pensioenfonds medewerkers apotheken

Privacybeleid

juni 2023

Inhoudsopgave

Algemene bepalingen

Inleiding
De Algemene Verordening Persoonsgegevensbescherming (AVG) is op 25 mei 2016 in werking getreden en vanaf 25 mei 2018 voldoet Stichting Pensioenfonds Medewerkers Apotheken aan de regels van de AVG en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). De AVG en de UAVG hebben als doel de privacyrechten van personen te verbeteren en brengen meer en andere verantwoordelijkheden met zich mee voor organisaties die werken met persoonsgegevens. De AVG is dwingendrechtelijk van toepassing op organisaties die met persoonsgegevensbestanden werken. De Gedragslijn verwerking persoonsgegevens pensioenfondsen van de Pensioenfederatie is in werking getreden op 1 januari 2020 en geactualiseerd met ingang van 1 januari 2023. Dit beleidsdocument heeft betrekking op de gegevensverwerking van de deelnemers van het fonds op basis van het pensioenreglement en de gegevensverwerking van de bedrijfsvoering van Stichting Pensioenfonds Medewerkers Apotheken.

Doel
Het doel van het Privacybeleid van Stichting Pensioenfonds Medewerkers Apotheken is het waarborgen dat het fonds voldoet aan de (U)AVG en meer algemeen het waarborgen dat de privacy van personen wiens persoonsgegevens door het pensioenfonds (en haar uitbestedingsrelaties) worden verwerkt, worden geëerbiedigd en worden beschermd door zorgvuldig met persoonsgegevens om te gaan en deze adequaat te beveiligen. Daarnaast strekt het privacybeleid tot doel over de persoonsgegevensbescherming door het pensioenfonds verantwoording af te leggen.

Begripsbepalingen

In dit beleid zijn de definities zoals opgenomen in de statuten en reglementen van Stichting Pensioenfonds Medewerkers Apotheken van overeenkomstige toepassing, tenzij in dit beleidsstuk nadrukkelijk anders wordt bepaald. In aanvulling daarop gelden in dit beleid de volgende definities:

a. *Autoriteit Persoonsgegevens*:
de toezichthoudende autoriteit;

b. *Betrokkene:*
een geïdentificeerde of identificeerbare natuurlijke persoon waarvan het fonds de hem/haar betreffende persoonsgegevens verwerkt;

c. *Datalek*:
een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens;

d. *DPIA:*
een Data Privacy Impact Assessment (gegevensbeschermingseffectbeoordeling) dat wordt uitgevoerd indien een verwerking van persoonsgegevens een hoog risico oplevert voor de rechten en vrijheden van betrokkene(n), gelet op de aard, omvang, context en doelen daarvan, een en ander conform de eventuele nadere concretisering door de Autoriteit Persoonsgegevens.

e. *Derde:*
ieder, niet zijnde de betrokkene, de verwerkingsverantwoordelijke, de verwerker of enig persoon die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd is om persoonsgegevens te bewerken;

f. *Fonds:*
Stichting Pensioenfonds Medewerkers Apotheken, gevestigd te ‘s-Gravenhage, kantoorhoudende Neuhuyskade 92, 2596 XM ‘s-Gravenhage;

g. *Gedragslijn:*
De Gedragslijn Verwerking Persoonsgegevens Pensioenfondsen, uitgebracht door de Pensioenfederatie die op 1 januari 2020 is geïmplementeerd en met ingang van 1 januari 2023 is gewijzigd;

h. *Persoonsgegeven(s):*
Alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;

i. *Toestemming van betrokkene:*
elke vrije, specifieke en op informatie berustende ondubbelzinnige wilsuiting waarmee de betrokkene aanvaardt dat hem of haar betreffende persoonsgegevens worden verwerkt;

j. *Verwerker:*
een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

k. *Verwerking van persoonsgegevens:*
elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van persoonsgegevens;

l. *Verwerkingsverantwoordelijke:*
een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Het fonds is een Verwerkingsverantwoordelijke.

Reikwijdte

Dit beleid is van toepassing op alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens van betrokkenen, alsmede op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen door of in opdracht van het fonds. Dit beleid is voorts van toepassing op de niet geautomatiseerde verwerking van persoonsgegevens door of in opdracht van het fonds die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Doelstellingen van de verwerkingen

Het geheel van verwerkingen heeft tot doel het verwerken van persoonsgegevens ten behoeve van:

a. Het verrichten van activiteiten die verband houden met een goede uitvoering van de pensioenregelingen en andere activiteiten die bijvoorbeeld samenhangen met de statuten van het fonds alsmede het beheren van daaruit voortvloeiende relaties;
b. Het voldoen aan wettelijke verplichtingen;
c. Het ten behoeve van betrokkenen kunnen verzorgen van correcte voorlichting en/of advisering.

Een en ander uitsluitend binnen de statutaire doelstelling van het fonds en in overeenstemming met de zorgplicht van het fonds jegens betrokkenen.

Rechtmatige grondslag

De rechtmatige grondslag voor de verwerkingen is gelegen in:

a. De ondubbelzinnige toestemming die de betrokkene heeft verleend;
b. De uitvoering van de (pensioen)overeenkomst waarbij de betrokkene partij is, voor de deelnemers van de werkgevers die op vrijwillige basis bij het fonds zijn aangesloten op grond van een uitvoeringsovereenkomst;
c. Een wettelijke verplichting van het fonds voor de deelnemers van de werkgevers die op basis van de verplichtstelling van het fonds bij het fonds zijn aangesloten;
d. Het gerechtvaardigde belang van het fonds.

Hierbij worden de volgende noodzakelijkheidsgrondslagen betrokken:
a. Een verwerking is effectief als met de verwerking het gestelde doel kan worden bereikt of als dat zeer waarschijnlijk is.
b. Een verwerking is evenredig als het doel dat met de verwerking wordt nagestreefd in verhouding staat tot het feit dat persoonsgegevens worden verwerkt.
c. Bij de vraag of de verwerking subsidiair is, kijkt het pensioenfonds of het doel niet op een andere, minder ingrijpende wijze bereikt kan worden.

Alleen als de verwerking niet te baseren valt op een van de noodzakelijkheidsgrondslagen, is toestemming van de betrokkene voor de verwerking van persoonsgegevens nodig.

Het fonds kan persoonsgegevens in verband met de behartiging van gerechtvaardigde belangen verwerken. Het fonds maakt hierbij vooraf een gedegen belangenafweging van de grondrechten en fundamentele vrijheden van de betrokkene. Een belangrijke factor hierbij is in hoeverre de betrokkene redelijkerwijs mag verwachten dat verwerking met dat doel kan plaatsvinden.

Dataminimalisatie

Het fonds hanteert het uitgangspunt dat de verwerking van persoonsgegevens wordt beperkt tot wat noodzakelijk is om de doeleinden te bereiken. Daartoe vinden er zo nodig periodiek analyses plaats van de (categorieën van) verwerkingen. Binnen de dataset van een verwerking wordt dan onderzocht of alle informatie relevant en nodig is en bekeken wordt of het doel ook met minder persoonsgegevens bereikt kan worden. Dataminimalisatie betekent niet alleen het beperken van het verzamelen van de gegevens tot het hoogst nodige, maar ook dat de gegevens niet langer bewaard worden dan noodzakelijk voor het gestelde doel. Het fonds geeft

invulling aan dit beginsel door bewaartermijnen vast te stellen in het beleidsdocument “Bewaartermijnen PMA”.

Juistheid

Het fonds draagt er zorg voor dat de persoonsgegevens die zij verwerkt juist en actueel zijn. De volgende maatregelen worden uitgevoerd om de juistheid van de gegevens te borgen:

- Waar mogelijk verkrijgen van de benodigde gegevens direct van betrokkene;
- Periodieke navraag/verificatie ten aanzien van de juistheid van de gegevens bij betrokkene;
- Heldere instructies bij het opvolgen van signalen van onjuiste gegevensverwerking.

Het beoordelen van de uitwerking en naleving van bovengenoemde maatregelen maakt onderdeel uit van de periodieke monitoringsactiviteiten die geïnitieerd worden door de Functionaris van Gegevensbescherming.

Verwerkingsregister

Het fonds houdt een overzicht van de verwerkingen bij in een verwerkingsregister waarin in ieder geval per verwerking wordt gedocumenteerd:

- naam en contactpersoonsgegevens van het fonds en van de functionaris voor de persoonsgegevensbescherming;
- de verwerkingsdoeleinden;
- beschrijving van de categorieën van betrokkenen en van de persoonsgegevens;
- met welke partijen de persoonsgegevens worden gedeeld; de bewaartermijnen (waarna de persoonsgegevens worden gewist);
- een beschrijving van de genomen technische en organisatorische beveiligingsmaatregelen;
- of een Privacy impact assessment (PIA) noodzakelijk is, is uitgevoerd en of naar aanleiding daarvan extra maatregelen zijn getroffen.

Het verwerkingsregister wordt op verzoek aan de Autoriteit Persoonsgegevens verstrekt.

Verwerking van persoonsgegevens

De volgende verwerkingen zijn te onderscheiden:

1. Verwerkingen ten behoeve van het uitvoeren van de pensioenovereenkomsten;
2. Verwerkingen ten behoeve van het uitvoeren van overeenkomsten;
3. Verwerkingen door het fonds als werkgever/opdrachtgever van personen die werkzaamheden bij of voor het fonds verrichten;
4. Verwerkingen om te kunnen voldoen aan verplichtingen vanuit wet- en regelgeving om informatie te verstrekken aan relevante instanties;
5. Verwerkingen om de belangen van het fonds en (gewezen) deelnemers en andere aanspraak- en pensioengerechtigden veilig te stellen;
6. Verwerkingen indien een betrokkene toestemming geeft om persoonsgegevens te verwerken.

Persoonsgegevens worden in overeenstemming met de wet- en regelgeving en op behoorlijke en zorgvuldige wijze verwerkt. Het fonds verkrijgt e-mailadressen van (gewezen) deelnemers en andere aanspraak- en pensioengerechtigden ten behoeve van communicatie met deze personen op verzoek van deze personen via de MijnOmgeving van PMA.

Persoonsgegevens worden slechts verwerkt, voor zover zij, gelet op de in dit beleid

genoemde doelstellingen, toereikend en ter zake dienend zijn.

Bijzondere persoonsgegevens worden niet verwerkt, tenzij daartoe een wettelijke plicht bestaat of dit voor het doel van de verwerking van persoonsgegevens noodzakelijk is en dan alleen met toestemming van de betrokkene.

Onder bijzondere persoonsgegevens wordt verstaan (limitatief):

a. persoonsgegevens betreffende iemands godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven;
b. lidmaatschap (vak)vereniging;
c. strafrechtelijke persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

De bijzondere persoonsgegevens die het fonds verwerkt betreffen gegevens ten aanzien van ziekte en arbeidsongeschiktheid van (gewezen) deelnemers ten behoeve van de uitvoering van de pensioenregeling (dekkingen in relatie tot arbeidsongeschiktheid).

De Gedragslijn verwerking persoonsgegevens pensioenfondsen hanteert de term ‘gevoelige persoonsgegevens’. Hoewel de AVG de term ‘gevoelige persoonsgegevens’ niet kent, zijn dit gegevens die bij verlies of onrechtmatige Verwerking ongunstige gevolgen kunnen hebben voor de persoonlijke levenssfeer. Dit betreffen BSN, bankrekeningnummer of financiële gegevens. Deze persoonsgegevens worden door het fonds verwerkt conform wet- en regelgeving. Deze categorie persoonsgegevens is niet apart opgenomen in het verwerkingsregister om verwarring te voorkomen.

Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de in paragraaf ‘Doelstellingen van de verwerkingen’ genoemde doelstellingen waarvoor zij worden verzameld en/of vervolgens worden verwerkt tenzij wettelijke bepalingen een langere bewaartermijn voorschrijven. In beginsel geldt er voor deelnemersgegevens vanuit praktische overwegingen een onbeperkte bewaartermijn. Een verdere uitwerking is/wordt opgenomen in het beleidsdocument “Bewaartermijnen PMA”.

Verkrijging van persoonsgegevens

De persoonsgegevens die worden verwerkt zijn, voor zover deze niet zijn afgeleid van andere in de verwerking voorkomende persoonsgegevens, verkregen van:

a. betrokkene of zijn/haar wettelijke vertegenwoordiger;
b. de aangesloten werkgever, als bedoeld in de statuten en pensioenregelingen;
c. de gemeentelijke basisadministratie;
d. de Uitvoering Werknemersverzekeringen (UWV) en andere organisaties op het terrein van de uitvoering van de sociale verzekeringswetten;
e. de belastingdienst;
f. andere natuurlijke personen, instellingen en organisaties die door de betrokkene gemachtigd zijn tot het verstrekken van persoonsgegevens
g. Kamer van Koophandel.

Indien de persoonsgegevens worden verkregen van een derde, dan informeert het fonds de betrokkene binnen een maand na verkrijging. Bij verkrijging van persoonsgegevens via diverse instanties, zoals hierboven genoemd, is betrokkene geïnformeerd via de privacyverklaring op de website van het fonds.

Ontvanger van de persoonsgegevens

Aan de (gewezen) deelnemer en pensioengerechtigde worden de persoonsgegevens verstrekt die op hemzelf betrekking hebben alsmede de persoonsgegevens van zijn partner, gewezen partner en kinderen die in de pensioenadministratie vastgelegd zijn op grond van hun relatie met de (gewezen) deelnemer of pensioengerechtigde.

Aan de partner, gewezen partner en kinderen van de (gewezen) deelnemer of gepensioneerde deelnemer worden die persoonsgegevens verstrekt die op henzelf betrekking hebben.

Uit de pensioenadministratie worden slechts persoonsgegevens verstrekt door de werknemers van het fonds die in het kader van de aan hen opgedragen werkzaamheden deze persoonsgegevens mogen verstrekken, met dien verstande dat deze verstrekking slechts plaatsvindt voor zover deze verenigbaar is met de in paragraaf ‘Doelstellingen van de verwerkingen’ van dit beleid omschreven doelstellingen van de verwerking van persoonsgegevens.

Aan derden worden slechts persoonsgegevens verstrekt voor zover zulks voortvloeit uit het doel van de pensioenadministratie of wordt vereist op grond van enige wettelijke bepaling. Als een uit het doel van de pensioenadministratie voortvloeiende verstrekking wordt ook beschouwd de verstrekking van persoonsgegevens aan derden in het kader van een door deze derden voor het fonds uit te voeren statistisch onderzoek of opinieonderzoek ten behoeve van de ontwikkeling van het pensioenbeleid, het financieringsbeleid of het beleggingsbeleid.

In overige gevallen worden aan derden slechts persoonsgegevens verstrekt, indien de betrokkene hiermee schriftelijk heeft ingestemd.

Verstrekking van persoonsgegevens aan derden geschiedt schriftelijk of desgewenst door middel van een automatisch verwerkbare informatiedrager. De verwerkingsverantwoordelijke kan besluiten om bepaalde persoonsgegevens mondeling aan derden te verstrekken. In dat geval wordt expliciet in dat besluit vastgelegd om welke persoonsgegevens en organisaties of instellingen het gaat.

In bijlage 3 is een overzicht opgenomen aan welke organisaties persoonsgegevens worden verstrekt.

Rechten van de betrokkene

Algemeen

Iedere betrokkene heeft recht op informatie, inzage en correctie (verbetering, aanvulling, verwijdering en/of afscherming), overdraagbaarheid van gegevens, alsmede het recht van verzet, zoals geformuleerd in de volgende paragrafen. In bijlage 1 is een praktische handleiding opgesteld indien een betrokkene zich beroept op een van de rechten. Betrokkenen, zoals de (gewezen) deelnemers, pensioengerechtigden en overige aanspraakgerechtigden van het fonds, kunnen op de website van het fonds en in de privacyverklaring van het fonds lezen hoe zij gebruik kunnen maken van deze rechten.

Recht op informatie en inzage

Iedere betrokkene kan het fonds verzoeken hem of haar mee te delen of hem of haar betreffende persoonsgegevens worden verwerkt. Verstrekking van persoonsgegevens aan een betrokkene geschiedt kosteloos op een daartoe strekkend aan het fonds of de verwerker gericht verzoek. Verstrekking geschiedt schriftelijk en uiterlijk binnen een maand na indiening van het verzoek.

Het fonds heeft de mogelijkheid een termijn van maximaal 3 maanden te nemen indien er sprake is van:
- een complex verzoek; of
- een grote hoeveelheid verzoeken.
Het fonds bericht de betrokkene over deze termijn binnen een maand en geeft daarbij een onderbouwing.

Het fonds kan weigeren aan een verzoek te voldoen, indien en voor zover dit noodzakelijk is in verband met gewichtige belangen van anderen dan de verzoeker. Het fonds deelt dit de verzoeker zo spoedig mogelijk, maar uiterlijk binnen 1 maand na ontvangst van het verzoek, schriftelijk en met redenen omkleed, mee.

De betrokkene heeft het recht om het fonds te vragen of zijn persoonsgegevens worden verwerkt. Als zijn persoonsgegevens worden verwerkt dan heeft hij recht om te weten welke persoonsgegevens dat zijn en heeft hij het recht een kopie van deze persoonsgegevens op te vragen. De persoonsgegevens moeten in een gangbare elektronische vorm worden verstrekt, tenzij het verzoek op papier is gedaan of er expliciet om een papieren kopie is gevraagd.

Recht op wijziging, verwijdering en aanvulling van persoonsgegevens

Iedere betrokkene kan het fonds schriftelijk verzoeken om de persoonsgegevens die op hem of haar betrekking hebben te wijzigen, te verwijderen of aan te vullen. Het fonds deelt de verzoeker zo spoedig mogelijk, maar uiterlijk binnen vier weken na ontvangst van het verzoek, schriftelijk mee of aan het verzoek wordt voldaan:

a. indien de beslissing toewijzend is onder vermelding van de datum waarop de wijziging, verwijdering of aanvulling ingaat, en
b. indien de beslissing afwijzend is onder vermelding van de gronden van afwijzing.

Wijziging van persoonsgegevens vindt plaats indien aan het fonds is gebleken dat deze persoonsgegevens onjuist zijn.

Na afloop van de verwerking, naargelang de keuze van het fonds, wist de verwerker alle persoonsgegevens of bezorgt deze aan het fonds terug en verwijdert de verwerker bestaande kopieën, tenzij opslag van de persoonsgegevens op grond van de wet verplicht is.

Aanvulling van persoonsgegevens vindt plaats indien aannemelijk is dat deze persoonsgegevens nodig zijn met het oog op het doel van de pensioenadministratie.

Het fonds brengt de in alinea 1 onder a bedoelde beslissing ter kennis van derden aan wie hij bij zijn weten onjuiste of onvolledige persoonsgegevens heeft verstrekt, met dien verstande dat kennisgeving achterwege kan blijven indien deze niet relevant is voor deze derden of de betrokkene te kennen heeft gegeven hierop geen prijs te stellen.

Recht op beperking van de verwerking

Een betrokkene kan een verzoek op beperking van de verwerking indienen. Het fonds zal het verzoek tot beperking van de verwerking uitvoeren indien:

a. De juistheid van de persoonsgegeven wordt betwist door de betrokkene, gedurende een periode die het fonds in staat stelt de juistheid van de persoonsgegeven te controleren;
b. De verwerking door het fonds onrechtmatig is maar de betrokkene verzet zich tegen het wissen van de persoonsgegevens en verzoekt in de plaats daarvan om beperking van het gebruik ervan;
c. Het fonds heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden, maar de betrokkene heeft deze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
d. De betrokkene heeft bezwaar gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van het fonds zwaarder wegen dan die van de betrokkenen.

Binnen een maand na ontvangst van het verzet beoordeelt het fonds of dit verzet gerechtvaardigd is. Het fonds beëindigt de verwerking direct, indien het verzet gerechtvaardigd is.

Recht op overdraagbaarheid

Iedere betrokkene heeft het recht zijn persoonsgegevens die door het fonds worden verwerkt in een gestructureerde, gangbare en machineleesbare vorm te ontvangen en over te dragen aan een andere verwerkingsverantwoordelijke.

Recht van bezwaar

Een betrokkene kan met betrekking tot een verwerking op grond van paragraaf ‘Rechtmatige grondslag’ onder d schriftelijk bij het fonds een recht tot bezwaar tegen de verwerking aantekenen in verband met bijzondere persoonlijke omstandigheden.

Binnen vier weken na ontvangst van het verzetschrift beoordeelt het fonds of dit bezwaar gerechtvaardigd is.

Het fonds brengt een beslissing op een verzoek als bedoeld in het eerste alinea schriftelijk ter kennis van de betrokkene:

a. indien de beslissing toewijzend is onder vermelding van de datum waarop de wijziging, verwijdering of aanvulling ingaat, en
b. indien de beslissing afwijzend is onder vermelding van de gronden van afwijzing.

Het fonds zorgt dat de verwerking terstond beëindigd wordt, indien het fonds het bezwaar gerechtvaardigd acht.

Overige bepalingen

Het inschakelen van een verwerker

Het fonds is bevoegd de technische verwerking van persoonsgegevens te doen plaatsvinden bij derden voor zover dit noodzakelijk is in verband met een verantwoorde bedrijfsvoering en de belangen van de betrokkene hiermee niet worden geschaad. Alvorens hiertoe over te

gaan, vergewist het fonds zich ervan dat bij de betreffende derde regels ter bescherming van de persoonlijke levenssfeer van betrokkene van toepassing zijn, die een bescherming bieden gelijkwaardig aan dit beleid.

Conform beleid vindt verwerking binnen de Europese Economische Ruimte (EER) plaats. Verwerking buiten de EER is in principe uitgesloten, tenzij er vooraf toestemming voor verwerking is gevraagd voor nieuwe (sub)verwerkers in de verwerkersovereenkomst. Indien verwerking buiten de EER plaatsvindt moet worden voldaan aan wet- en regelgeving. De doorgifte van persoonsgegevens buiten de EER is slechts toegestaan in enkele gevallen:

- doorgifte op basis van een adequaatheidsbesluit (Met een dergelijk besluit geeft de Europese Commissie aan dat een derde land over een passend beschermingsniveau beschikt en dat doorgifte van persoonsgegevens is toegestaan);
- doorgifte op basis van passende waarborgen (Deze waarborgen zijn in art. 46 AVG beschreven);
- doorgifte in afwijkende situaties.

Verwerkersovereenkomst

De verwerking van persoonsgegevens door een verwerker wordt geregeld in een verwerkersovereenkomst tussen de verwerker en het fonds. In deze verwerkingsovereenkomst wordt het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen en de rechten en verplichtingen van het fonds en de verwerker omschreven.

Een verwerkersovereenkomst wordt alleen gesloten 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 AVG, in het bijzonder maatregelen om een passend beveiligingsniveau te waarborgen.

Een verwerkingsovereenkomst bepaalt onder meer dat de verwerker:

- de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van het fonds, tenzij een op de verwerker van toepassing zijnde wettelijk voorschrift hem tot verwerking verplicht;
- waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden;
- alle voorgeschreven beveiligingsmaatregelen ten aanzien van de beveiliging van de persoonsgegevens neemt;
- na afloop van de verwerking, naargelang de keuze van het fonds, alle persoonsgegevens wist of deze aan hem terugbezorgt, en bestaande kopieën verwijdert, tenzij opslag van de persoonsgegevens op grond van de wet verplicht is;
- het fonds alle informatie ter beschikking stelt die nodig is om de nakoming van de verplichtingen aan te tonen en audits, waaronder inspecties, door het fonds of een door het fonds gemachtigde controleur mogelijk maakt en eraan bijdraagt.

Beveiliging en geheimhouding

Medewerkers van het fonds voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennisnemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

Het fonds heeft passende organisatorische en technische maatregelen getroffen ter beveiliging van de persoonsgegevens, die in ieder geval bestaan uit:

- een ICT- en Informatiebeveiligingsbeleid;
- fysieke beveiliging en beveiliging van apparatuur;
- toewijzen van verantwoordelijkheden;
- toegangsbeveiliging;
- verwerkersovereenkomsten; en
- geheimhoudingsbepalingen in overeenkomsten.

Voorts zijn de nodige voorzieningen aanwezig die waarborgen dat bij verlies of beschadiging van persoonsgegevens vervanging of herstel kan plaatsvinden.

Voor een nadere beschrijving van de beveiliging van persoonsgegevens wordt verwezen naar het ICT beleid van het fonds, op te vragen bij het fonds en bijlage 2 Clean Office beleid.

Data privacy impact analyse (DPIA)

Indien de AVG hiertoe aanleiding geeft, wordt er een DPIA uitgevoerd. Hierbij kan onder andere gedacht worden aan nieuwe verwerkingen door het fonds, of wijzigingen van verwerkingen door het fonds en het toepassen van nieuwe technologieën of profileringsmethodieken. Een DPIA hoeft alleen uitgevoerd te worden als na uitvoering van een risicoanalyse de inschatting is dat waarschijnlijk sprake is van een hoog privacy-risico. Het doel van de DPIA is om inzichtelijk te maken in hoeverre voldoende technische en organisatorische maatregelen zijn getroffen om dit privacy-risico te beheersen. Als er een DPIA conform de vereiste van de AVG is uitgevoerd is de minimale frequentie 1x per drie jaar, tenzij er eerder wezenlijke wijzigingen zijn in de verwerking. Verwerking zal pas plaatsvinden als de DPIA volledig is uitgevoerd en is afgerond, inclusief implementatie van de benodigde beheersmaatregelen. Bij het uitvoeren van een DPIA zal het fonds als uitgangspunt nemen dat de omvang en de diepgang van de DPIA proportioneel is, kijkend naar onder meer de omvang van de nieuwe of gewijzigde verwerking en de gevolgen voor de betrokken persoonsgegevens.

Conform de Gedragslijn verwerking persoonsgegevens pensioenfondsen (ingangsdatum 1 juli 2019 en gewijzigd per 1 januari 2023) zal er 1x per drie jaar, tenzij daartoe eerder aanleiding is, een DPIA uitgevoerd worden op relevante/key uitbestedingspartijen

De Functionaris Gegevensbeheer (FG) zal toezicht houden op de uitvoering van de DPIA’s.

Beperking in de verwerking

Het fonds kan de uitvoering ten aanzien van verplichtingen en rechten van betrokkene en van de beginselen van verwerking van persoonsgegevens beperken conform de AVG alleen in geval van:

1. Een betrokkene beroept zich hierop (zie rechten betrokkene)
2. Er vindt pensioenbeslag plaats door een deurwaarder
3. Er loonbeslag plaatsvindt (in geval van een werknemer van het fonds)

Meldplicht datalekken

Sinds 1 januari 2016 is het fonds verplicht om een datalek te melden aan de Autoriteit Persoonsgegevens en - als een datalek waarschijnlijk ongunstige gevolgen zal hebben voor

betrokkenen - aan de betrokkenen.

De procedures voor het melden van een datalek aan de Autoriteit Persoonsgegevens en de betrokkenen zijn beschreven in de Incidentenregeling van het fonds.

Het fonds registreert de datalekken die zich in de organisatie hebben voorgedaan. Alle datalekken worden zodanig gedocumenteerd dat de Autoriteit Persoonsgegevens met deze documentatie kan controleren of aan de meldplicht van datalekken is voldaan. De registratie van een datalek bevat ten minste de feiten, de gevolgen voor de betrokkenen en de genomen maatregelen.

Controle

Op de deugdelijkheid en naleving van alle, mede op grond van dit privacybeleid getroffen, voorzieningen ter bescherming en geheimhouding van de persoonsgegevens in de pensioenadministratie vindt periodieke controle plaats.

FG & monitoring

Het fonds heeft een Functionaris Gegevensbescherming (FG) aangesteld. De FG is verantwoordelijk voor de monitoring van het privacybeleid van het fonds en het blijven voldoen aan de AVG en Gedragslijn verwerking persoonsgegevens pensioenfondsen van de Pensioenfederatie.

De naleving van de AVG en de Gedragslijn verwerking persoonsgegevens pensioenfonds wordt jaarlijks getoetst door de FG, waarbij het volgende proces wordt gevolgd:

- De FG rapporteert zijn bevindingen aan het bestuur van het fonds;
- Het bestuur van het fonds legt aan de hand van de rapportage van de FG verantwoording af over de naleving van de AVG en deze Gedragslijn. Het fonds verklaart jaarlijks of zij zich heeft gehouden aan de AVG en deze Gedragslijn. Deze verklaring wordt opgenomen in het jaarverslag van het fonds.

De FG vervult een onafhankelijke (adviserende en toetsende) rol ten aanzien van het privacybeleid en draagt er zorg voor dat er geen conflicterende belangen ontstaan in de organisatie.

Onafhankelijke toetsing

Onafhankelijke toetsing (op onderdelen van het privacy framework) zal periodiek plaatsvinden in een (meerjaarlijks) risk-based audit-aanpak.

Klachten

Wanneer een betrokkene het niet eens is met de manier waarop het fonds zijn persoonsgegevens verwerkt of de manier waarop wordt omgegaan met de uitoefening van de rechten die betrokkene heeft op grond van de privacywetgeving, dan kan betrokkene een klacht hierover indienen. Het fonds draagt er zorg voor dat de contactgegevens voor het indienen van een klacht in de privacyverklaring en op de website zijn terug te vinden.

Bekendmaking van het beleid

Dit beleid ligt ter inzage bij het fonds te ‘s-Gravenhage. Indien een aangesloten werkgever c.q. een betrokkene hierom verzoekt wordt dit beleid hem of haar kosteloos verstrekt. De privacyverklaring kan worden ingezien op www.pma-pensioenen.nl.

Vaststelling Privacybeleid

Dit beleid is vastgesteld door het bestuur van het fonds d.d. 16 mei 2018 en gewijzigd vastgesteld in de bestuursvergadering van 6 juni 2023.