# Privacybeleid Stichting Pensioenfonds Tandartsen en Tandarts-specialisten

## Inhoud

# 1. Inleiding

## 1.1 Inleiding

*De Stichting Pensioenfonds Tandartsen en Tandarts-specialisten (het Fonds) verwerkt persoonsgegevens* van onder andere aanspraak- en pensioengerechtigden, (ex-)leden van fondsgremia, gezamenlijk voortaan aangeduid met betrokkenen. Deze betrokkenen moeten erop kunnen vertrouwen dat het Fonds, binnen de kaders van de geldende wet- en regelgeving, op een veilige en zorgvuldige manier omgaat met de persoonsgegevens van zijn betrokkenen. In dit beleid wordt vastgelegd op welke wijze het Fonds omgaat met persoonsgegevens en privacy.

## 1.2 Wetgeving en definities

Op dit moment heeft elke lidstaat van de Europese Unie een eigen privacywet, gebaseerd op de Europese richtlijn van 1995. De Wet bescherming persoonsgegevens (Wbp) regelt het juridische kader voor de omgang met persoonsgegevens in Nederland. Op 25 mei 2018 vervalt de Wbp en treedt de Europese Verordening; de Algemene Verordening Gegevensbescherming (AVG), in werking, samen met de uitvoeringswet. De AVG zorgt onder andere voor versterking en uitbreiding van de privacyrechten met meer verantwoordelijkheden voor organisaties.

De volgende begrippen worden in de AVG gebruikt:

*Betrokkene:* De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt. Voor het Fonds zijn de belangrijkste betrokkenen de aanspraak- en pensioengerechtigden, (ex)-leden van fondsgremia, natuurlijke personen.

*Verwerker:* De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie. De belangrijkste verwerkers voor het Fonds zijn pensioenuitvoeringsorganisatie, adviserend actuaris en dergelijke derden, mits zij persoonsgegevens verwerken.

*Persoonsgegevens:* Alle gegevens die gaan over natuurlijke personen en waaraan je een natuurlijk persoon als individu kunt herkennen. Het gaat hierbij om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld; naam, adres, geboortedatum). Naast gewone persoonsgegevens kent de wet ook bijzondere *categorieën van persoonsgegevens. Het gaat specifiek om: gegevens waaruit ras of etnische afkomst blijkt, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.*

*Gegevensbeschermingseffectbeoordeling*: Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit heet ook wel een Privacy Impact Assessment.

*Verwerkingsverantwoordelijke*: Een persoon of organisatie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Het Fonds is gewoonlijk de verwerkingsverantwoordelijke en bepaalt in ieder geval het doel van de verwerking en heeft ook de zeggenschap over de wijze van verwerken. In dit beleid wordt voortaan de term verantwoordelijke gebruikt.

*Verwerking*: Een verwerking is alles wat met een persoonsgegeven gedaan wordt, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.

## 1.3 Scope

Dit beleid is van toepassing op alle verwerkingen van persoonsgegevens die door of namens het Fonds plaatsvinden.

## 1.4 Rollen en verantwoordelijkheden

**Verantwoordelijke**
Het bestuur van het Fonds is verantwoordelijke voor de verwerkingen van persoonsgegevens die door of namens het Fonds plaatsvinden. Daarbij dient ook de privacyregelgeving in acht te worden genomen bij de uitvoering in de praktijk, alsook voor de adequate inrichting van de Privacy Compliance Functie.
Het bestuur is “accountable”, dat wil zeggen dat het aanspreekbaar is op een veilige en zorgvuldige gegevensverwerking en bewijs moet kunnen produceren dat het bestuur voldoet aan de eisen van de wet- en regelgeving. Dat leidt tot documentatie, zoals dit beleid, correcte verwerkersovereenkomsten, adequate beveiligingsmaatregelen en implementatie. Alsook monitoring op de correcte naleving, zoals testen, audits, evaluatie en registratie. Voorts indien noodzakelijk actualisatie van dit beleid en de uitvoering daarvan. Dit vraagt om een proactieve houding van zowel het bestuur als de uitvoeringsorganisatie, bij wie veelal de daadwerkelijk verwerking van de persoonsgegevens van betrokkene plaatsvindt.

**Privacy Functie**
Het bestuur heeft besloten om vooralsnog geen aparte privacy functionaris te benoemen, maar wel een bestuurder aan te wijzen, die dit onderwerp in zijn portefeuille heeft.

# 2. Uitgangspunten voor verwerking

Het Fonds respecteert de privacy van betrokkenen en houdt bij de verwerking van hun persoonsgegevens de volgende uitgangspunten in acht:

## 2.1 Rechtmatigheid, behoorlijkheid en transparantie

De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet, en op een zorgvuldige wijze. Voor betrokkenen moet inzichtelijk zijn waarom en op welke manier persoonsgegevens worden verwerkt. Het Fonds moet hier helder en toegankelijk over communiceren in een zogenoemd privacy statement en in de eerste communicatie met betrokkenen, zoals bij het verzenden van de Pensioen 1-2-3.

## 2.2 Doeleinden

Volgens de AVG mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. De gegevens mogen niet voor andere doelen verwerkt worden. Het Fonds moet die doeleinden concreet vaststellen en beschrijven voordat de verwerking begint.
Het Fonds verwerkt de persoonsgegevens van betrokkenen voor de volgende doelen:

- Om de dienstverlening van het Fonds richting betrokkenen conform de vastgestelde pensioenreglementen te kunnen uitvoeren, bijvoorbeeld om de pensioenrechten of -aanspraken of (aanvullende) inkomensverzekeringen zorgvuldig en juist te berekenen, betrokkenen daarover tijdig en correct te informeren en de uitkering stipt uit te betalen, om ALM studies te doen en premies te berekenen.
- Om contractuele afspraken of wettelijke of internationale verplichtingen na te komen.
- Om de gebruiksvriendelijkheid van de website te verbeteren.
- Voor interne (kwaliteits)analyes en productontwikkeling. Hiermee kunnen de regelingen en dienstverlening naar betrokkenen verbeterd worden.
- Om communicatie over de pensioenzaken van betrokkenen en daarmee samenhangende onderwerpen via verschillende communicatiekanalen zo relevant en persoonlijk mogelijk te maken. Om dat mogelijk te maken, koppelt, combineert en analyseert het Fonds beschikbare (persoons)ge-

gevens om zo de meest relevante doelgroepen en segmenten, inhoud, informatie, momenten en kanalen te bepalen, op elkaar af te stemmen en het aantal contactmomenten te beperken.

Verdere verwerking voor een ander doel dan waarvoor de gegevens oorspronkelijk werden verzameld, moet separaat gerechtvaardigd kunnen worden als de verwerking niet berust op toestemming of wettelijke verplichting. De verwerking moet in ieder geval noodzakelijk zijn voor het doel dat wordt nagestreefd. Hoe het Fonds hierover communiceert aan betrokkenen, wordt uitgewerkt in de paragraaf transparantie en de rechten van betrokkenen.

## 2.3 Rechtmatige grondslag

De wet bepaalt dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag, zoals vastgelegd in de AVG, van toepassing moet zijn. Dat betekent dat de verwerking alleen mag plaatsvinden, indien:

a) de aanspraak- of pensioengerechtigde toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens; een voorbeeld hiervan is toestemming voor het gebruik van tracking cookies op de website van het Fonds.
b) de verwerking noodzakelijk is 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 Fonds wettelijk verplicht is de verwerking uit te voeren; denk hierbij aan alle voorschriften uit de Pensioenwet of fiscaal verplichte administratieve taken,
d) de verwerking noodzakelijk is om de vitale belangen (lees: het leven) van de aanspraak- en pensioengerechtigden of andere personen te beschermen; deze grondslag zal bij het Fonds niet snel voorkomen;
e) de verwerking noodzakelijk is voor een taak van algemeen belang of een publieke taak; deze grondslag zal bij het Fonds niet snel voorkomen;
f) een eigen gerechtvaardigd belang van het Fonds 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 Fonds van toepassing is.

## 2.4 Bijzondere gegevens

In principe verwerkt het Fonds geen bijzondere categorieën van persoonsgegevens, behalve informatie over iemands gezondheid (denk aan een arbeidsongeschiktheidspercentage in geval van premievrijstelling), waarvoor een grondslag zoals vermeld in de AVG en/of Uitvoeringswet Algemene Verordening gegevensbescherming is benodigd om deze gegevens te mogen verwerken. Denk bijvoorbeeld aan uitdrukkelijke toestemming van betrokkene of een wettelijke regeling die dat mogelijk maakt. Hetgeen ook geldt voor strafrechtelijke gegevens en het Burgerservicenummer (BSN), waarvan de verwerking alleen geschiedt voor zover dat is toegestaan op basis van een specifiek wettelijke grondslag. Daarnaast kennen we nog een categorie gevoelige gegevens, zoals bijvoorbeeld financiële of locatiegegevens. Indien er bijvoorbeeld een datalek plaatsvindt, waarbij gevoelige gegevens zijn gelekt, dan dient er in ieder geval melding bij de AP plaats te vinden en mogelijk ook aan betrokkenen.

## 2.5 Wijze van verwerking

Er moet sprake zijn van minimale gegevensverwerking. Het beginsel van dataminimalisatie betekent dat verwerking moet worden beperkt tot wat noodzakelijk is om de vastgestelde doeleinden te bereiken. Wanneer met geen, of minder (belastende), persoonsgegevens hetzelfde doel bereikt kan worden moet daar altijd voor gekozen worden. Hiermee hangt samen dat persoonsgegevens ook zo snel mogelijk moeten worden geaggregeerd (als daarmee ook het doel kan worden gerealiseerd), geanonimiseerd of

gewist. De AVG gaat ook uit van subsidiariteit. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt.

Het Fonds 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.

Het Fonds bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van zijn taken en neemt daarbij ook de wettelijke verplichting uit hoofde van bijvoorbeeld het Burgerlijk Wetboek, de Pensioenwet, of fiscale wetgeving in acht. Het uitgangspunt voor de gehanteerde bewaartermijn is het Servicedocument Bewaartermijnen van de Pensioenfederatie.

Het Fonds zorgt dat door middel van passende technische en organisatorische beveiligingsmaatregelen ongeoorloofde toegang tot c.q. ongeoorloofd gebruik van persoonsgegevens wordt voorkomen en heeft daartoe een informatiebeveligingsbeleid vastgesteld en stelt aan uitbestede partijen stringente eisen op het gebied van IT-security. Zie hiervoor de paragraaf uitbesteding.
De persoonsgegevens worden alleen verwerkt door personen of bedrijven met een geheimhoudingsplicht.

## 3. Transparantie & Communicatie

Het Fonds informeert betrokkenen over het verwerken van hun persoonsgegevens. Met de AVG wordt als gevolg van versterking en vernieuwing van de rechten van betrokkenen het transparantiebeginsel in de wet geïntroduceerd. Dit beginsel 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. Voorts dient dat in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm te geschieden, desgewenst met gebruikmaking van gestandaardiseerde iconen. Onderwerpen waarover naar betrokkene dient te worden gecommuniceerd zijn de navolgende:

- contactgegevens m.b.t. het Fonds en hoe betrokkenen contact kunnen opnemen met het pensioenfonds
- waarom persoonsgegevens worden verzameld en waarom dat mag (doel en rechtsgrond van de verwerking van de persoonsgegevens);
- wat zijn de gerechtvaardigde belangen van het Fonds voor de gegevensverwerking, indien dat de rechtsgrond van de verwerking is;
- aan wie de persoonsgegevens verder nog worden verstrekt (ontvangers of categorieën van ontvangers);
- zijn betrokkenen verplicht om de gevraagde persoonsgegevens te verstrekken of niet? En wat zijn de gevolgen als een betrokkene de persoonsgegevens niet verstrekt (noodzaak)?;
- waar en hoe kan de betrokkene vragen om inzage, rectificatie, wissen of overdracht van persoonsgegevens, klachten indienen, bezwaar maken of een verwerking beperken?;
- hoe kan een betrokkene een verleende toestemming intrekken?;
- hoe lang verwacht het Fonds de persoonsgegevens te gaan bewaren?;
- 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;
- doet het Fonds aan geautomatiseerde besluitvorming (computergestuurde verwerking van persoonsgegevens zonder menselijke tussenkomst, bijvoorbeeld profilering)? En zo ja, welke logica wordt daarvoor gebruikt?;
- maakt het Fonds gebruik van zogenoemde cookies, welke persoonsgegevens worden dan verzameld, waarom en op welke wijze?

Wanneer betrokkenen gegevens aan het Fonds aanleveren, dan dienen zij van vorengenoemde informatie op de hoogte gesteld te worden. Dit kan bijvoorbeeld via standaardformulieren, de zogenaamde Pensioen 1-2-3 communicatie. Wanneer de gegevens via een andere weg verkregen worden, bijvoorbeeld via de werkgever dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze gegevens voor de eerste keer worden verwerkt. Dit kan uiterlijk op het moment van

eerste contact met betrokkenen, indien deze niet te laat wordt verstuurd, op zijn vroegst binnen een maand na ontvangst gegevens van de werkgever.

Informatie die gedurende de looptijd aan de betrokkene moet worden verstrekt kan ook via een internetportal van het Fonds geschieden. Van belang is ook dat betrokkenen daarbij verwezen worden naar de website van het landelijk pensioenregister, www.mijnpensioenoverzicht.nl.

De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat het Fonds persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.
De standaardteksten m.b.t. de persoonlijke communicatie aan betrokkenen zullen nader worden uitgewerkt door de communicatie-commissie.

**Privacy statement**
Daarnaast beschikt het Fonds over een privacy statement, indien persoonsgegevens worden verzameld via de website. Ook dit statement dient aan de bovenvermelde eisen te voldoen.

## 4. Rechten van betrokkenen

De AVG geeft betrokkenen meer rechten dan onder de Wbp en het Fonds faciliteert het uitoefenen van deze rechten, indien een betrokkene daarop een beroep doet. Hieronder wordt kort toegelicht wat deze rechten inhouden en voorts worden deze rechten nader uitgewerkt in de procedure rechten betrokkenen.

De AVG kent betrokkenen de navolgende rechten toe:

- **Inzage:** Betrokkenen hebben het recht om aan het Fonds te vragen of zijn/haar 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.
- **Rectificatie**: Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij het Fonds om deze te wijzigen of aan te vullen. Als de betrokkene terecht een beroep doet op dit recht dan moet het Fonds volgens de AVG iedere ontvanger van de gegevens, zoals bijvoorbeeld de belastingdienst, het UWV en subverwerkers, hiervan op de hoogte stellen.
- **Wissen (recht op vergetelheid)**: De betrokkene heeft het recht om de gegevens te laten wissen indien bijvoorbeeld de persoonsgegevens niet meer nodig zijn voor het doeleinde van verwerking, bij intrekking toestemming terwijl er geen andere grondslag aanwezig is of als terecht bezwaar aangetekend is tegen de verwerking. Voorts in geval van onrechtmatige verwerking. Overigens is dit geen absoluut recht en bestaat hierop bijvoorbeeld geen recht indien het Fonds voldoet aan een wettelijke verplichting en bijvoorbeeld in geval van een onderbouwing van een rechtsvordering. Het wissen moet kosteloos geschieden en zo spoedig mogelijk, in ieder geval binnen een maand. Ook de wissing moet het Fonds doorgeven aan de ontvangers.
- **Beperking**: De betrokkene heeft het recht de verwerking te beperken in vier situaties:
  • als de juistheid van de gegevens wordt betwist en het Fonds moet dat controleren;
  • als de verwerking onrechtmatig is en de betrokkene zich verzet tegen wissen, maar een beperking wenst.
  • als het Fonds de gegevens niet meer nodig heeft, 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 Fonds niet meteen beslist, dan kan de betrokkene een beperking verlangen.
  Overigens ook dit is geen absoluut recht en verwerking kan toch plaatsvinden bijvoorbeeld in geval van louter opslag, instellen rechtsvordering en ter bescherming van rechten van anderen.
- **Dataportabiliteit**: De betrokkene heeft het recht op overdraagbaarheid van gegevens, hetgeen inhoudt dat de betrokkene het recht heeft om zijn persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm te ontvangen en deze ongehinderd aan een andere verantwoordelijke 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.

- **Bezwaar:** Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens. Het Fonds zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

- **Indienen van verzoek:** Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de e-mail ingediend worden. Het Fonds heeft in beginsel vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. 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 het verzoek niet wordt opgevolgd, 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. Het inroepen van alle rechten is in beginsel kosteloos, echter indien het verzoek kennelijk ongegrond of buitensporig is mag het Fonds hetzij redelijke kosten vragen voor het inwilligen van het verzoek of het verzoek weigeren.

Met de verwerker AZL zijn afspraken hoe de verzoeken van betrokkenen dienen te worden behandeld en dat is ook uitgewerkt in een procedure “AVG rechten van betrokkenen”.

# 5. Verplichtingen verantwoordelijke

## 5.1 Register van verwerkingen

Het Fonds is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan het Fonds de verantwoordelijke is. Elk register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:

- De naam en contactgegevens van de verantwoordelijke en, mogelijk, de gezamenlijke verantwoordelijke;
- De doelen van de verwerking;
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- Een beschrijving van de ontvangers van de persoonsgegevens;
- Een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van de beveiligingsmaatregelen.

Ook verwerkers moeten een soortgelijk register aanhouden, waarin per pensioenfonds inzichtelijk is welke categorieën verwerkingen voor het pensioenfonds worden uitgevoerd. De registers moeten op verzoek aan de AP worden verstrekt. De registers dienen als bewijs dat het Fonds en de verwerkers de AVG naleven. Om die reden moeten de registers schriftelijk worden vastgelegd. Dat kan ook in elektronische vorm (database).

## 5.2 Gegevensbeschermingseffectbeoordeling (PIA)

Met een gegevensbeschermingseffectbeoordeling, ook wel aangeduid met Privacy Impact Assessment (PIA), worden de effecten en risico’s van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Het Fonds voert deze uit indien een gegevensverwerking een hoog privacyrisico oplevert voor betrokkenen. Volgens de AVG is hiervan sprake indien het Fonds:

- systematisch en uitvoerig persoonlijke aspecten evalueert (gebaseerd op geautomatiseerde verwerking), waaronder profilering en waarop besluiten worden gebaseerd waaraan rechtsgevolgen voor betrokkenen zijn verbonden;
- op grote schaal bijzondere persoonsgegevens of strafrechtelijke gegevens 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.

Vooralsnog gaat het Fonds ervan uit, dat het niet noodzakelijk is om een PIA uit te voeren.

### 5.3 Geautomatiseerde verwerkingen

Betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft. Profilering komt bijvoorbeeld voor indien betrokkene een overeenkomst wenst af te sluiten en voordat de overeenkomst tot stand komt eerst een creditscore van betrokkene wordt opgevraagd om na te gaan of betrokkene voldoende kredietwaardig is. Dit is veelal een geheel geautomatiseerd proces, waarbij geen menselijke tussenkomst plaatsvindt. Het Fonds maakt vooralsnog geen gebruik van geautomatiseerde beslissingen noch van profilering. Indien daarvan sprake zal zijn, dan zullen daar specifieke eisen aan worden gesteld.

### 5.4 Privacy by design & default

Privacy by design beginsel 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 betrokkenen. Wanneer een dataset wordt samengesteld, dient bijvoorbeeld het beginsel van dataminimalisatie te worden toegepast. Daarnaast kunnen persoonsgegevens worden gepseudonimiseerd, zodat zij niet direct herleidbaar zijn tot een persoon. Zo worden de direct herleidbare naw-gegevens van betrokkene gesplitst van de overige gegevens, en bijvoorbeeld met een encrypte sleutel opgeslagen. Voorstelbaar is dat in het systeem een dergelijk ontwerp wordt geïmplementeerd, indien met name bijzondere en/of gevoelige persoonsgegevens worden verwerkt. Voorts dat de standaard instelling bijvoorbeeld van de website van het Fonds is ingeschakeld op de “privacy-vriendelijke” instelling. Indien het Fonds bijvoorbeeld tracking cookies wenst te gebruiken, dan is deze standaard uitgeschakeld (default), dus daarvan wordt geen gebruik gemaakt, tenzij betrokkene daarvoor zijn uitdrukkelijke toestemming heeft gegeven.

### 5.5 Datalekken

Bij een datalek gaat het om in handen komen van persoonsgegevens bij ongeautoriseerde personen, als gevolg van een inbreuk op de beveiliging. Bij een datalek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking, hetgeen dus niet de bedoeling is van het Fonds. Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker. De nu al bestaande meldplicht datalekken blijft onder de artikelen AVG grotendeels hetzelfde. De verantwoordelijke, dus het Fonds, 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.

Als er wel een hoog risico is en het Fonds 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 Fonds ook verplichten tot melding aan de deelnemers.
Zie voor de uitwerking van de melding de procedure datalekken van het Fonds.

## 6. Verwerkers

### 6.1 Uitbesteding aan een verwerker

De verantwoordelijke is de entiteit die het doel van en de middelen voor de verwerking van persoonsgegevens bepaalt. De verwerker is de partij die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt. De verwerker heeft een uitvoerende taak en heeft geen zeggenschap over de wijze van

verwerken. Essentieel is dat de gegevens alleen in opdracht van de verantwoordelijke mogen worden verwerkt en niet voor eigen doeleinden door de verwerker. Het gaat om uitbestede / gedelegeerde verwerkingsactiviteiten, die een verantwoordelijke ook zelf had kunnen verrichten.

*Voorbeeld: het verwerken van de pensioenadministratie van het Fonds door een pensioenuitvoerings-organisatie.*

In de praktijk wordt wel gedacht dat met iedere derde partij waarmee persoonsgegevens worden uitgewisseld een verwerkersovereenkomst moet worden gesloten. Dat is niet het geval. Bijvoorbeeld indien persoonsgegevens dienen te worden aangeleverd aan het CBS, de belastingdienst en het UWV. Al deze instanties of derden verwerken de gegevens op grond van hun eigen (wettelijke) taken en zijn zelf verantwoordelijke voor de gegevensverwerking. Een verwerkersovereenkomst is alleen nodig voor zover de betreffende derde partij (deels) zich kwalificeert als verwerker.

Indien het Fonds persoonsgegevens laat verwerken door een verwerker, wordt de uitvoering van de verwerkingen geregeld in een schriftelijke overeenkomst tussen het Fonds als de verantwoordelijke en de verwerker. Daarin worden in ieder geval de in 6.2 genoemde eisen opgenomen.

## 6.2 Eisen verwerkersovereenkomst

**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, dit kan het best in een bijlage worden vastgelegd.

**Instructies verwerking & geheimhouding**
De verwerking vindt uitsluitend plaats op basis van schriftelijke instructies van het Fonds. De verwerker mag de persoonsgegevens niet voor eigen (commerciële) doeleinden gebruiken. Als een instructie een inbreuk oplevert op de AVG stelt de verwerker het Fonds hier onmiddellijk van op de hoogte. Personen in dienst van of werkzaam voor verwerker hebben een geheimhoudingsplicht.

**Beveiliging**
De verwerker garandeert passende technische en organisatorische maatregelen om de verwerking te beveiligen; daarbij gelden de navolgende eisen:

- de verwerker werkt conform de maatregelen genoemd in de meest recente ISO27001 norm of soortgelijke standaarden;
- het vermogen om op permanente basis de vertrouwelijkheid, de integriteit, de beschikbaarheid en de veerkracht van de verwerkingssystemen en diensten te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid en de toegang tot de persoonsgegevens tijdig te herstellen;
- Een procedure voor het jaarlijks testen, beoordelen en evalueren van de doeltreffendheid van de technische maatregelen ter beveiliging van de verwerking en bij geconstateerde manco's zal de verwerker zo spoedig mogelijk voor eigen rekening aanvullende beveiligingsmaatregelen treffen;
- logische toegangscontrole, gebruik makend van wachtwoorden;
- fysieke maatregelen voor toegangsbeveiliging;
- automatische logging van alle handelingen rond de persoonsgegevens;
- pseudonimisering en encryptie (versleuteling) van digitale bestanden met persoonsgegevens;
- organisatorische maatregelen voor toegangsbeveiliging;
- beveiliging van netwerkverbindingen via Secure Socket Layer (SSL) technologie;
- doelgebonden toegangsbeperkingen;
- controle op toegekende bevoegdheden;
- maatregelen ter preventie van top 10 bedreigingen zoals geformuleerd door OWASP;
- Een procedure m.b.t. melden van datalekken.

**Gegevens verwijderen**
Na afloop van de opdracht verwijdert de verwerker de persoonsgegevens of geeft de persoonsgegevens terug aan het Fonds. Ook verwijdert de verwerker alle kopieën, tenzij er een wettelijke verplichting is om de gegevens te bewaren.

**Sub-verwerkers**
De verwerker schakelt geen sub-verwerker(s) in zonder voorafgaande schriftelijke toestemming van het Fonds. De verwerker legt aan een sub-verwerker in een verwerkersovereenkomst dezelfde verplichtingen op als het Fonds aan de verwerker.

**Andere verplichtingen**
De verwerker faciliteert het Fonds om te voldoen aan zijn plichten zoals privacyrechten van aanspraak- en pensioengerechtigden en 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 in geval van een hoog risicovolle PIA. De verwerker hanteert ook ISAE3402 als raamwerk om in-control te zijn aantoonbaar te maken. Voorts draagt de verwerker zorg voor voldoende kwaliteit van de persoonsgegevens.

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

Het Fonds zorgt ervoor dat de verwerkersovereenkomsten minimaal voldoen m.b.t. bovengenoemde aspecten en ziet ook toe op de naleving daarvan. Daartoe wordt een monitoringsproces ingericht en jaarlijks wordt daarover gerapporteerd.

**Verwerkingen buiten de EU/EER**
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. Het Fonds en zijn verwerkers passen de nieuwe privacyregels dus ook toe 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.

Het is belangrijk om de afspraken hierover goed vast te leggen in de verwerkersovereenkomst. Bij doorgifte buiten de EU wordt door het Fonds nagegaan of doorgifte is toegestaan. Er zijn enkele mogelijkheden, zoals bijvoorbeeld het Privacy Shield tussen de EU en de VS, en de Europese modelcontracten (Standard Contractual Clauses).

In principe is het beleid van het Fonds dat er geen verwerking van persoonsgegevens plaatsvindt buiten de EU/EER.

# 7. Non-Compliance & Klachten

## 7.1 Non-Compliance

De Autoriteit Persoonsgegevens (AP) heeft tot taak de naleving van de verplichtingen ingevolge de AVG te monitoren en te handhaven. De AP beschikt daartoe over verschillende bevoegdheden, zoals het doen van onderzoeken, het verkrijgen van toegang tot alle bedrijfsruimten en middelen van gegevensverwerkingen. In geval van een onderzoek door het AP, zal het Fonds daaraan zijn medewerking verlenen. Voorts heeft de AP de bevoegdheid tot het opleggen van corrigerende maatregelen, oplopend van een

waarschuwing, last om betrokkenen te informeren, tot een verwerking te beperken, tijdelijk dan wel definitief. Tenslotte afhankelijk van de aard, ernst en duur van de overtreding, kan de AP forse boetes opleggen oplopend tot 20 miljoen Euro. Het is derhalve van belang dat het Fonds, betrokken gremia, de uitvoerders en alle anderen de AVG naleven.

### 7.2 Klachten & Schadevergoeding

Elke betrokkene heeft het recht om een klacht bij de AP in te dienen, indien hij van mening is dat de verwerking van hem betreffende persoonsgegevens inbreuk maakt op de AVG. De Autoriteit stelt een onderzoek in en stelt de klager in kennis van de voortgang en het resultaat van de klacht, alsmede van de mogelijkheid tot voorziening in rechte, ook tegen de AP. De AP faciliteert de indiening kosteloos en bijvoorbeeld middels een klachtenformulier.

Een betrokkene die materiele of immateriële schade heeft geleden als gevolg van een inbreuk op de AVG, heeft het recht om van de verantwoordelijke of de verwerker een schadevergoeding te ontvangen voor de geleden schade. Betrokkene kan daarbij een orgaan, organisatie of vereniging, zonder winstoog-merk, inschakelen om de klacht in te dienen dan wel de schadeclaim in te stellen.

## 8. Inwerkingtreding

Dit Privacybeleid treedt in werking na goedkeuring door het Bestuur van het Fonds op 9 april 2018 en wordt minimaal elke twee jaar door het Fonds geëvalueerd.