bedrijfstakpensioenfonds schoonmaak- en glazenwassersbedrijf

Privacybeleid

Vastgesteld door het bestuur op 27 mei 2021

Inhoudsopgave

1. Inleiding

Stichting Pensioenfonds voor het Schoonmaak- en Glazenwassersbedrijf (hierna: BPF Schoonmaak of het fonds) heeft als doel binnen de wettelijke werkingssfeer de deelnemers, gewezen deelnemers, pensioengerechtigden en overige aanspraakgerechtigden te beschermen tegen de geldelijke gevolgen van ouderdom, arbeidsongeschiktheid en overlijden. Daartoe voert BPF Schoonmaak een pensioenregeling uit.

Bij de uitvoering van de pensioenregeling verwerkt BPF Schoonmaak persoonsgegevens. BPF Schoonmaak stelt daarbij het doel van en de middelen voor de gegevensverwerking vast. Daarmee is BPF Schoonmaak een ‘verwerkingsverantwoordelijke’ als bedoeld in de Algemene Verordening Gegevensbescherming van de EU (Verordening EU 2016/679 van 27 april 2016; hierna ‘AVG’). Dat betekent dat BPF Schoonmaak bepaalt welke persoonsgegevens worden verwerkt, met welk doel en op welke wijze.

Het fonds vindt het belangrijk dat er sprake is van een behoorlijke, transparante, en rechtmatige verwerking van de persoonsgegevens van betrokkenen. In het privacybeleid van BPF Schoonmaak geeft het fonds daar invulling aan door aan te geven welke uitgangspunten BPF Schoonmaak belangrijk vindt bij de verwerking van persoonsgegevens en hoe het fonds de verwerking van persoonsgegevens organiseert.

2. Doel en plaats van het privacybeleid

2.1 Doel van privacybeleid

Het doel van het privacybeleid van BPF Schoonmaak is om de uitgangspunten te beschrijven van de wijze waarop BPF Schoonmaak met de verwerking van persoonsgegevens omgaat en hoe externe partijen die BPF Schoonmaak inschakelt omgaan met de persoonsgegevens van BPF Schoonmaak.

Het privacybeleid van BPF Schoonmaak gaat verder in op de wijze waarop BPF Schoonmaak er naar streeft om de persoonsgegevens van betrokkenen te beschermen, welke maatregelen BPF Schoonmaak hiervoor heeft genomen en hoe het beschermen van persoonsgegevens wordt geborgd binnen BPF Schoonmaak.

Daarnaast moet het privacybeleid bijdragen aan een verdere bewustwording bij BPF Schoonmaak en een ieder die onder eindverantwoordelijkheid van het bestuur van het fonds persoonsgegevens van BPF Schoonmaak verwerkt.

2.2 Privacybeleid als onderdeel integraal risicomanagement

Het fonds vindt het beschermen van de persoonsgegevens belangrijk. Daarom legt BPF Schoonmaak de daarbij geldende rechten en plichten vast in dit privacybeleid.

Bij BPF Schoonmaak moet op grond van de Pensioenwet sprake zijn van een beheerst en integer uitvoeren van activiteiten. Dit privacybeleid van BPF Schoonmaak is onderdeel van de compliance en maakt daarbij deel uit van het risicomanagementbeleid van BPF Schoonmaak. Het schenden van de privacy en of het niet voldoen aan de wettelijke eisen kan financiële schade en/of reputatieschade tot gevolg hebben en daarmee in de weg staan aan het realiseren van de doelstellingen van BPF Schoonmaak.

Het verwerken van persoonsgegevens is integraal onderdeel van de kernactiviteiten van BPF Schoonmaak. De beheersing van het privacy-risico is verankerd in het beleid, de processen, de systemen en de governance van de organisatie. Hiermee is het privacybeleid onderdeel van het integraal risicomanagement en wordt het regelmatig getoetst aan opzet, bestaan en werking.

2.3 Reikwijdte van privacy-bescherming

De verwerking van persoonsgegevens betreft deelnemers, gewezen deelnemers, pensioengerechtigden en aanspraakgerechtigden, maar ook bijvoorbeeld de leden van het bestuur en het verantwoordingsorgaan van BPF Schoonmaak en van personen waarmee BPF Schoonmaak extern contacten onderhoudt. Ook verwerkt BPF Schoonmaak persoonsgegevens van de functionarissen die op grond van een wettelijke taak voor het fonds werkzaamheden verrichten en bezoekers van de website van het fonds.

De Pensioenfederatie heeft per 1 januari 2020 de Gedragslijn Verwerking Persoonsgegevens Pensioenfondsen opgesteld. Doel hiervan is om als sector te laten zien op welke manier pensioenfondsen gegevens van (gewezen) deelnemers, pensioengerechtigden of andere aanspraakgerechtigden beheren. De Gedragslijn wordt periodiek getoetst op wijzigingen in de Uitvoeringswet AVG en nieuwe interpretaties. Pensioenfondsen die lid zijn van de Pensioenfederatie zoals BPF Schoonmaak worden geacht de gedragslijn na te leven. De Gedragslijn is een integraal onderdeel van het privacybeleid.

Het privacybeleid heeft ook raakvlakken met andere beleidsterreinen van BPF Schoonmaak.

Bij de uitvoering van de pensioenregeling schakelt BPF Schoonmaak externe partijen in. Ook deze externe partijen verwerken in meer of mindere mate persoonsgegevens van BPF Schoonmaak. Allereerst geeft het privacybeleid kaders voor het uitbestedingsbeleid. Omdat BPF Schoonmaak een groot deel van zijn werkzaamheden heeft uitbesteed, is het van belang dat het richting de uitbestedingspartners vastlegt waaraan zij moeten voldoen om de persoonsgegevens te beschermen. Dit wordt vooral geborgd via het sluiten van verwerkersovereenkomsten met de betreffende uitbestedingspartner.

De meeste activiteiten met betrekking tot de verwerking van persoonsgegevens zijn uitbesteed aan APG DWS en Rechtenbeheer N.V. (hierna: APG). Zij treedt daarbij op als verwerker van BPF Schoonmaak, zoals bedoeld in de AVG. Er zijn echter ook andere verwerkers, waarmee BPF Schoonmaak verwerkingsovereenkomsten sluit.

Het borgen van een passend beschermingsniveau voor de persoonsgegevens is essentieel. Daarmee heeft het privacybeleid ook een belangrijke relatie met het IT- en het informatiebeveiligingsbeleid. In het ICT-beleid staat welke maatregelen BPF Schoonmaak heeft getroffen om de persoonsgegevens via organisatorische en technische maatregelen te beschermen.

Het privacy beleid heeft eveneens raakvlakken met het communicatiebeleid. In eerste instantie bij het opstellen van de privacyverklaring. Daarnaast ook inhoudelijk, bijvoorbeeld bij doelgroep-specifieke communicatie. Dit kan raakvlakken hebben met *profiling* als bedoeld in de AVG.

De procedure over melding van data-lekken maakt deel uit van de incidentenregeling van BPF Schoonmaak.

3. Uitgangspunten privacybeleid voortvloeiend uit wet- en regelgeving

3.1 Het verwerken van persoonsgegevens

Een persoonsgegeven is alle informatie op basis waarvan een natuurlijk persoon geïdentificeerd kan worden. Dat kan een identificatie zijn:
- op directe wijze: bijvoorbeeld een naam, het aanwijzen van iemand of een foto;
- op indirecte wijze, door het combineren van verschillende gegevens met elkaar, bijvoorbeeld als in een bestand geen naam staat, maar wel een salaris, werkgever en een geboortedatum.

Er is al snel sprake van het verwerken van persoonsgegevens. Verwerken moet dus ruim worden opgevat: niet alleen het ordenen, bewerken, wijzigen, archiveren, verspreiden en ter beschikking stellen van persoonsgegevens valt hieronder, maar ook al het opslaan, vernietigen, verzamelen en vastleggen. Dus er is in feite al sprake van een verwerkingshandeling als BPF Schoonmaak een persoonsgegeven op elektronische wijze (bijvoorbeeld per mail) ontvangt.

3.2 Verwerkingsverantwoordelijke, verwerker en betrokkene

Het fonds is de verwerkingsverantwoordelijke. Dit wil zeggen dat BPF Schoonmaak het doel en de middelen voor de verwerking van de persoonsgegevens van BPF Schoonmaak bepaalt. De (categorieën van) persoonsgegevens die BPF Schoonmaak verwerkt, worden in het verwerkingsregister opgenomen. De verwerker is degene die daadwerkelijk in opdracht van BPF Schoonmaak persoonsgegevens verwerkt. Dat kan BPF Schoonmaak zijn, maar ook externe organisaties aan wie werkzaamheden zijn uitbesteed. De betrokkene is degene van wie de persoonsgegevens worden verwerkt.

3.3 Verwerkingsbeginselen

Iedere verwerking van persoonsgegevens moet voldoen aan de in de AVG genoemde verwerkingsbeginselen:

a. ***Rechtmatig, behoorlijk en transparant.***
   Dit betekent dat de persoonsgegevens op een nette en verantwoorde wijze verwerkt moeten worden. En dat de informatieverstrekking en de communicatie eenvoudig en begrijpelijk moeten zijn. Bijvoorbeeld bij de reactie van BPF Schoonmaak op een verzoek van betrokkenen om inzage van de persoonsgegevens en bij het afhandelen van bezwaren. En bijvoorbeeld bij de privacyverklaring. Dus geen gebruik van juridische taal.

b. ***Gerechtvaardigde doeleinden.***
   De persoonsgegevens mogen alleen verwerkt worden op basis van bepaalde, op grond van de AVG toegestane gronden. Voor BPF Schoonmaak gaat het daarbij om de volgende mogelijke gronden waarop een verwerking is toegestaan.
   - De verwerking is noodzakelijk om uitvoering te kunnen geven aan een wettelijke regeling (bij de uitvoering van de pensioenregeling bij een verplichtgestelde aansluiting en bij het verstrekken van informatie aan toezichthouders).
   - De verwerking is noodzakelijk om uitvoering te kunnen geven aan de pensioenovereenkomst waarbij de betrokkene partij is (bij de uitvoering van de pensioenregeling bij een vrijwillige aansluiting).

- De verwerking vindt plaats op basis van de uitdrukkelijke toestemming van de betrokkene voor een of meer specifieke doeleinden. Dit speelt bij verwerkingen van persoonsgegevens die niet strikt noodzakelijk zijn om de pensioenregeling als zodanig te kunnen uitvoeren. Bijvoorbeeld bij het versturen van een nieuwsbrief en in het algemeen in het kader van relatiemanagement.
- De verwerking vindt plaats op basis van een gerechtvaardigd belang van BPF Schoonmaak. Op basis hiervan kan BPF Schoonmaak bijvoorbeeld onder bepaalde omstandigheden profielen aanmaken en deze profielen gebruiken voor een op de betrokkene afgestemde communicatie. Ook fraudepreventie kan een gerechtvaardigd belang zijn om persoonsgegevens te verwerken. BPF Schoonmaak maakt in beginsel geen gebruik van de verwerkingsgrond gerechtvaardigd belang .
- Het fonds kan ook persoonsgegevens verwerken in relatie tot historische, statistische en wetenschappelijke doeleinden. Bijvoorbeeld om scenario's voor de waardering van de pensioenverplichtingen en kasprojecties op te stellen.

c. ***Dataminimalisatie.***
Het fonds verwerkt alleen persoonsgegevens die toereikend, ter zake dienend en noodzakelijk zijn voor de doeleinden waarvoor ze worden verwerkt. Dit betekent dat BPF Schoonmaak zich beperkt tot een minimale gegevensverwerking. Dit betekent dat BPF Schoonmaak alleen persoonsgegevens verwerkt als het doel niet op een andere wijze bereikt kan worden. Als voor bepaalde berekeningen volstaan kan worden met bijvoorbeeld kasstroomgegevens, moeten er geen persoonsgegevens gebruikt worden. Of als in de notulen volstaan kan worden met anonieme personen, dan moeten er geen persoonsgegevens gebruikt worden.

d. ***Juist en actueel.***
Het fonds heeft een inspanningsverplichting om ervoor te zorgen dat de gehanteerde persoonsgegevens juist zijn en geactualiseerd worden indien dat nodig is. BPF Schoonmaak moet onjuiste of achterhaalde persoonsgegevens wissen. BPF Schoonmaak moet hierbij een actieve houding hebben en mag bijvoorbeeld niet afwachten totdat een betrokkene klaagt over onjuiste gegevens.

e. ***Opslagbeperking.***
Het fonds moet de persoonsgegevens niet langer in een identificeerbare vorm bewaren dan noodzakelijk is voor de doeleinden waarvoor ze worden verwerkt. BPF Schoonmaak houdt daarbij in ieder geval ook rekening met de wettelijke (minimale en maximale) bewaartermijnen. De bewaartermijnen worden in het verwerkingsregister vermeld.

Het fonds stelt dat persoonsgegevens die nodig zijn voor het berekenen van pensioenen in principe onbeperkt bewaard moeten worden (pensioenen verjaren niet tijdens het leven). In de Gedragslijn Verwerking Persoonsgegevens Pensioenfondsen wordt voor het beleid bewaartermijnen aangesloten bij het Servicedocument Bewaartermijnen van de Pensioenfederatie.

De Gedragslijn en het Servicedocument stellen beide dat pensioenfondsen een beleid bewaartermijnen moeten hebben met daarin minimale en maximale bewaartermijnen. De minimale bewaartermijn is 7 jaren na het eindigen van de deelnemersrelatie door waardeoverdracht of overlijden. Een concrete maximale

bewaartermijn noemen Gedragslijn en Servicedocument niet. Alleen dat de persoonsgegevens, zoals ook in de AVG is bepaald, niet langer bewaard mogen worden dan noodzakelijk is voor de doeleinden waarvoor de gegevens zijn verzameld of vervolgens verwerkt. Het is aan de pensioenfondsen om zelf onderbouwde invulling te geven aan de maximale bewaartermijn. Wel geeft de Gedragslijn aan dat dit een termijn van tientallen jaren kan zijn.

De AVG kent overigens geen minimale bewaartermijn, maar enkel een abstracte maximale bewaartermijn.

BPF Schoonmaak hanteert een maximale bewaartermijn van 55 jaar na het eindigen van de deelnemersrelatie door waardeoverdracht of overlijden.
Verder hanteert BPF Schoonmaak dat persoonsgegevens:

- in de tussentijdse periode vanaf 7 jaar na het eindigen van de deelnemersrelatie van de deelnemer tot 55 jaar na het eindigen van de deelnemersrelatie in retentie worden geplaatst (d.w.z. het bewaren op een wijze waarbij de groep van raadplegers beperkt is);
- na het verlopen van de bewaartermijn van 55 jaar na het eindigen van de deelnemersrelatie niet worden verwijderd, maar worden geanonimiseerd.

Gedragslijn en Servicedocument kennen niet de eis van in retentie plaatsen. Wel die van vernietiging, eventueel middels anonimiseren.

Waar nodig vindt *pseudonimisering* of *anonimisering* plaats.

- Pseudonimisering betekent dat de gegevens zodanig gescheiden worden opgeslagen dat BPF Schoonmaak eerst nog andere gegevens uit een ander beschermd bestand nodig heeft om een betrokkene te kunnen identificeren.
- Anonimisering betekent dat de gegevens sowieso geen betrekking meer hebben op identificeerbare personen en dus ook geen persoonsgegevens meer zijn. Van anonimisering is sprake bij gebruikmaking van kasstromen; de AVG is daarop niet van toepassing.

f. ***Passende organisatorisch en technische beveiligingsmaatregelen.***
Het fonds neemt zodanige technische en organisatorische maatregelen om te waarborgen dat de persoonsgegevens passend zijn beveiligd. De persoonsgegevens moeten worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen verlies, vernietiging of beschadiging. Een belangrijke maatregel om dit te waarborgen betreft het inregelen van een procedure voor het melden van data-lekken.
Passend wil zeggen dat de beveiligingsmaatregelen afgezet moeten worden tegen de aard van de persoonsgegevens en de risico's die bij de verwerking optreden. Dat blijkt bijvoorbeeld uit de gegevensbeschermingseffectbeoordeling (= DPIA: Data Protection Impact Assessment). Dat betekent dus ook dat BPF Schoonmaak afhankelijk van de aard van de te verwerken persoonsgegevens en de risico's verschillende beveiligingsniveaus kan eisen van zichzelf en van de verwerkers.
De beveiliging van persoonsgegevens is onderdeel van de DPIA en de IT-risico-analyse van BPF Schoonmaak.

Het fonds moet deze verwerkingsbeginselen constant toepassen. BPF Schoonmaak moet er verder voor zorgen dat de verwerkers die onder de verantwoordelijkheid van BPF Schoonmaak verwerkingshandelingen verrichten, deze verwerkingsbeginselen ook toepassen.

3.4 Bijzondere situaties

In deze paragraaf is een aantal bijzondere situaties met betrekking tot het verwerken van persoonsgegevens opgenomen waar BPF Schoonmaak meer dan incidenteel mee te maken krijgt of kan krijgen.

a. Toestemming

Een van de rechtsgrondslagen voor een gerechtvaardigde gegevensverwerking is toestemming. Het gaat hierbij om de toestemming van de betrokkene. Dus niet van bijvoorbeeld een werkgever. Er is sprake van geldige toestemming als de toestemming:

- in vrijheid is gegeven, zonder enige vorm van dwang;
- specifiek is, dat wil zeggen niet verstopt is in een grotere tekst, maar via een aparte vraag is vormgegeven;
- in een begrijpelijk en toegankelijke vorm en in duidelijke en eenvoudige taal is voorgelegd aan de betrokkene;
- ondubbelzinnig is, zodat er geen twijfel bestaat dat betrokkene toestemming heeft gegeven en waarvoor de betrokkene toestemming heeft gegeven; en
- via een actieve handeling van de betrokkene is gegeven.

Bij het vragen van toestemming zal BPF Schoonmaak de betrokkene ook altijd erover informeren dat de hij/zij de toestemming ook op elk moment kan intrekken.

b. Bijzondere categorieën van persoonsgegevens

Verwerking van bijzondere categorieën van persoonsgegevens (bijv. gegevens over ras, politieke opvattingen, religieuze overtuigingen, seksueel leven, vakbondslidmaatschap of genetische, biometrische of gezondheidsgegevens) is omwille van de gevoeligheid in beginsel verboden. Het verwerken van het bijzondere persoonsgegeven omtrent arbeids(on)geschiktheid is voor BPF Schoonmaak toegestaan voor zover de verwerking hiervan noodzakelijk voor de uitvoering van verplichtingen op het gebied van het arbeidsrecht: namelijk de uitvoering van de pensioenregeling.
Het fonds verwerkt deze bijzondere persoonsgegevens omtrent arbeids-(on)geschiktheid voor een goede uitvoering van de pensioenregeling die voorziet in aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene. Dat speelt bij het uitkeren van het arbeidsongeschiktheidspensioen en de premievrije voortzetting bij arbeidsongeschiktheid zoals vastgelegd in de pensioenregeling.

In het algemeen geldt dat BPF Schoonmaak in afwijking van het verbod op verwerking van bijzondere persoonsgegevens onder de volgende omstandigheden bijzondere persoonsgegevens kan verwerken:

- de betrokkene heeft daarvoor zijn uitdrukkelijke toestemming gegeven, dat wil zeggen dat er op geen enkele wijze ook maar enige twijfel mag bestaan of de betrokkene de toestemming heeft gegeven;
- de verwerking is noodzakelijk in het kader van de uitvoering van regels op het gebied van arbeids- en sociaal zekerheidsrecht;
- de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt.

Daarnaast zijn er nog specifieke uitzonderingsgronden, waarin BPF Schoonmaak bijzondere persoonsgegevens mag verwerken zoals:

- persoonsgegevens over ras en etnische afkomst uitsluitend mogen verwerkt worden als dit noodzakelijk is voor de identificatie van de betrokkene;
- biometrische gegevens uitsluitend mogen verwerkt worden als dit noodzakelijk is voor authenticatie of beveiligingsdoeleinden.

c. ***Burgerservicenummer (BSN)***
Het fonds verwerkt nationale identificatienummers, waarvan het meest gangbare voorbeeld het Burgerservicenummer (BSN) is, uitsluitend als hiervoor een wettelijke grondslag bestaat. Verwerking van het BSN zal binnen BPF Schoonmaak alleen plaatsvinden bij het pensioenuitvoeringsbedrijf aan welke BPF Schoonmaak de pensioenadministratie heeft uitbesteed.

d. ***Privacy by design en by default***
Het eventueel ontwikkelen van producten en diensten kan BPF Schoonmaak uitbesteden aan een uitbestedingspartner. Indien door of voor BPF Schoonmaak producten of diensten worden ontwikkeld wordt bij het ontwikkelen van nieuwe producten en diensten en het ontwerp van nieuwe gegevenssystemen rekening gehouden met de eisen die de privacy en de gegevensbescherming stellen aan de omgang met persoonsgegevens.

Hierbij wordt er voor zorggedragen dat de inbreuk op de privacy of persoonlijke levenssfeer bij de gegevensverwerking tot een minimum beperkt blijft.

Daartoe worden passende technische en organisatorische maatregelen genomen om de gegevensbeschermingsbeginselen, zoals het alleen verwerken van noodzakelijke gegevens, op een doeltreffende wijze uit te voeren en de bescherming van persoonsgegevens te waarborgen.

3.5 Aantonen

Het fonds moet kunnen aantonen dat het rekening houdt met de hiervoor genoemde verplichtingen die uit wet- en regelgeving voortvloeien. Dat doet BPF Schoonmaak door vastlegging van het beleid in het privacybeleid en door de genoemde uitgangspunten consequent na te leven.

4. Rechten van betrokkenen

4.1 Informatie en communicatie in het algemeen

Het fonds informeert de betrokkene over de gegevensverwerkingen. Hierna gaan wij in op de informatie die aan de betrokkene moet worden verstrekt als BPF Schoonmaak de persoonsgegevens van de betrokkene zelf ontvangt of als BPF Schoonmaak de persoonsgegevens van een ander (bijvoorbeeld van de werkgever, het UWV, de Sociale Verzekeringsbank of de gemeente) ontvangt. Deze informatieverstrekking gebeurt in principe via de privacyverklaring. De privacyverklaring staat op de website van BPF Schoonmaak en kan ook naar de betrokkene worden gestuurd.

Daarnaast moet BPF Schoonmaak informatie verstrekken in het kader van de wettelijke rechten die de betrokkene heeft ten aanzien van de verwerking van zijn of haar persoonsgegevens en/of de persoonsgegevens aanpassen dan wel overdragen of vernietigen. Het beleid van BPF Schoonmaak ten aanzien van deze rechten wordt hierna beschreven.

Uitsluitend de betreffende betrokkene heeft het recht op de hierna beschreven informatie en het recht op de uitoefening van de hierna beschreven rechten van betrokkenen. BPF Schoonmaak zal dan moeten vaststellen of het met de juiste persoon te maken heeft. In dat kader dient BPF Schoonmaak de betrokken verzoeker bij het uitoefenen van een recht te identificeren.

Het fonds heeft de werkzaamheden ten aanzien van de rechten van de betrokkenen (grotendeels) uitbesteed aan een uitbestedingspartner.

4.2 Informatieverstrekking door BPF Schoonmaak bij het ontvangen van persoonsgegevens van de betrokkene zelf of van een ander

Het fonds verstrekt de betrokkene bij het ontvangen van de persoonsgegevens van de betrokkene zelf of van een ander de volgende informatie:

a. de contactgegevens van BPF Schoonmaak;
b. de contactgegevens van de Functionaris Gegevensbescherming van wiens diensten het fonds gebruik maakt;
c. de doeleinden waarvoor de gegevens worden verwerkt;
d. de rechtsgrond van de verwerking en de gerechtvaardigde belangen als dit de rechtsgrond is;
e. de betrokken categorieën van persoonsgegevens;
f. bewaartermijnen of criteria die gebruikt worden om de bewaartermijnen te bepalen;
g. het recht op inzage, rectificatie, het wissen en beperking van de gegevensverwerking en het recht om bezwaar te maken tegen de gegevensverwerking;
h. het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP);
i. de bron waar persoonsgegevens vandaan komen als ze niet door de betrokkene zelf zijn verstrekt;
j. het bestaan van geautomatiseerde besluitvorming en/of profilering en het belang en de verwachte gevolgen van die verwerking voor de betrokkene;
k. in voorkomend geval, de (categorieën van) ontvangers van de persoonsgegevens;
l. in voorkomend geval, bij voorgenomen doorgifte van persoonsgegevens aan een land buiten de Europese unie of een internationale organisatie:

- of er een adequaatheidsbesluit van de Europese Commissie is;
- of en welke passende of geschikte waarborgen zijn getroffen en hoe en waar ze kunnen worden geraadpleegd.

Als de persoonsgegevens van de betrokkene zelf worden ontvangen, wordt de hiervoor onder a t/m l bedoelde informatie bij de verkrijging van de persoonsgegevens aan de betrokkene verstrekt. In de privacyverklaring van het fonds staat dat persoonsgegevens ook buiten de betrokkene om worden verkregen (bijvoorbeeld van de werkgever, het UWV, de Sociale Verzekeringsbank of de Gemeente) voor zover sprake is van een wettelijke bevoegdheid om persoonsgegevens te verstrekken aan het fonds .

Indien de persoonsgegevens aan een andere ontvanger worden verstrekt, verstrekt BPF Schoonmaak de informatie uiterlijk op het tijdstip waarop de gegevens voor het eerst aan die ander worden verstrekt aan de betrokkene.

De AVG bepaalt dat het verstrekken van de informatie aan betrokkenen voor de betrokkene kosteloos is. De informatieverstrekking kan achterwege blijven indien en voor zover:
- de betrokkene reeds over deze informatie beschikt;
- het informeren onmogelijk blijkt, onevenredig veel inspanning vergt of tot onevenredige uitvoeringskosten leidt.

Als BPF Schoonmaak de persoonsgegevens voor een ander doel gaat gebruiken dan waarvoor BPF Schoonmaak ze verkregen heeft, verstrekt BPF Schoonmaak ingevolge de AVG de betrokkene voor die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie.

4.3 Recht op inzage

De betrokkene heeft het recht om bij BPF Schoonmaak te vragen of er bepaalde persoonsgegevens van hem of haar bij BPF Schoonmaak worden verwerkt. Als dat het geval is heeft de betrokkene het recht om deze persoonsgegevens in te zien. Tevens heeft de betrokkene het recht op de volgende informatie over de persoonsgegevens:
a. de verwerkingsdoeleinden;
b. de categorieën van persoonsgegevens;
c. de (categorieën van) ontvangers van de persoonsgegevens;
d. indien mogelijk, hoe lang de persoonsgegevens worden bewaard;
e. het recht op rectificatie, wissen, beperking en bezwaar;
f. het recht om klacht in te dienen bij de AP;
g. de bron waar die persoonsgegevens vandaan komen, als ze niet van de betrokkene zelf afkomstig zijn;
h. het bestaan van geautomatiseerde besluitvorming, waaronder profilering, en het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Als BPF Schoonmaak de persoonsgegevens doorstuurt naar een land buiten de Europese Unie of een internationale organisatie, informeert BPF Schoonmaak de betrokkene over de passende waarborgen inzake deze doorgifte.

De informatie wordt middels een kopie verstrekt. Wanneer de betrokkene zijn verzoek elektronisch indient en niet om een andere wijze van verstrekking van de informatie verzoekt, verstrekt BPF Schoonmaak de informatie in een gangbare elektronische vorm.

4.4 Recht op rectificatie van de persoonsgegevens

Op schriftelijk verzoek van de betrokkene kan BPF Schoonmaak persoonsgegevens verbeteren of aanvullen. Onjuiste of verouderde persoonsgegevens zullen worden gecorrigeerd.
Bij een verzoek van de betrokkene om rectificatie zal BPF Schoonmaak toetsen of de verbetering of aanvulling valide is.
Het fonds is op grond van de AVG verplicht om de verwerkingsverantwoordelijken met wie de persoonsgegevens gedeeld zijn (de ontvangers van persoonsgegevens) op de hoogte te stellen van de rectificatie(s), tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt.

4.5 Recht op wissen van de persoonsgegevens

Indien de betrokkene gebruik maakt van zijn of haar recht om zijn of haar persoonsgegevens bij BPF Schoonmaak te wissen, zal BPF Schoonmaak de persoonsgegevens van de betrokkene zo snel mogelijk wissen als een van de volgende situaties van toepassing is:

a. de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins zijn verwerkt;
b. betrokkene trekt zijn of haar toestemming voor het verwerken in en dit is de enige grondslag waarop de verwerking berust of kan berusten;
c. betrokkene heeft gegrond bezwaar gemaakt tegen:
    - een verwerking op basis van onder meer de grondslag, noodzakelijk voor de behartiging van het gerechtvaardigd belang van de verwerkings-verantwoordelijke of van een derde; of
    - tegen een verwerking ten behoeve van direct marketing;
d. de persoonsgegevens zijn onrechtmatig verwerkt;
e. de persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting die op BPF Schoonmaak rust.

Het fonds stelt andere verwerkingsverantwoordelijken met wie de persoonsgegevens zijn gedeeld (ontvangers zoals het Pensioenregister) op de hoogte van het wissen van de persoonsgegevens, zodat ook deze verwerkingsverantwoordelijken maatregelen kunnen nemen. Dit informeren blijft echter achterwege als dit informeren van andere verwerkingsverantwoordelijken onmogelijk blijkt, een onevenredige inspanning en/of onevenredige uitvoeringskosten van BPF Schoonmaak vergt.

4.6 Recht op beperking van de verwerking van de persoonsgegevens

Indien de betrokkene gebruik maakt van zijn of haar recht op beperking van de verwerking, stopt BPF Schoonmaak de gegevensverwerking indien:

a. de juistheid van de persoonsgegevens worden betwist, gedurende de periode waarin het fonds de juistheid van de persoonsgegevens controleert;
b. de verwerking onrechtmatig is;
c. het fonds de persoonsgegevens niet meer nodig heeft voor de verwerkingsdoeleinden, maar de betrokkene ze nodig ten behoeve van een rechtsvordering;
d. de betrokkene bezwaar maakt tegen de verwerking op basis van de rechtsgrond gerechtvaardigd belang in afwachting van de vraag of de gerechtvaardigde belangen van BPF Schoonmaak zwaarder wegen dan die van de betrokkenen.

Wanneer de verwerking is beperkt, verwerkt BPF Schoonmaak – met uitzondering van de opslag ervan – alleen nog persoonsgegevens:

- met toestemming van de betrokkene;
- in het kader van een rechtsvordering; of
- ter bescherming van de rechten van andere personen.

Het fonds stelt verwerkingsverantwoordelijken met wie de persoonsgegevens zijn gedeeld (de ontvangers van persoonsgegevens) op de hoogte van de beperkingen van de verwerking van de persoonsgegevens, tenzij dit onmogelijk blijkt, een onevenredige inspanning en/of onevenredige uitvoeringskosten van BPF Schoonmaak vergt.

4.7 Recht op overdraagbaarheid van de persoonsgegevens

Het recht op overdraagbaarheid van persoonsgegevens (dataportabiliteit) betekent dat de betrokkene het recht heeft de persoonsgegevens over te dragen naar een andere verwerkingsverantwoordelijke. Het is een belangrijk middel in het vrije verkeer van gegevens binnen de EU. Dit leidt tot meer concurrentie, omdat iemand dan makkelijker van (commerciële) dienstverlener kan veranderen. Dit speelt echter niet of nauwelijks bij organisaties zoals een verplichtgesteld bedrijfstakpensioenfonds, zoals BPF Schoonmaak. Het recht op overdraagbaarheid van de persoonsgegevens is daarom ook geen algemeen recht.

Het recht op overdraagbaarheid geldt alleen voor de persoonsgegevens die de betrokkene zelf heeft verstrekt die bij BPF Schoonmaak geautomatiseerd worden verwerkt als dit plaatsvindt op basis van de verwerkingsgronden:
- ondubbelzinnige dan wel uitdrukkelijke toestemming van de betrokkene;
- noodzakelijk voor de uitoefening van een overeenkomst.

Het fonds zal er daarbij voor zorgen dat de betrokkene een kopie krijgt van deze persoonsgegevens. De kopie wordt aan de betrokkene verstrekt in een gestructureerde, gangbare en machine-leesbare vorm.

4.8 Bezwaarrecht tegen de verwerking van de persoonsgegevens

Een betrokkene kan in bepaalde gevallen bezwaar maken tegen het verwerken van zijn of haar persoonsgegevens. Het betreft verwerkingen die eventueel plaatsvinden op basis van de verwerkingsgrond ‘gerechtvaardigd belang’. Dat kan bijvoorbeeld spelen bij ‘profilering’ (het aanleggen van profielen) en bij ‘direct marketing’. Ook kan een betrokkene bezwaar maken wegens bijzondere omstandigheden bij het verwerken van persoonsgegevens voor wetenschappelijk of historisch onderzoek of bij het verzamelen voor statistische doeleinden.

Indien de betrokkene gebruik maakt van zijn of haar recht op bezwaar tegen gegevensverwerking op basis van de grondslag gerechtvaardigd belang, stopt BPF Schoonmaak de betreffende verwerking van persoonsgegevens, tenzij de belangen voor BPF Schoonmaak om de persoonsgegevens te verwerken zwaarder wegen dan de belangen van de betrokkene om de gegevensverwerking te staken.

Indien de betrokkene bezwaar maakt tegen de verwerking van persoonsgegevens voor direct marketing, stopt BPF Schoonmaak de verwerking onmiddellijk en onvoorwaardelijk.

Bij het verwerken van persoonsgegevens voor wetenschappelijk of historisch onderzoek of bij het verzamelen voor statistische doeleinden stopt BPF Schoonmaak met de verwerking hiervan, behalve wanneer de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang.

4.9 Geautomatiseerde individuele besluitvorming, waaronder profilering

Het fonds kan bij de pensioencommunicatie op basis van de persoonsgegevens bepaalde profielen opstellen. Artikel 48 lid 2 van de Pensioenwet geeft BPF Schoonmaak ook de opdracht te bevorderen dat de te verstrekken persoonlijke informatie aansluit bij de informatiebehoefte en kenmerken van de deelnemer, gewezen deelnemer, gewezen partner of pensioengerechtigde.

Het fonds maakt gebruik van profilering om de communicatie beter af te stemmen op de persoonlijke situatie van de deelnemer, gewezen deelnemer, gewezen partner of pensioengerechtigde. Op basis van de persoonsgegevens wordt bepaald in welke doelgroep een deelnemer, gewezen deelnemer, gewezen partner of een pensioengerechtigde ingedeeld wordt. Deze doelgroepen bepalen op welke wijze met de betreffende personen wordt gecommuniceerd en waarover. In de privacyverklaring van BPF Schoonmaak worden de deelnemers, gewezen deelnemers, gewezen partners en pensioengerechtigden hierover geïnformeerd.

Het fonds kan deze vorm van profilering toepassen op basis van de grondslag ‘gerechtvaardigd belang’. BPF Schoonmaak zal deze vorm van profilering stopzetten als de betrokkene bezwaar maakt tegen deze vorm van gegevensverwerking, tenzij uit de belangenafweging van BPF Schoonmaak blijkt dat de belangen van BPF Schoonmaak bij de betreffende vorm van profilering zwaarder wegen dan de belangen van de betrokkene bij het staken van deze profilering.

Andere vormen van profilering worden niet toegepast. In het bijzonder niet profilering die leidt tot een op een enkel op geautomatiseerde verwerking gebaseerd besluit dat rechtsgevolgen heeft voor de betrokkene of de betrokkene anderszins in aanzienlijke mate treft. BPF Schoonmaak heeft niet de intentie om de persoonsgegevens van betrokkenen aan een dergelijke geautomatiseerde verwerking van persoonsgegevens te onderwerpen.

4.10 Termijn voor het reageren op het recht van de betrokkene

Het fonds informeert de betrokkene op grond van de AVG uiterlijk binnen een maand na ontvangst van het verzoek om uitvoering van zijn of haar rechten als bedoeld in voorgaande artikelen over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van het verzoek kan deze termijn met nog eens twee maanden worden verlengd. Van deze verlenging wordt de betrokkene binnen een maand na ontvangst van het verzoek in kennis gesteld.

Als BPF Schoonmaak geen gevolg geeft aan het verzoek van de betrokken, deelt BPF Schoonmaak dat de betrokkene binnen de hiervoor aangegeven termijn gemotiveerd mee. Ook informeert BPF Schoonmaak de betrokken daarbij over de mogelijkheid om gebruik te maken van de klachtenregeling van BPF Schoonmaak, een klacht in te dienen bij de Autoriteit Persoonsgegevens en/of de mogelijkheid tot het instellen van beroep bij de rechter.

5. Plichten verwerkingsverantwoordelijke en verwerker

5.1 Verantwoordingsplicht

Als verwerkingsverantwoordelijke is BPF Schoonmaak verantwoordelijk voor een rechtmatige en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de verwerkingsbeginselen. Dat betekent dat BPF Schoonmaak:

- de verplichtingen uit de privacy wet- en regelgeving moet naleven; en
- deze naleving moet kunnen aantonen (‘accountability’).

De wijze waarop en de maatregelen waarmee BPF Schoonmaak deze verantwoordingsplicht invult, wordt beschreven in dit privacybeleid.

5.2 Gegevensbeschermingseffectbeoordeling (DPIA)

De eerste stap is de ketenanalyse: dat wil zeggen het in kaart brengen van de diverse stromen van persoonsgegevens binnen BPF Schoonmaak. Nadat deze stromen in kaart zijn gebracht kan de risicobeoordeling plaatsvinden.

De gegevensbeschermingseffectbeoordeling wordt meestal aangeduid met de afkorting (DPIA: Data Protection Impact Assessment). In het privacybeleid spreken we hierna steeds over DPIA. De DPIA houdt een risicobeoordeling in van de stromen van persoonsgegevens bij een verwerkingsverantwoordelijke. De DPIA bestaat verplicht uit de volgende onderdelen:

a. een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;
b. een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
c. een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen; en
d. de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan de AVG is voldaan.

Een DPIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacy-risico oplevert voor de betrokkenen. Dat is volgens de AVG in ieder geval zoals een organisatie:
a. systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profiling;
b. op grote schaal bijzondere persoonsgegevens verwerkt;
c. op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Voor BPF Schoonmaak is alleen sub b. eventueel van toepassing. De werkgroep van Europese privacytoezichthouders (de *WP29* genoemd) heeft een lijst van 9 criteria opgesteld om te beoordelen of er sprake is van (een kernactiviteit tot) het “op grote schaal” verwerken van (bijzondere) persoonsgegevens. Als er voldaan wordt aan 2 of meer van de genoemde 9 criteria is een DPIA verplicht. Zie:
https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacycheck/privacy-impact-assessment-pia
https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg#wat-ziet-de-avg-als-een-grootschalige-verwerking-van-persoonsgegevens-6019

https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879

Op basis van de informatie van de Autoriteit Persoonsgegevens en de lijst van de WP29 met 9 criteria heeft BPF Schoonmaak vastgesteld dat het niet verplicht is zelf een DPIA uit te voeren. De meest risicovolle verwerkingen van persoonsgegevens vinden plaats bij de uitbestedingspartner. BPF Schoonmaak beschikt zelf niet over deze persoonsgegevens.

Het fonds zal voor de overige verwerkingshandelingen, na eerst een ketenanalyse te hebben uitgevoerd, wel een risico-inschatting maken van de diverse verwerkings-handelingen die binnen BPF Schoonmaak plaatsvinden (korte DPIA). De uitkomst van deze analyse is de basis voor de classificatie van data in het kader van informatiebeveiliging. BPF Schoonmaak sluit hierbij aan bij de BIV-classificaties inzake beschikbaarheid, integriteit en veiligheid zoals deze gebruikelijk bij informatiebeveiliging worden gehanteerd.

Daarnaast wordt een analyse uitgevoerd op het risico op een data-lek. De uitkomsten van de analyse op een data-lek worden vastgelegd en ten minste jaarlijks geëvalueerd.

Bij de analyse wordt onderscheid gemaakt tussen het brutorisico (zonder de gevolgen van beheersmaatregelen mee te nemen) en het nettorisico (rekening houdend met de effectiviteit van de beheersmaatregelen):

a. Bruto risico (de inschatting van het risico indien geen rekening wordt gehouden met beheersmaatregelen):
   - Wat is de kans dat het risico zich voordoet? De kans wordt bepaald door het gebruik, het beheer en de wijze van verwerking.
   - Wat is de impact als het risico zich voordoet? De impact wordt bepaald door de classificatie van de data.

b. Wat zijn de beheersmaatregelen die zijn getroffen?
   - Is de opzet van de beheersmaatregelen effectief?
   - Is de werking van de beheersmaatregelen effectief?

c. Netto risico (het restrisico, rekening houdend met de effectiviteit van de beheersmaatregelen)
   - Wat is de kans dat het risico zich voordoet?
   - Wat is de impact als het risico zich voordoet?

Uit de risico-inschatting en de risicohouding van BPF Schoonmaak volgt een indeling van soorten persoonsgegevens en de mate waarop deze beschermd moeten worden, de dataclassificatie. Het Informatiebeveiligingsbeleid van BPF Schoonmaak moet dus aansluiten op de dataclassificatie die uit de risico-inventarisatie volgt.

5.3 Verwerkingsregister (register van verwerkingsactiviteiten)

Als verwerkingsverantwoordelijke houdt BPF Schoonmaak (lees: de uitvoerder ten behoeve van het fonds op grond van uitbesteding door het fonds) een elektronisch register van verwerkingsactiviteiten bij waarvoor BPF Schoonmaak verwerkingsverantwoordelijke is. De uitkomsten van de (periodieke) ketenanalyse worden in dit verwerkingsregister opgenomen. De voor het verwerkingsregister

noodzakelijke gegevens worden zoveel mogelijk via een bijlage bij de standaard verwerkingsovereenkomsten van BPF Schoonmaak verzameld.

In dit register worden in ieder geval de volgende gegevens opgenomen:

a. naam en contactgegevens van BPF Schoonmaak;
b. naam en contactgegevens van de functionaris gegevensbescherming;
c. de verwerkingsdoeleinden;
d. een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
e. de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
f. indien van toepassing, doorgifte aan een land buiten de Europese Unie of een internationale organisatie;
g. indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van persoonsgegevens worden gewist (bewaartermijnen);
h. indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

5.4 Verwerkersovereenkomst

Het fonds dient te borgen dat de door BPF Schoonmaak als uitgangspunt genomen privacy-normen ook door de externe partijen die persoonsgegevens van BPF Schoonmaak verwerken worden nageleefd. Daartoe sluit BPF Schoonmaak met deze externe partijen verwerkersovereenkomsten af.

Het fonds hanteert een eigen standaard voor de verwerkersovereenkomst. In deze standaard zijn de uitgangspunten van BPF Schoonmaak geborgd. BPF Schoonmaak zorg ervoor dat in de verwerkersovereenkomsten wordt opgenomen dat de externe partij die persoonsgegevens van BPF Schoonmaak verwerkt de Gedragslijn Verwerking Persoonsgegevens Pensioenfondsen naleeft. BPF Schoonmaak neemt expliciet op in alle verwerkersovereenkomsten die worden gesloten vanaf het moment van het van kracht worden van de AVG. De bestaande bewerkingsovereenkomst met de uitbestedingspartner APG is daartoe in 2019 aangepast en heet sindsdien verwerkersovereenkomst. In alle vóór het van kracht worden van de AVG gesloten verwerkersovereenkomsten wordt de nalevingsverplichting bij de eerstvolgende herziening van de verwerkersovereenkomst opgenomen.

Als de verwerkingshandelingen van een verwerker zeer specifiek zijn of omvangrijk, kan het gebruik maken van verwerkersovereenkomsten die de verwerker hanteert. BPF Schoonmaak beoordeelt deze door de verwerker opgestelde verwerkersovereenkomst op basis van een checklist die is opgenomen in de Guidance verwerking persoonsgegevens pensioenfondsen.

Via de verwerkersovereenkomsten waarborgt BPF Schoonmaak ook verwerkingen via sub-verwerkers.

Hoewel de gedragslijn stelt dat gezamenlijke verwerkingsverantwoordelijkheid bij pensioenfondsen niet voorkomt, kan BPF Schoonmaak samen met een andere organisatie het doel en de middelen voor de gegevensverwerking bepalen. BPF Schoonmaak kan op deze wijze bij andere zelfstandig verwerkingsverantwoordelijken betere waarborgen treffen voor de verwerking van de persoonsgegevens die afkomstig zijn van BPF Schoonmaak. Dat betekent dat er in deze situaties wel sprake zal zijn van een gezamenlijke verantwoordelijkheid voor de gegevensverwerking: BPF Schoonmaak en deze andere organisatie zijn dan beide verwerkingsverantwoordelijken. BPF Schoonmaak moet dan samen met deze andere organisatie (contractuele) afspraken maken over de verdeling van de verantwoordelijkheid bij deze verwerking van persoonsgegevens. Daarvan kan bijvoorbeeld sprake zijn bij de werkzaamheden van een accountant of een certificerend actuaris.

In zulke gevallen kan in plaats van een verwerkersovereenkomst een verklaring gebruikt worden waaruit in ieder geval blijkt dat BPF Schoonmaak en die andere organisatie ten aanzien van de door BPF Schoonmaak verstrekt persoonsgegevens gezamenlijk verwerkingsverantwoordelijken zijn, een zogeheten *Verklaring gezamenlijke verwerkingsverantwoordelijken*. Dit houdt in dat die andere organisatie als gezamenlijke verwerkingsverantwoordelijke in ieder geval verklaart:

- dat de betreffende gegevens door de deze organisatie alleen gebruikt zullen worden voor het doel waarvoor ze door BPF Schoonmaak zijn verstrekt en vernietigd zullen worden als ze niet meer voor dat doel nodig zijn;
- dat er bij de betreffende organisatie waaraan de persoonsgegevens worden verstrekt sprake is van passende organisatorische en technische beveiligingsmaatregelen bij de verwerking van deze persoonsgegevens;
- hoe deze organisatie zal omgaan met de verplichtingen uit artikel 13 en 14 AVG (informatieverstrekking aan de betrokkene bij ontvangen van de persoonsgegevens).
- dat de betreffende organisatie zichzelf bij de eigen verwerking van deze persoonsgegevens als verwerkingsverantwoordelijke in de zin van de AVG beschouwt en op basis daarvan eindverantwoordelijkheid draagt voor de betreffende verwerkingen die het zelf doet.

In relatie tot de aangesloten werkgevers is het niet geheel duidelijk wat de AVG precies eist bij verplichtgestelde pensioenregelingen. Werkgevers moeten er enerzijds op kunnen vertrouwen dat de door de werkgevers aan BPF Schoonmaak verstrekte persoonsgegevens van betrokkenen in overeenstemming met de regels over privacybescherming worden behandeld. Werkgevers zijn echter wettelijk verplicht de betreffende persoonsgegevens aan BPF Schoonmaak te verstrekken, zonder daar voorwaarden aan te kunnen stellen. Een verwerkersovereenkomst is ook niet passend in de situatie van een verplichtgesteld pensioenfonds. Praktisch geeft dit geen problemen, omdat BPF Schoonmaak volledig in overeenstemming met de AVG zal (moeten) handelen.

In de verhouding tot de toezichthouders DNB, AFM en de AP geldt ook een gezamenlijke verwerkingsverantwoordelijkheid, waarbij AFM, DNB en de AP ieder op transparante wijze moeten aangeven hoe zij met persoonsgegevens omgaan en hoe de verantwoordelijkheden ten aanzien van de bescherming van persoonsgegevens en de rechten van betrokkenen verdeeld zijn.

In bepaalde situaties is er sprake van ‘verwerken’ in de zin van de AVG, maar vindt er volgens de algemene opvattingen geen *verwerking* plaats van persoonsgegevens. Dat is bijvoorbeeld het geval bij adviseurs die notulen, nieuwsbrieven of andere stukken van BPF Schoonmaak ontvangen op hun computer. Of adviseurs die alleen contactgegevens van BPF Schoonmaak ontvangen. Het ontvangen leidt dan al tot een verwerkingshandeling (opslaan of vernietigen). Deze adviseurs bewerken deze persoonsgegevens vaak niet. Een verwerkersovereenkomst is dan een zeer zwaar middel. BPF Schoonmaak hanteert voor deze situaties een vertrouwelijkheidsverklaring. Met deze verklaring wordt vooral geborgd dat de gegevens alleen gebruikt zullen worden voor het doel waarvoor ze verstrekt zijn en dat de gegevens na afloop van de dienstverlening door de adviseur zullen worden vernietigd.

De bepalingen in de Verklaring gezamenlijke verwerkingsverantwoordelijken en de vertrouwelijkheidsverklaring kunnen ook in de uitbestedingsovereenkomst met de dienstverlener worden opgenomen. Een aparte verklaring is dan niet meer nodig.

In bepaalde gevallen moet een dienstverlener de vertegenwoordigers van BPF Schoonmaak identificeren, al dan niet in verband met de identificatie van de zogeheten UBO’s (Ultimate Beneficial Owner). Dat speelt bijvoorbeeld bij vermogensbeheerders in het kader van MIFID II. Identificatie betreft vaak meer gevoelige persoonsgegevens, zoals een handtekening en/of een foto. Identificatiegegevens van leden van organen van BPF Schoonmaak worden alleen verstrekt voor zover deze ook echt noodzakelijk zijn voor de identificatie. Dat wil zeggen dat bijvoorbeeld bij het verstrekken van een paspoort, identiteitskaart, rijbewijs en dergelijke het BSN en het documentnummer altijd onzichtbaar (zwart) moeten zijn. En als de foto en/of de handtekening niet nodig is, deze ook zwart gemaakt moeten worden.

5.5 Privacyverklaring

Het fonds heeft een privacyverklaring opgenomen op de website van BPF Schoonmaak. In deze verklaring worden betrokkenen geïnformeerd over het feit dat en hoe hun persoonsgegevens worden verzameld en waarvoor ze gebruikt kunnen worden.

Het fonds voldoet met de privacyverklaring aan de AVG-verplichtingen die uit artikel 13 en 14 AVG voortvloeit: de bij de eerste ontvangst van de persoonsgegevens te verstrekken informatie aan de betrokkene over de doeleinden en rechtsgronden van de verwerking van de persoonsgegevens. Ook en vooral als deze via de website plaatsvinden.

5.6 Melding data-lekken

Het fonds heeft een procedure over het melden van data-lekken opgenomen in de incidentenregeling. Daarin is geregeld hoe BPF Schoonmaak als verwerkingsverantwoordelijke omgaat met een data-lek en welke eisen BPF Schoonmaak hieraan stelt bij de verwerkers.

Indien er sprake is van een datalek die aan de Autoriteit Persoonsgegevens gemeld moet worden wordt dit door de Functionaris Gegevensbescherming gedaan.

6. Governance

Het beschermen van de persoonsgegevens valt onder de reguliere werkzaamheden van BPF Schoonmaak.

6.1 Bestuur is eindverantwoordelijk

Het bestuur identificeert en analyseert de privacy-risico's van BPF Schoonmaak. Daarnaast beheert het bestuur de risico's en implementeert het acties met betrekking tot de bescherming van persoonsgegevens. Tevens ziet het bestuur erop toe dat al het beleid voldoet aan de bescherming van persoonsgegevens.

Het bestuur kan deze taken uitbesteden aan bestuurscommissies of uitbestedingspartijen. Het bestuur blijft echter te allen tijde eindverantwoordelijk.

De verantwoordelijkheid van het opstellen en het beheren van het privacybeleid en het toezien op de naleving van het privacybeleid ligt bij het bestuur. Hiertoe laat het bestuur zich bijstaan door de functionaris gegevensbescherming (FG) uit. Daarnaast is het bestuur verantwoordelijk voor het (uiterlijk binnen 72 uur na de ontdekking) melden van data-lekken aan de Autoriteit Persoonsgegevens. Daarnaast toetst het uitvoerend bestuur op grond van de rapportages van uitbestedingspartijen of binnen deze partijen de afspraken rond privacy die BPF Schoonmaak gemaakt heeft, goed worden nagekomen.

De werkzaamheden van functie van functionaris gegevensbescherming zijn:

- informeren en adviseren over verplichtingen ten aanzien van het beschermen van persoonsgegevens;
- toezien op de naleving van de privacy-regels en op het beleid ten aanzien van de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding;
- begeleiden en adviseren bij de uitvoering en/of interpretatie van de gevolgen van eventuele DPIA's voor BPF Schoonmaak;
- samenwerken met en als contactpersoon functioneren van de Autoriteit Persoonsgegevens.

6.2 Periodieke toetsing naleving

Het fonds kan periodiek een toetsing laten uitvoeren van de naleving van het privacybeleid (inclusief de Gedragslijn Verwerking Persoonsgegevens Pensioenfondsen).

6.3 Het fonds legt verantwoording af over de naleving van de AVG

Het fonds houdt voor zijn verwerkingen die niet betrekking hebben op verwerkingen als bedoeld onder 5.3 een verwerkingsregister bij (het gaat daarbij om persoonsgegevens die niet verband houden met de uitbesteding van de pensioenregeling, bijvoorbeeld de persoonsgegevens van leden van het bestuur en verantwoordingsorgaan). Dit verwerkingsregister wordt op verzoek van de Autoriteit Persoonsgegevens ter inzage gegeven.

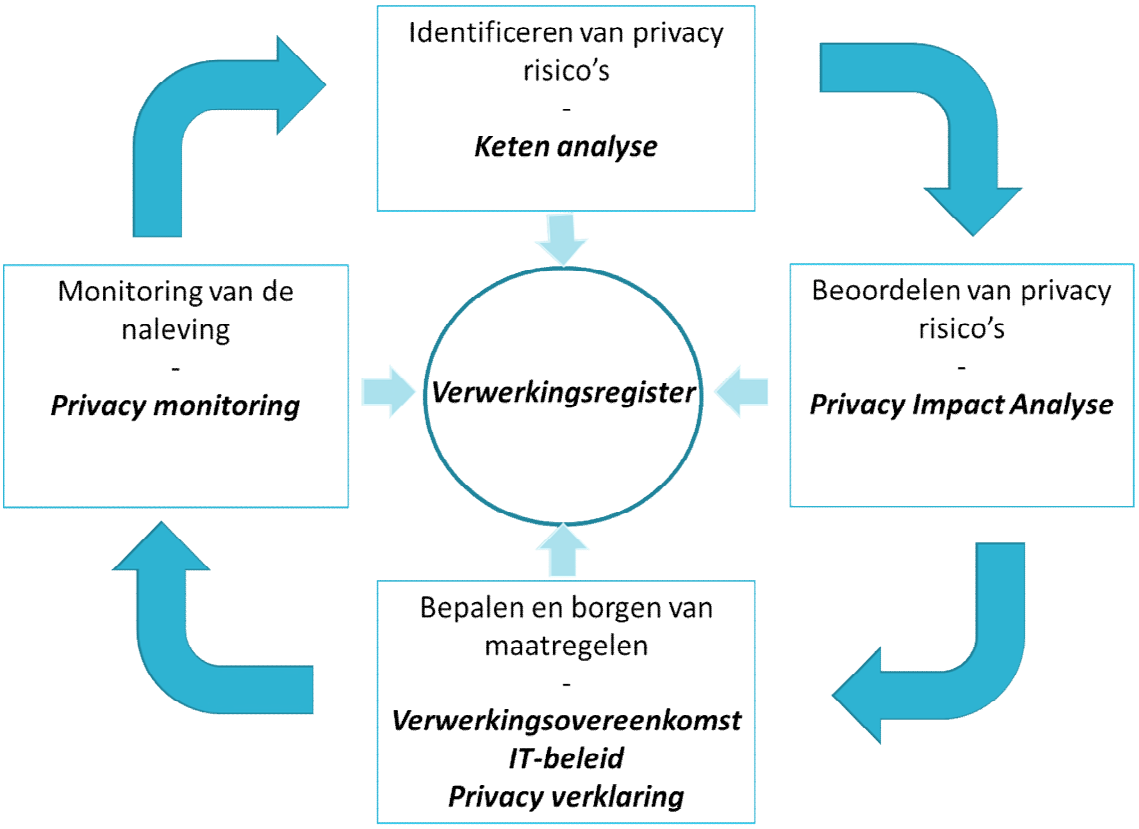
Daarnaast is het privacy-risico onderdeel van het integraal risicomanagement van BPF Schoonmaak.

De eindverantwoordelijkheid voor het naleven van de afspraken uit de AVG ligt bij het bestuur van BPF Schoonmaak. Het bestuur laat zich bijstaan door de functionaris gegevensbescherming.

Het fonds verklaart jaarlijks in het bestuursverslag of het zich heeft gehouden aan dit privacybeleid (inclusief de Gedragslijn Verwerking Persoonsgegevens Pensioen-fondsen. De vorm waarin de verantwoording wordt afgelegd wordt door het bestuur van BPF Schoonmaak bepaald.

7. Privacy proces

Schematisch weergegeven ziet het privacy risicomanagement proces van BPF Schoonmaak er als volgt uit:



Hieronder volgt een toelichting op de uitwerking van dit schema.

7.1 Ketenanalyse

Het fonds stelt een ketenanalyse op en actualiseert deze jaarlijks. Het doel van deze ketenanalyse is om:

- inzichtelijk te krijgen of BPF Schoonmaak volledig is bij de identificatie van persoonsgegevens;
- vast te stellen welke systemen worden gebruikt bij het verwerken van persoonsgegevens;
- vast te stellen van welke verwerkers BPF Schoonmaak gebruik maakt;
- de verantwoordelijkheden te identificeren.

De ketenanalyse wordt als basis gebruikt voor de risicoanalyse ten aanzien van de verwerkingen (DPIA of verkorte risico-beoordeling). Daarnaast wordt deze ketenanalyse als basis gebruikt voor het actualiseren van het verwerkingsregister van BPF Schoonmaak en het toetsen van de verwerkingsregisters van de partijen waaraan het fonds werkzaamheden heeft uitbesteed.

7.2 IT-beleid

Passende informatiebeveiliging is essentieel voor de adequate bescherming van persoonsgegevens. Hiervoor neemt BPF Schoonmaak in het IT-beleid op hoe het omgaat met de informatiebeveiliging van categorieën persoonsgegevens. Hierbij wordt rekening gehouden met de classificatie van de data op basis van de categorieën persoonsgegevens.

Aan de hand van de uitkomsten van de risicoanalyse op basis van de ketenanalyse in combinatie met de risicohouding van BPF Schoonmaak heeft BPF Schoonmaak de onderstaande dataclassificatie bepaald:

Classificatie vertrouwelijkheid	Categorie persoonsgegevens	Voorbeeld
1	Gewoon	Naam en salaris
2	Zeer gevoelig	BSN en bankrekeningnummers
3	Bijzonder	A. Persoonsgegevens waaruit blijken: 1. ras of etnische afkomst, 2. politieke opvattingen, 3. religieuze of levensbeschouwelijke overtuigingen, of, 4. het lidmaatschap van een vakbond B. Verwerking van: 1. genetische gegevens, 2. biometrische gegevens met het oog op de unieke identificatie van een persoon, 3. gegevens over gezondheid, of 4. gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Op basis van het beveiligingsniveau dat is vastgelegd in de dataclassificatie in het informatiebeveiligingsbeleid worden de noodzakelijke maatregelen bepaald.

7.3 Privacy monitoring

De periodieke monitoring van het privacy risico, is onderdeel van het integraal risicomanagement van het fonds en betreft ten minste:

- Het evalueren van de ketenanalyse en het, driejaarlijks of bij grote wijzigingen, uitvoeren van een DPIA.
- Het toetsen van de beheersmaatregelen zoals vastgesteld naar aanleiding van de (DPIA):
  - toetsen van de opzet en het bestaan;
  - toetsen van de werking.
- Het vaststellen van de naleving van het IT-beleid.
- Het monitoren van de ‘key risk indicators’ op basis van de bij de risicobereidheid gedefinieerde tolerantiegrenzen.
- Het nagaan of er in de rapportages van uitbestedingspartners melding gedaan wordt van een incident met betrekking tot de bescherming van de privacy.
- Het toetsen van de verwerkingsregisters.