gevolgd, bijvoorbeeld om op grond van die gegevens specifieke informatie toe te sturen, dan moet voor het mogen plaatsen van cookies eerst toestemming van de betrokkene zijn verkregen. De deelnemer moet ook altijd de mogelijkheid hebben om zijn toestemming weer in te trekken;
- doelgebruik; pensioenfondsen moeten van tevoren duidelijk en begrijpelijk aangeven waarvoor zij de verschillende soorten gegevens, en dus ook de door middel van profilering verkregen gegevens, gebruiken;
- informatieplicht, met name de privacyverklaring; pensioenfondsen moeten zorgen voor een leesbare, begrijpelijke en toegankelijke privacyverklaring. Hierin moet de volgende informatie staan:
  - de doelen van profilering;
  - de verschillende soorten gegevens die de organisatie daarvoor gebruikt;
  - hoe lang de organisatie deze gegevens bewaart;
  - waarom het nodig is om een profiel vast te stellen;
- privacyrechten; pensioenfondsen moeten betrokkenen de mogelijkheid geven om:
  - hun eigen gegevens in te zien, waaronder de profileringsgegevens;
  - deze gegevens, en dus ook de profileringsgegevens, te laten corrigeren of verwijderen;
  - bezwaar aan te tekenen tegen het gebruik van die (profilerings)gegevens bij gegevensverwerking op grond van een gerechtvaardigd belang en bij direct marketing.

- besluit door een persoon; pensioenfondsen moeten beslissingen op basis van een profiel in principe laten nemen door een persoon. Geautomatiseerde besluitvormingssystemen mogen alleen als hulpmiddel worden gebruikt. Als een deelnemer dat niet wil, dan mag hij niet onderworpen worden aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit;
- privacy impact assessment (PIA); bij het uitvoeren van gesystematiseerde beoordeling, waaronder profilering, op basis van geautomatiseerde verwerking van persoonsgegevens moet altijd eerst een PIA worden uitgevoerd.

Wat een pensioenfonds moet doen bij een vraag of klacht over profilering
Er moet een afhandelingsprocedure worden ingericht voor de behandeling van vragen of klachten van deelnemers over profilering. Het is raadzaam om deze procedure te koppelen aan de klachtenprocedure van het pensioenfonds en/of de pensioenuitvoeringsorganisatie.