Stichting Molenaarspensioenfonds

Privacybeleid

24 juni 2024

DOCUMENTMANAGEMENT

VASTSTELLING		
Versie	**Datum vastgesteld door bestuur**	**Belangrijkste wijzigingen**
1	10 DECEMBER 2018	
2	19 MEI 2020	- UITBREIDEN EN AANSCHERPEN (INTERNE) TAAKVERDELING EN (EIND)VERANTWOORDELIJKHEDEN BESTUUR - REGISTER VERWERKINGSACTIVITEITEN - UITBESTEDINGSPARTIJEN DIENEN PERIODIEK TE RAPPORTEREN OVER AVG
3	25 SEPTEMBER 2023	- AANPASSEN VERWERKINGSBEGINSELEN/IN LIJN BRENGEN MET HANDLEIDING AVG - CONSISTENTIE AANBRENGEN IN VERWIJZINGEN VERWERKINGSVERANTWOORDELIJKE - TEKSTUELE WIJZIGINGEN/ VERDUIDELIJKINGEN
4	24 JUNI 2024	OPNEMEN CATEGORIEEN PERSOONSGEGEVENS, BESCHRIJVING DOELEINDEN EN GRONDSLAGEN VERWERKING PERSOONSGEGEVENS EN BEWAARTERMIJN PERSOONSGEGEVENS.

Inhoudsopgave

1. Inleiding

Stichting Molenaarspensioenfonds (hierna: het fonds) heeft als doel binnen de kring van de aangesloten werkgevers en overeenkomstig de bepalingen van de statuten en het pensioenreglement het uitkeren of doen uitkeren van pensioenen aan de (gewezen) deelnemers en hun nabestaanden.

Bij de uitvoering van de pensioenregeling verwerkt het fonds persoonsgegevens. Het fonds stelt daarbij het doel van en de middelen voor de gegevensverwerking vast. Daarmee is het fonds een ‘verwerkingsverantwoordelijke’ als bedoeld in de Algemene Verordening Gegevensbescherming (Verordening EU 2016/679 van 27 april 2016; hierna: AVG). Dat betekent dat het fonds 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, rechtmatige, veilige en kwalitatief hoogwaardige verwerking van de persoonsgegevens van betrokkenen. In het privacybeleid van het fonds geeft het fonds daar invulling aan door aan te geven welke uitgangspunten het fonds 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 privacybeleid van het fonds beschrijft de uitgangspunten van de wijze waarop het fonds met de verwerking van persoonsgegevens omgaat en hoe de door het fonds ingeschakelde externe partijen met de persoonsgegevens van het fonds moeten omgaan.

Het privacybeleid van het fonds gaat verder in op de wijze waarop het fonds de persoonsgegevens van betrokkenen beschermt en welke maatregelen het fonds hiervoor heeft genomen.

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

2.2 Privacybeleid als onderdeel integraal risicomanagement

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

Bij het fonds moet er sprake zijn van een beheerst en integer uitvoeren van activiteiten. Dit privacybeleid van het fonds is onderdeel van de compliance en maakt daarbij deel uit van het risicomanagementbeleid van het fonds. 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 het realiseren van de doelstellingen van het fonds in de weg staan.

Het verwerken van persoonsgegevens is integraal onderdeel van de kernactiviteiten van het fonds. 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 de organen van het fonds en van personen waarmee het fonds extern contacten onderhoudt. Ook worden er door het fonds persoonsgegevens verwerkt van bezoekers van de website van het fonds.

Het privacy beleid heeft ook raakvlakken met andere beleidsterreinen van het fonds.

Bij de uitvoering van de pensioenregeling schakelt het fonds externe partijen in. Ook deze externe partijen verwerken in meer of mindere mate persoonsgegevens van het fonds. Allereerst geeft het privacybeleid kaders voor het uitbestedingsbeleid. Omdat het fonds een groot deel van zijn werkzaamheden heeft uitbesteed, is het van belang om ook naar de uitbestedingspartners vast te leggen 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 de uitvoerder Appel Pensioenuitvoering (hierna: Appel). Zij treedt daarbij op als verwerker van het fonds, zoals bedoeld in de AVG.

Het borgen van een passend beschermingsniveau voor de persoonsgegevens is essentieel. Daarmee heeft het privacybeleid ook een belangrijke relatie met het IT- en datakwaliteitsbeleid. In het IT- en datakwaliteitsbeleid staat welke maatregelen het fonds 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 profilering als bedoeld in de AVG.

3. Uitgangspunten privacybeleid voortvloeiend uit wet- en regelgeving

3.1 Het verwerken van persoonsgegevens

Een persoonsgegeven is alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. 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.

Het verwerken van persoonsgegevens moet ruim worden opgevat. Naast het ordenen, bewerken, wijzigen, archiveren, verspreiden en ter beschikking stellen van persoonsgegevens valt ook het opslaan, vernietigen, verzamelen en vastleggen daaronder.

Doel gegevensverwerking
De verwerking van persoonsgegevens dient de volgende doelen:

a. Uitvoering van de pensioenregeling van het fonds; en
b. het voldoen aan de wettelijke verplichtingen; en
c. het onderhouden van zakelijke relaties van het fonds.

Deze doelstellingen liggen in lijn met het statutaire doel van het fonds.

Grondslag gegevensverwerking
De juridische grondslag voor de verwerking van de persoonsgegevens door het fonds betreft:

a. De uitvoering van de pensioenregeling waarbij betrokkene partij is;
b. het voldoen aan wettelijke verplichtingen;
c. de toestemming van betrokkene indien de onder a en b genoemde grondslagen niet van toepassing zijn voor de betreffende verwerking.

Soorten persoonsgegevens
Het fonds verwerkt onder meer de volgende soorten persoonsgegevens:

a. Naam
b. Adres, postcode en woonplaats
c. Geboorte- en overlijdensdatum
d. Geslacht
e. Burgerlijke staat
f. Dienstverband (start en einde), pensioengevend salaris en parttimepercentage
g. Bankrekeningnummer
h. Burgerservicenummer (BSN)
i. Arbeidsongeschiktheidsgegevens vastgesteld door UWV
j. E-mailadres
k. Telefoonnummer
l. Datum ingang en einde huwelijk, aanvang geregistreerd partnerschap of gezamenlijke huishouding en echtscheidingsovereenkomsten
m. Gegevens van (ex) partners en eventuele kinderen

n. Ingangs- en einddatum van pensioenuitkeringen
o. Educatiebevestigingsbrieven
p. Identiteitsbewijs
q. Gegevens met betrekking tot de wettelijke vertegenwoordiger
r. Curriculum Vitae
s. IP adres bij gebruik van de website

3.2 Verwerkingsverantwoordelijke, verwerker en betrokkene

Het fonds is de verwerkingsverantwoordelijke. Dit wil zeggen dat het fonds het doel en de middelen voor de verwerking van de persoonsgegevens van het fonds bepaalt. De (categorieën van) persoonsgegevens die het fonds verwerkt, worden in het verwerkingsregister van het fonds opgenomen. De verwerker is degene die daadwerkelijk in opdracht van het fonds persoonsgegevens verwerkt. Dat kan het fonds zijn, maar ook een externe organisatie. 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***
   Uitgangspunt is dat persoonsgegevens alleen mogen worden verwerkt voor gerechtvaardigde doeleinden. Dit betekent dat de verwerking noodzakelijk moet zijn met het oog op het bereiken van specifiek in de AVG genoemde doelen, dan wel dat er toestemming is verkregen van diegene wiens gegevens worden verwerkt. Wanneer het gerechtvaardigd is om persoonsgegevens te verwerken, dan moet de verwerking ervan correct en verantwoord gebeuren. Duidelijk moet zijn voor welke doelen persoonsgegevens worden verwerkt en hoe dat gebeurt. Persoonsgegevens verwerken zonder dat ook maar iemand daarvan weet is niet toegestaan.
b. ***Gerechtvaardigde doeleinden (doelbinding)***
   Persoonsgegevens mogen alleen verzameld en verwerkt worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Wanneer de gegevens later voor een ander doel worden gebruikt, dan moet dat nieuwe doel verenigbaar zijn met het oorspronkelijke verzameldoel. Voor het fonds 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 verplichtgestelde aansluitingen).
   - De verwerking is noodzakelijk om uitvoering te kunnen geven aan de pensioenovereenkomst waarbij de betrokkene partij is (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.
   - De verwerking vindt plaats op basis van een gerechtvaardigd belang van het fonds.

c. ***Minimale gegevensverwerking***
   Wanneer persoonsgegevens worden verwerkt dan moeten zij voor het doel toereikend en ter zake dienend zijn. Er mogen niet meer persoonsgegevens

worden verwerkt dan noodzakelijk voor het doel. Gelet op het doel mogen er niet te veel, maar ook niet te weinig gegevens worden verwerkt, want dan kan ten onrechte een onvolledig beeld ontstaan van de betrokkene.

d. ***Juist en actueel***
Het fonds moet alle redelijke maatregelen nemen om ervoor te zorgen dat gegevens correct en actueel zijn. Gegevens die dat niet (meer) zijn, dienen te worden gewist of gecorrigeerd.

e. ***Bewaartermijn persoonsgegevens***
Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor het doel waarvoor ze zijn verzameld of waarvoor ze worden verwerkt. Wanneer gegevens niet langer nodig zijn, dan worden deze gewist/vernietigd. Het fonds houdt daarbij rekening met de geldende wettelijke (minimale en maximale) bewaartermijnen. Persoonsgegevens worden in principe bewaard tot maximaal zeven jaren na het einde van de relatie.

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). De persoonsgegevens worden daartoe opgeslagen in een niet algemeen toegankelijk archief.

Indien nodig vindt pseudonimisering of anonimisering plaats. Pseudonimisering betekent dat de gegevens zodanig gescheiden worden opgeslagen dat het fonds 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. ***Integriteit en vertrouwelijkheid***
Het fonds neemt maatregelen om te waarborgen dat persoonsgegevens worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Een belangrijke maatregel om dit te waarborgen betreft het inregelen van een procedure voor het melden van inbreuken op de beveiliging van persoonsgegevens.
De beveiligingsmaatregelen moeten worden afgezet tegen de aard van de persoonsgegevens en de risico's die bij de verwerking optreden. Dat blijkt bijvoorbeeld uit de gegevensbeschermingseffectbeoordeling (= PIA: Privacy Impact Assessment). Dat betekent dus ook dat het fonds, 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 PIA en de IT-risico-analyse van het fonds.

Het fonds en de 'medewerkers' van het fonds moeten deze verwerkingsbeginselen constant toepassen. Het fonds moet er verder voor zorgen dat de verwerkers die onder de verantwoordelijkheid van het fonds 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 het fonds 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 het fonds de betrokkene ook altijd erover informeren dat de betrokkene 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 het fonds 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 het fonds 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 persoonsgegeven die kennelijk door de betrokkene openbaar zijn gemaakt.

Daarnaast zijn er nog specifieke uitzonderingsgronden, waarin het fonds bijzondere persoonsgegevens mag verwerken zoals:

- persoonsgegevens over ras en etnische afkomst mogen verwerkt worden als dit noodzakelijk is voor de identificatie van de betrokkene of om feitelijke nadelen op te heffen;
- biometrische gegevens 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 het fonds alleen plaatsvinden bij de uitvoerder Appel.

d. Privacy by design en by default

Het ontwikkelen van producten en diensten heeft het fonds uitbesteed aan Appel. Appel houdt bij het ontwikkelen van nieuwe producten en diensten en het ontwerp van nieuwe gegevenssystemen rekening met de eisen die privacy- en gegevensbescherming stellen aan de omgang met persoonsgegevens.

Appel zorgt ervoor dat de inbreuk op de privacy of persoonlijke levenssfeer bij de gegevensverwerking tot een minimum beperkt blijft. Daartoe neemt Appel passende technische en organisatorische maatregelen 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 het fonds 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 het fonds de persoonsgegevens van de betrokkene zelf ontvangt of als het fonds de persoonsgegevens van een ander (bijvoorbeeld van de werkgever, het UWV, de Sociale Verzekeringsbank of de gemeente) ontvangt. Deze informatieverstrekking gebeurt via de privacyverklaring. De privacyverklaring staat op de website van het fonds en kan ook naar de betrokkene worden gestuurd.

Daarnaast moet het fonds 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 het fonds ten aanzien van deze rechten wordt hierna beschreven.

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

Het fonds heeft de werkzaamheden ten aanzien van de rechten van de betrokkenen uitbesteed aan Appel. Alle verzoeken die betrekking hebben op de onderstaande rechten en die binnenkomen bij het fonds, worden doorverwezen naar Appel voor de verdere afhandeling. Het fonds blijft te allen tijde eindverantwoordelijk voor de navolging van deze verzoeken.

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

Het fonds verstrekt de betrokkene bij het ontvangen van de persoonsgegevens de volgende informatie:

a. de contactgegevens van het fonds;
b. de contactgegevens van de Functionaris Gegevensbescherming van het fonds (indien die er is);
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 hier bedoelde informatie bij de verkrijging van de persoonsgegevens aan de betrokkene verstrekt. Indien de persoonsgegevens buiten de betrokkene om worden verkregen (bijvoorbeeld van de werkgever, het UWV, de Sociale Verzekeringsbank of de gemeente) verstrekt het fonds de informatie uiterlijk binnen een maand na de verkrijging van de persoonsgegevens aan de betrokkene. Indien de persoonsgegevens aan een andere ontvanger worden verstrekt, verstrekt het fonds de informatie uiterlijk op het tijdstip waarop de gegevens voor het eerst aan die ander worden verstrekt aan de betrokkene.

Het verstrekken van de informatie aan betrokkenen gebeurt voor de betrokkene kosteloos. 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 het fonds de persoonsgegevens voor een ander doel gaat gebruiken dan waarvoor het fonds ze verkregen heeft, informeert het fonds de betrokkene vóór die verdere verwerking en verstrekt de betrokkene alle relevante informatie.

4.3 Recht op inzage

Iedere betrokkene heeft het recht om de persoonsgegevens die van hem zijn verzameld in te zien. De betrokkene heeft daarom het recht om aan het fonds, met redelijke tussenpozen, te vragen of, en zo ja welke, persoonsgegevens van hem worden verwerkt. Het fonds is verplicht om gehoor te geven aan dergelijke verzoeken en de beschikbare informatie te verstrekken. Het kan hierbij onder andere gaan om de volgende gegevens:
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 het fonds de persoonsgegevens doorstuurt naar een land buiten de Europese Unie of een internationale organisatie, informeert het fonds 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 het fonds de informatie in een gangbare elektronische vorm.

4.4 Recht op rectificatie en aanvulling

Op schriftelijk verzoek van de betrokkene moet het fonds persoonsgegevens verbeteren of aanvullen. Onjuiste of verouderde persoonsgegevens worden gecorrigeerd.
Bij een verzoek van de betrokkene om rectificatie zal het fondsen toetsen of de verbetering of aanvulling valide is.
Het fonds stelt verwerkers met wie de persoonsgegevens gedeeld zijn (de ontvangers van persoonsgegevens) op de hoogte van de rectificatie(s), tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt.

4.5 Recht op gegevenswissing

Betrokkene heeft recht op het wissen van zijn persoonsgegevens, indien:

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 het fonds rust.

Indien het technisch onmogelijk is de betreffende persoonsgegevens te wissen dan wel wanneer dit enkel mogelijk is tegen hoge kosten, zal het fonds de persoonsgegevens afdoende afschermen.

Het fonds stelt andere verwerkers met wie de persoonsgegevens zijn gedeeld (ontvangers zoals het Pensioenregister) op de hoogte van het wissen van de persoonsgegevens, zodat ook deze verwerkers maatregelen kunnen nemen. Deze handeling kan echter achterwege blijven als het informeren van andere verwerkers onmogelijk blijkt, een onevenredige inspanning en/of onevenredige uitvoeringskosten van het fonds vergt.

4.6 Recht op beperking van de verwerking

Betrokkene heeft recht op beperking van de verwerking, indien:

a. de juistheid van de persoonsgegevens worden betwist;
b. de verwerking onrechtmatig is;
c. het fonds de persoonsgegevens niet meer nodig heeft voor de verwerkingsdoeleinden, maar de betrokkene ze nodig heeft voor de instelling, uitoefening of onderbouwing 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 het fonds zwaarder wegen dan die van de betrokkenen.

Wanneer de verwerking is beperkt, verwerkt het fonds – 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 verwerkers 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 het fonds vergt.

4.7 Recht op overdraagbaarheid (dataportabiliteit)

Betrokkene heeft het recht persoonsgegevens over te dragen naar een andere verwerker. Het is een 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 verplichtgestelde bedrijfstakpensioenfonds. Het recht op overdraagbaarheid van de persoonsgegevens is daarom ook geen algemeen recht.

Het recht op overdraagbaarheid geldt alleen voor de door de betrokkene zelf verstrekte persoonsgegevens die bij het fonds 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 zorgt ervoor dat de betrokkene een kopie krijgt van de overgedragen persoonsgegevens. De kopie wordt aan de betrokkene verstrekt in een gestructureerde, gangbare en machine-leesbare vorm.

4.8 Recht op bezwaar

Een betrokkene kan in bepaalde gevallen bezwaar maken tegen het verwerken van zijn of haar persoonsgegevens. Bezwaar kan door de betrokkene worden gemaakt tegen 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 het fonds de betreffende verwerking van persoonsgegevens, tenzij de belangen voor het fonds 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 het fonds de verwerking onmiddellijk en onvoorwaardelijk.

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

4.9 Geautomatiseerde individuele besluitvorming

Het fonds kan bij de pensioencommunicatie op basis van de persoonsgegevens bepaalde profielen opstellen. Artikel 48 lid 2 van de Pensioenwet geeft het fonds 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 geen gebruik van profilering.

4.10 Termijn voor het reageren op het recht van de betrokkene

Het fonds informeert de betrokkene 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 het fonds geen gevolg geeft aan het verzoek van de betrokken, deelt het fonds dat de betrokkene binnen de hiervoor aangegeven termijn gemotiveerd mee. Ook informeert het fonds de betrokken daarbij over de mogelijkheid om gebruik te maken van de Klachtenregeling van het fonds, 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 het fonds verantwoordelijk voor een rechtmatige en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de verwerkingsbeginselen. Dat betekent dat het fonds:

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

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

5.2 Gegevensbeschermingseffectbeoordeling (PIA)

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

De gegevensbeschermingseffectbeoordeling wordt meestal aangeduid met de afkorting (D)PIA: de (Data) Privat Impact Assessment. In het privacybeleid spreken we hierna steeds over PIA. De PIA houdt een risicobeoordeling in van de stromen van persoonsgegevens bij de verwerkingsverantwoordelijke. De PIA 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 PIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacy-risico oplevert voor de betrokkenen. Dat is volgens de AVG in ieder geval zo als een organisatie:
a. systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profilering;
b. op grote schaal bijzondere persoonsgegevens verwerkt;
c. op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied .

Voor het fonds is alleen sub b. van toepassing. De werkgroep van Europese privacy-toezichthouders heeft een lijst met negen 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 twee of meer van de genoemde negen criteria is een PIA verplicht. Zie:

Het fonds heeft voor de overige verwerkingshandelingen wel een risico-inschatting gemaakt van de diverse verwerkingshandelingen die binnen het fonds plaatsvinden. De uitkomst van deze analyse is de basis voor de classificatie van data in het kader van informatiebeveiliging. Het fonds 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 inbreuk op de beveiliging van persoonsgegevens. De uitkomsten van de analyse op een inbreuk 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 het fonds volgt een indeling van soorten persoonsgegevens en de mate waarop deze beschermd moeten worden, de dataclassificatie. Het IT- en datakwaliteitsbeleid van het fonds moet dus aansluiten op de dataclassificatie die uit de risico-inventarisatie volgt.

De PIA wordt uitgevoerd door het fonds. Het bestuur kan besluiten de PIA door een uitbestedingspartij te laten uitvoeren, maar blijft te allen tijde eindverantwoordelijk. In de verwerkersovereenkomsten is opgenomen dat uitbestedingspartijen het fonds redelijke bijstand dienen te verlenen bij het uitvoeren van een PIA.

5.3 Verwerkingsregister

Als verwerkingsverantwoordelijke houdt het fonds een elektronisch register van verwerkingsactiviteiten bij waarvoor het fonds 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 het fonds verzameld. Het bestuur heeft het bijhouden van het verwerkingsregister belegd bij Appel.

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

a. naam en contactgegevens van het fonds;
b. naam en contactgegevens van de functionaris gegevensbescherming van het fonds en van de uitvoerder Appel;
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 het fonds als uitgangspunt genomen privacy-normen ook door de externe partijen die persoonsgegevens van het fonds verwerken worden nageleefd. Daartoe sluit het fonds met deze externe partijen verwerkers-overeenkomsten af.

Het fonds hanteert een eigen standaard voor de verwerkersovereenkomst. In deze standaard zijn de uitgangspunten van het fonds geborgd.

Als de verwerkingshandelingen van een verwerker zeer specifiek zijn of omvangrijk, kan het gebruik maken van verwerkersovereenkomsten die de verwerker hanteert. Het fonds beoordeelt deze door de verwerker opgestelde verwerkersovereenkomst op basis van een checklist die het fonds daar specifiek voor heeft opgesteld.

Via de verwerkersovereenkomsten waarborgt het fonds ook verwerkingen via sub-verwerkers.

Het fonds kan ook samen met een andere organisatie het doel en de middelen voor de gegevensverwerking bepalen. Dat betekent dat er sprake is van een gezamenlijke verantwoordelijkheid voor de gegevensverwerking: het fonds en deze andere organisatie zijn dan beide verantwoordelijk. Het fonds 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 het fonds en die andere organisatie ten aanzien van de door het fonds verstrekt persoonsgegevens gezamenlijk verantwoordelijk zijn: 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 het fonds 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 het ontvangen van de persoonsgegevens).

- dat de betreffende organisatie door de eigen verwerking van deze persoonsgegevens de 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 het fonds verstrekte persoonsgegevens van betrokkenen in overeenstemming met de regels over privacybescherming worden behandeld. Werkgevers zijn echter wettelijk verplicht de betreffende persoonsgegevens aan het fonds te verstrekken, zonder daar voorwaarden aan te kunnen stellen. Een verwerkersovereenkomst is niet passend in de situatie van een verplichtgesteld pensioenfonds. Praktisch geeft dit geen problemen, omdat het fonds 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 het fonds ontvangen op hun computer. Of adviseurs die alleen contactgegevens van het fonds 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. Het fonds hanteert voor deze situaties de Verklaring vertrouwelijkheid. 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 Verklaring vertrouwelijkheid 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 het fonds identificeren. Dat speelt bijvoorbeeld bij vermogensbeheerders in het kader van MIFID II (voor efficiënter/ transparanter maken van Europese financiële markten en bescherming van beleggers). Identificatie betreft vaak meer gevoelige persoonsgegevens (zoals handtekening en/of foto). In zulke gevallen werkt het fonds met een verwerkersovereenkomst of een Verklaring gezamenlijke verwerkingsverantwoordelijken.

Identificatiegegevens van leden van organen van het fonds worden alleen verstrekt voor zover deze ook echt noodzakelijk zijn voor de identificatie. Gegevens op identificatiedocumenten die niet nodig zijn worden onherkenbaar gemaakt.

5.5 Privacyverklaring

Het fonds heeft een privacyverklaring opgenomen op de website van het fonds. 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.

De privacyverklaring en eventuele wijziging daarvan worden door het bestuur vastgesteld nadat de communicatiecommissie hierover is gehoord.

5.6 Meldplicht inbreuken

In de klokkenluiders- en incidentenregeling van het fonds is het protocol opgenomen in het geval van een inbreuk in verband met persoonsgegevens. In dit protocol is geregeld hoe het fonds als verwerkingsverantwoordelijke omgaat met een (mogelijke) inbreuk op de beveiliging van persoonsgegevens en welke eisen het fonds hieraan stelt bij de verwerkers.

Het protocol gaat in op:

- het constateren van een (mogelijke) inbreuk;
- het constateren of er een risico is bij een inbreuk en hoe hoog dit risico is;
- het al dan niet melden van een inbreuk aan de Autoriteit Persoonsgegevens;
- het administreren van een inbreuk;
- het al dan niet melden van een inbreuk aan een betrokkene.

In overleg met Appel bepaalt het fonds of er sprake is van een inbreuk die aan de Autoriteit Persoonsgegevens gemeld moet worden. De eventuele melding wordt door de Functionaris Gegevensbescherming van het fonds gedaan, in afstemming met de Functionaris Gegevensbescherming van Appel.

6. Governance

Het beschermen van de persoonsgegevens valt onder de reguliere werkzaamheden van het fonds.

6.1 Bestuur is eindverantwoordelijk

Het bestuur identificeert en analyseert de privacy-risico's van het fonds. 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 wordt hierin ondersteund door de IRM-commissie.

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

In het verwerkingsregister zijn alle activiteiten opgenomen waarbij sprake is van verwerking van persoonsgegevens. Daarbij is per activiteit aangegeven wie bij de betreffende uitbestedingspartij intern verantwoordelijk is. Ook hier geldt echter: de eindverantwoordelijkheid ligt altijd bij het bestuur.

6.2 Functionaris Gegevensbescherming

De verantwoordelijkheid van het opstellen en het beheren van het privacybeleid en het toezien op de naleving van het privacybeleid ligt bij de externe Functionaris Gegevensbescherming (FG). De FG kan het bestuur in die hoedanigheid gevraagd en ongevraagd adviseren op het gebied van privacy. Daarnaast is de FG verantwoordelijk voor het (uiterlijk binnen 72 uur na de ontdekking) melden van inbreuken op de beveiliging van persoonsgegevens aan de Autoriteit Persoonsgegevens. De IRM-commissie toetst in de rapportages van uitbestedingspartijen of binnen deze partijen de afspraken rond privacy die het fonds gemaakt heeft, goed worden nagekomen.

De werkzaamheden van de FG 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;
- begeleidt en adviseert bij de uitvoering en/of interpretatie van de gevolgen van eventuele PIA's voor het fonds;
- samenwerken met en als contactpersoon functioneren van de Autoriteit Persoonsgegevens.

Het bestuur draagt er zorg voor dat de FG deze functie goed kan uitvoeren door de FG tijdig bij ontwikkelingen te betrekken, met voldoende bevoegdheden en middelen.

6.3 Externe audit

Het bestuur kan verder indien dat nodig wordt geacht onafhankelijke audits laten uitvoeren op privacy en IT.

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

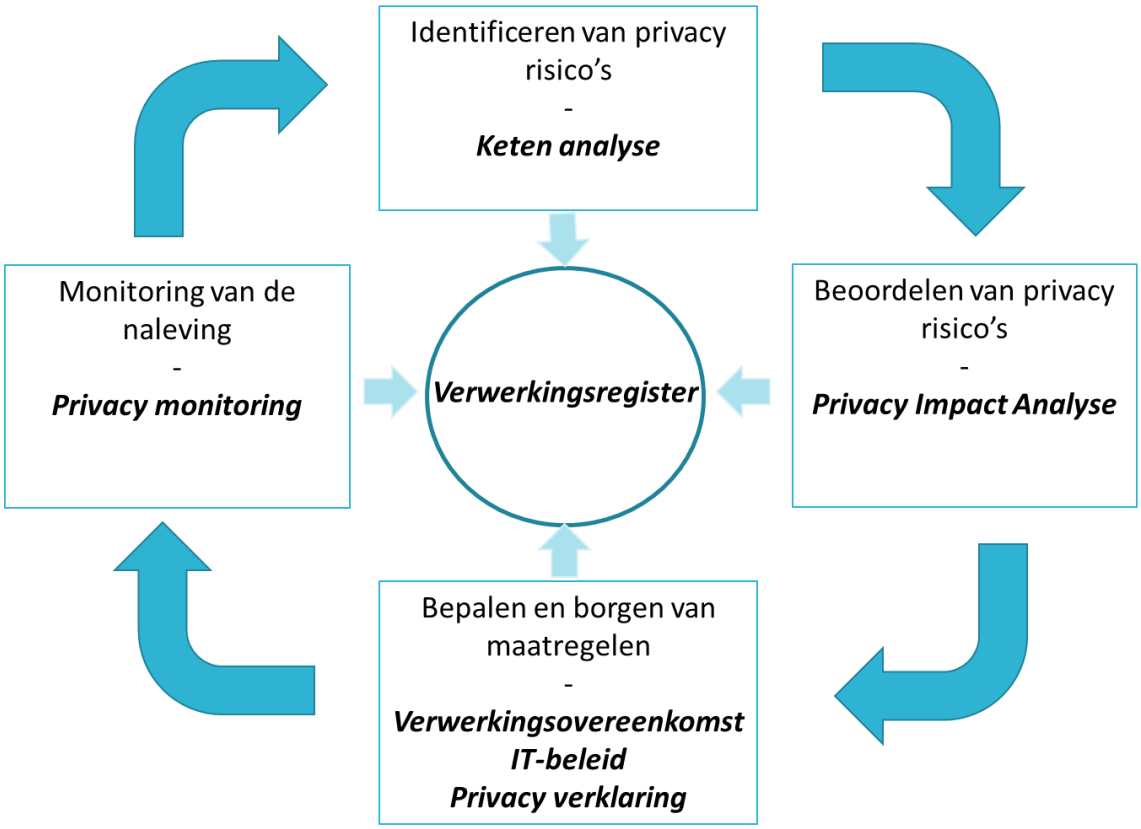
Het fonds houdt voor zijn eigen verwerkingen een verwerkingsregister bij. Dit verwerkingsregister wordt op verzoek van de Autoriteit Persoonsgegevens ter inzage gegeven.

Daarnaast is het privacy-risico onderdeel van het integraal risicomanagement van het fonds.

De eindverantwoordelijkheid voor het naleven van de afspraken uit de AVG ligt bij het bestuur van het fonds. Voor zover het fonds dit nodig acht rapporteren uitbestedingspartijen over de naleving van de AVG, de getroffen technische en organisatorische maatregelen, inbreuken op de AVG en de werkzaamheden ten aanzien van de rechten van betrokkenen. Afspraken over deze rapportage worden vastgelegd in de verwerkersovereenkomst.

7. Privacy proces

Schematisch weergegeven ziet het privacy risicomanagement proces van het fonds 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 het fonds 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 het fonds gebruik maakt;
- de verantwoordelijkheden te identificeren.

De ketenanalyse wordt als basis gebruikt voor de risicoanalyse ten aanzien van de verwerkingen (PIA of verkorte risico-beoordeling). Daarnaast wordt deze ketenanalyse als basis gebruikt voor het actualiseren van het verwerkingsregister van het fonds en het toetsen van de verwerkingsregisters van (sub)verwerkers.

7.2 IT- en datakwaliteitsbeleid

Passende informatiebeveiliging is essentieel voor de adequate bescherming van persoonsgegevens.

Het fonds heeft in het IT- en datakwaliteitsbeleid opgenomen 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 het fonds heeft het fonds 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 IT- en datakwaliteitsbeleid worden de noodzakelijke maatregelen bepaald.

7.3 Privacy monitoring

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

- Het jaarlijks evalueren van de ketenanalyse en driejaarlijks (als de AP dit verlangt) of bij grote wijzigingen het uitvoeren van een PIA.
- Het ten minste tweemaal per jaar toetsen van de beheersmaatregelen zoals vastgesteld naar aanleiding van een PIA:
  - toetsen van de opzet en het bestaan;
  - toetsen van de werking.
- Het per kwartaal vaststellen van de naleving van het IT- en datakwaliteitsbeleid.
- Het monitoren van de ‘key risk indicators’ op basis van de bij de risicobereidheid gedefinieerde tolerantiegrenzen.
- Per kwartaal nagaan of er in de rapportages van uitbestedingspartners melding gedaan wordt van een incident met betrekking tot de bescherming van de privacy.
- Ten minste tweemaal per jaar het verwerkingsregisters toetsen.