Privacybeleid
Stichting Pensioenfonds F. van Lanschot

Versie: 2022-09-15

Privacybeleid
Stichting Pensioenfonds F. van Lanschot

Inhoud

Privacybeleid
Stichting Pensioenfonds F. van Lanschot

1. Inleiding

1.1 Inleiding
Stichting Pensioenfonds F. van Lanschot (het pensioenfonds) verwerkt persoonsgegevens van pensioendeelnemers en personen werkzaam voor het pensioenfonds, gezamenlijk aangeduid met betrokkenen. Deze betrokkenen moeten erop kunnen vertrouwen dat het pensioenfonds, binnen de kaders van de geldende wet- en regelgeving, op een veilige en zorgvuldige manier omgaat met hun persoonsgegevens. In dit beleid is vastgelegd op welke wijze het pensioenfonds omgaat met persoonsgegevens en privacy.

1.2 Wetgeving en definities
Op de verwerking van persoonsgegevens zijn de privacyvoorschriften van de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) van toepassing. De AVG zorgt voor versterking en uitbreiding van de privacyrechten van betrokkenen en meer verantwoordelijkheden voor het pensioenfonds.

De volgende begrippen worden in de AVG gebruikt. Om aan te sluiten bij de wet, hanteert het onderhavige beleid deze begrippen ook.

Betrokkene: De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt. Voor het pensioenfonds zijn de belangrijkste betrokkenen pensioendeelnemers en personen die voor het pensioenfonds werken, beide natuurlijke personen.

Verwerker: De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie. Belangrijke verwerkers voor het pensioenfonds zijn bijvoorbeeld de pensioenuitvoeringsorganisatie en adviserend actuaris.

Persoonsgegevens: Alle gegevens die gaan over natuurlijke personen en waaraan je een natuurlijk persoon als individu kunt herkennen. Het gaat hierbij om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld; naam, adres, geboortedatum). Naast gewone persoonsgegevens kent de wet ook bijzondere categorieën van persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals gezondheidsgegevens (arbeidsongeschiktheid), politieke voorkeuren, godsdienst of het lidmaatschap van een vakbond.

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

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

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

1.3 Scope

Het privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens die door of namens het pensioenfonds plaatsvinden.

1.4 Rollen en verantwoordelijkheden

Verantwoordelijke

Het bestuur van het pensioenfonds is verantwoordelijke voor de verwerkingen van persoonsgegevens die door of namens het pensioenfonds plaatsvinden. Daarbij neemt het pensioenfonds de privacyregelgeving in acht en draagt zij zorg voor controle daarop via invulling van een privacy officer (PO).
Het bestuur is aanspreekbaar op een veilige en zorgvuldige gegevensverwerking en moet bewijs kunnen produceren dat zij voldoet aan de eisen van de wet- en regelgeving. Dat leidt tot documentatie, zoals dit beleid, correcte verwerkersovereenkomsten, adequate beveiligingsmaatregelen en implementatie. Alsook monitoring op de correcte naleving daarvan, zoals testen, audits, registratie, evaluatie en ontwikkeling.

Privacy officer

Gelet op het feit dat het pensioenfonds op grote schaal persoonsgegevens verwerkt, heeft het bestuur een privacy officer aangesteld. De privacy officer heeft tot taak om de naleving van privacywet- en regelgeving te bevorderen. Hiertoe verstrekt deze adviezen, stelt documenten en procedures op en monitort de naleving van privacyregelgeving binnen het pensioenfonds. De privacy officer ondersteunt de bestuurders, commissieleden en het bestuursbureau zodat er voldoende aandacht is voor privacy. Voorts brengt de privacy officer verslag uit over zijn activiteiten en de naleving van de privacyregelgeving.

2. Uitgangspunten voor verwerking

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

2.1 Rechtmatigheid, behoorlijkheid en transparantie

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

2.2 Doeleinden

Het pensioenfonds verwerkt de persoonsgegevens van betrokkenen voor de volgende doelen:

- Om de dienstverlening van het pensioenfonds richting betrokkenen conform de vastgestelde pensioenreglementen te kunnen uitvoeren, bijvoorbeeld om de pensioenrechten of -aanspraken of (aanvullende) inkomensverzekeringen zorgvuldig en juist te berekenen, betrokkenen daarover tijdig en correct te informeren en de uitkering stipt uit te betalen, om ALM-studies te doen en premies te berekenen.
- Om contractuele afspraken of wettelijke of internationale verplichtingen na te komen.
- Om de gebruiksvriendelijkheid van de website te verbeteren.
- Voor interne (kwaliteits)analyses en productontwikkeling. Hiermee kunnen de regelingen en dienstverlening naar betrokkenen verbeterd worden.
- Om communicatie over de pensioenzaken van betrokkenen en daarmee samenhangende onderwerpen via verschillende communicatiekanalen zo relevant en persoonlijk mogelijk te maken. Hiervoor worden programma's als Google Analytics ingezet en wordt informatie verzameld wanneer de website wordt bezocht en welke onderwerpen worden bekeken. Er worden niet tot de persoon herleidbare gegevens verzameld en er wordt voldaan aan de privacyvriendelijke instellingen, zoals vereist door de Autoriteit Persoonsgegevens (AP).

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

2.3 Rechtmatige grondslag

Verwerking van persoonsgegevens mag alleen plaatsvinden, indien:

a) De betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens; een voorbeeld hiervan is toestemming voor het gebruik van tracking cookies op de website van het pensioenfonds.
b) De verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is (inclusief precontractuele maatregelen), zoals de pensioenovereenkomst tussen de werkgever en de werknemers.
c) Het pensioenfonds wettelijk verplicht is de verwerking uit te voeren; denk hierbij aan alle voorschriften uit de Pensioenwet of fiscaal verplichte administratieve taken.
d) Een eigen gerechtvaardigd belang van het pensioenfonds of een derde, dat zwaarder weegt dan de grondrechten van de betrokkene, zoals bijvoorbeeld fraudepreventie; er moet sprake zijn van een belangenafweging op basis van alle omstandigheden van het geval.
   Hierbij wordt rekening gehouden met de Normuitleg "gerechtvaardigd belang" van de AP en de drie gestelde cumulatieve voorwaarden. Deze zijn: 1) behartiging van een gerechtvaardigd belang voor de verwerking van het pensioenfonds of een derde, 2) de noodzaak daartoe en 3) bij de gemaakte afweging prevaleren niet de fundamentele rechten en vrijheden van betrokkenen. Voor alle duidelijkheid, deze grondslag zal niet worden gebruikt om commerciële belangen van het pensioenfonds te dienen.

2.4 Welke gegevens en bijzondere gegevens

De verschillende persoonsgegevens worden door het pensioenfonds verzameld via onder meer, Uitvoeringsinstituut Werknemersverzekeringen (UWV), Basisregistratie Personen (BRP), de Kamer van Koophandel (KvK) en van andere pensioenuitvoerders. Daarnaast verzamelt het pensioenfonds persoonsgegevens via telefoon, e-mail en website.

Identificatie persoonsgegevens

De volgende categorieën van persoonsgegevens worden door het pensioenfonds verwerkt:

- personalia (zoals naam, adres, geboortedatum, leeftijd, geslacht, burgerlijke staat, kinderen, telefoon en e-mail)
- identificatiegegevens (zoals BSN, identiteitskaartnummer, paspoort, rijbewijsnummer en/of pensioennummer)
- financiële gegevens (zoals bankrekeningnummer, salarisgegevens, dienstverbanden en alle andere pensioengevende componenten)
- pensioengegevens (zoals hoogte pensioenaanspraken of pensioenrechten)
- registratie op portal en website (digitale post en interactiegegevens)

Bijzondere gegevens

In principe verwerkt het pensioenfonds geen bijzondere categorieën van persoonsgegevens, behalve informatie over iemands gezondheid c.q. een arbeidsongeschiktheidspercentage in geval van premievrijstelling, waarvoor een grondslag zoals vermeld in de AVG en/of Uitvoeringswet Algemene Verordening Gegevensbescherming is benodigd om deze gegevens te mogen verwerken.

2.5 Wijze van verwerking

Het pensioenfonds streeft naar een minimale gegevensverwerking. Het beginsel van dataminimalisatie betekent dat verwerking moet worden beperkt tot wat noodzakelijk is om de vastgestelde doeleinden te bereiken. Wanneer het pensioenfonds met geen, of minder (belastende), persoonsgegevens hetzelfde doel bereikt, wordt daar altijd voor gekozen. Hiermee hangt samen dat persoonsgegevens ook zo snel mogelijk worden geaggregeerd (als daarmee ook het doel kan worden gerealiseerd), geanonimiseerd of gewist.
Het pensioenfonds zorgt er actief voor dat de verwerkte gegevens juist en actueel zijn en neemt daar alle redelijke maatregelen voor.
Het pensioenfonds bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van zijn taken en neemt daarbij ook de wettelijke verplichting uit hoofde van bijvoorbeeld het Burgerlijk Wetboek, de Pensioenwet, of fiscale wetgeving in acht. Het uitgangspunt voor de gehanteerde bewaartermijnen is het Servicedocument Bewaartermijnen van de Pensioenfederatie.

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

3. Transparantie & Communicatie

Het pensioenfonds informeert betrokkenen over het verwerken van hun persoonsgegevens. Het pensioenfonds informeert de deelnemers duidelijk over dat en hoe hun persoonsgegevens verzameld, gebruikt, geraadpleegd of op een andere manier worden verwerkt, waarom en door wie. Het pensioenfonds zal dit doen in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm. Onderwerpen waarover naar betrokkene wordt gecommuniceerd zijn de navolgende:

- Contactgegevens met betrekking tot het pensioenfonds en hoe betrokkenen contact kunnen opnemen met het pensioenfonds en de privacy officer.
- Waarom persoonsgegevens worden verzameld en waarom dat mag (doel en rechtsgrond van de verwerking van de persoonsgegevens).
- Wat de gerechtvaardigde belangen zijn van het pensioenfonds voor de gegevensverwerking, indien dat de rechtsgrond van de verwerking is.
- Aan wie de persoonsgegevens verder nog worden verstrekt (ontvangers of categorieën van ontvangers).
- Zijn betrokkenen verplicht om de gevraagde persoonsgegevens te verstrekken of niet? En wat zijn de gevolgen als een betrokkene de persoonsgegevens niet verstrekt (noodzaak)?
- Waar en hoe kan de betrokkene vragen om inzage, rectificatie, wissen of overdracht van persoonsgegevens, klachten indienen, bezwaar maken of een verwerking beperken?
- Hoe kan een betrokkene een verleende toestemming intrekken?
- Hoe lang verwacht het pensioenfonds de persoonsgegevens te gaan bewaren?
- Als persoonsgegevens buiten de EU verwerkt gaan worden, welke waarborgen zijn er getroffen dat de persoonsgegevens in dat derde land conform de AVG worden verwerkt en passend beveiligd zijn?
- Doet het pensioenfonds aan geautomatiseerde besluitvorming (computergestuurde verwerking van persoonsgegevens zonder menselijke tussenkomst, bijvoorbeeld profilering)? En zo ja, welke logica wordt daarvoor gebruikt?
- Maakt het pensioenfonds gebruik van zogenoemde cookies, welke persoonsgegevens worden dan verzameld, waarom en op welke wijze?

Wanneer betrokkenen gegevens aan het pensioenfonds aanleveren, dan worden zij van voorgenoemde informatie op de hoogte gesteld. Dit kan bijvoorbeeld via standaardformulieren of de zogenaamde Pensioen 1-2-3 communicatie.
Informatie die gedurende de looptijd aan de betrokkene wordt verstrekt kan ook via een internetportal van het pensioenfonds geschieden. Van belang is ook dat betrokkenen daarbij verwezen worden naar de website van het landelijk pensioenregister: www.mijnpensioenoverzicht.nl.

De betrokkene wordt niet nogmaals geïnformeerd als deze al weet dat het pensioenfonds persoonsgegevens van hem / haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.

Privacyverklaring
Het pensioenfonds beschikt over een privacverklaring. Ook deze verklaring dient aan de bovenvermelde eisen te voldoen en wordt gepubliceerd op de website van het pensioenfonds.

Samenvatting beleid
Tenslotte deelt het pensioenfonds een persoonsgerichte en duidelijke samenvatting van onderhavig beleid op haar website. Dit om een lage informatiedrempel te creëren ten aanzien van de omgang met persoonsgegevens.

4. Rechten van betrokkenen

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

De AVG kent betrokkenen de navolgende rechten toe:
- **Inzage:** Betrokkenen hebben het recht om aan het pensioenfonds te vragen of zijn / haar persoonsgegevens worden verwerkt. Als zijn persoonsgegevens worden verwerkt dan heeft hij recht om te weten welke gegevens dat zijn en heeft hij het recht deze persoonsgegevens op te vragen.
- **Rectificatie**: Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij het pensioenfonds om deze te wijzigen of aan te vullen. Als de betrokkene terecht een beroep doet op dit recht dan moet het pensioenfonds volgens de AVG iedere ontvanger van de gegevens, zoals bijvoorbeeld de belastingdienst, UWV en subverwerkers, hiervan op de hoogte stellen.
- **Wissen (recht op vergetelheid)**: De betrokkene heeft het recht om de gegevens te laten wissen indien bijvoorbeeld de persoonsgegevens niet meer nodig zijn voor het doeleinde van verwerking of als terecht bezwaar aangetekend is tegen de verwerking. Voorts in geval van onrechtmatige verwerking. Overigens is dit geen absoluut recht en bestaat hierop bijvoorbeeld geen recht indien het pensioenfonds voldoet aan een wettelijke verplichting en bijvoorbeeld in geval van een onderbouwing van een rechtsvordering. Het wissen moet kosteloos geschieden en zo spoedig mogelijk, in ieder geval binnen een maand. Ook het wissen van gegevens moet het pensioenfonds doorgeven aan de ontvangers.

- **Beperking**: De betrokkene heeft het recht de verwerking te beperken in vier situaties:
  - als de juistheid van de gegevens wordt betwist en het pensioenfonds moet dat controleren;
  - als de verwerking onrechtmatig is en de betrokkene zich verzet tegen wissen, maar een beperking wenst;
  - als het pensioenfonds de gegevens niet meer nodig heeft, maar de betrokkene wel, bijvoorbeeld voor het voeren van een rechtszaak tegen het pensioenfonds of derden;

  - als de betrokkene bezwaar heeft gemaakt tegen een verwerking waarop het pensioenfonds niet meteen beslist, dan kan de betrokkene een beperking verlangen.

  Overigens ook dit is geen absoluut recht en verwerking kan toch plaatsvinden bijvoorbeeld in geval van louter opslag, instellen rechtsvordering en ter bescherming van rechten van anderen.
- **Bezwaar:** Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn / haar persoonsgegevens. Het pensioenfonds zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.
- **Dataportabiliteit**: De betrokkene heeft het recht op overdraagbaarheid van gegevens, hetgeen inhoudt dat de betrokkene het recht heeft om zijn persoonsgegevens in een gestructureerde, gangbare en machine leesbare vorm te ontvangen en deze ongehinderd aan een andere verantwoordelijke over te dragen. Het doel van dit nieuwe recht is om betrokkenen meer controle over hun gegevens te geven en het voor hen gemakkelijker te maken van dienstverlener te wisselen. Het recht op dataportabiliteit is alleen van toepassing op verwerkingen die op basis van geautomatiseerde procedés worden verricht. Bovendien moet het gaan om persoonsgegevens die met toestemming van de betrokkene of op basis van een overeenkomst met de betrokkene worden verwerkt.
- **Indienen van verzoek:** Om gebruik te maken van zijn / haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de e-mail ingediend worden. Het pensioenfonds heeft in beginsel vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Indien dat niet lukt, dan moet in ieder geval binnen een maand worden gemeld waarom het niet lukt en kan de termijn met maximaal twee maanden worden verlengd. Als het verzoek niet wordt opgevolgd, dan wordt dit binnen een maand meegedeeld met de reden van weigering en informatie over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens en beroep in te stellen bij de rechter. Er zal moeten worden vastgesteld dat de betrokkene zelf het recht inroept, oftewel identificatie. Het inroepen van alle rechten is in beginsel kosteloos, echter indien het verzoek kennelijk ongegrond of buitensporig is mag het pensioenfonds hetzij redelijke kosten vragen voor het inwilligen van het verzoek of het verzoek weigeren.

5. Verplichtingen verantwoordelijke

5.1 Register van verwerkingen

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

- De naam en contactgegevens van de verantwoordelijke en, mogelijk, de gezamenlijke verantwoordelijke.
- De doelen van de verwerking.
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen.
- Een beschrijving van de ontvangers van de persoonsgegevens.
- Een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie.

- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist.
- Een algemene beschrijving van de beveiligingsmaatregelen.

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

5.2 Privacy Impact Analyse (PIA)

Met een PIA (ook wel gegevensbeschermingseffectbeoordeling genoemd), worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Het pensioenfonds laat een PIA uitvoeren indien een gegevensverwerking een hoog privacyrisico oplevert voor betrokkenen. Volgens de AVG is hiervan sprake indien het pensioenfonds:

- Systematisch en uitvoerig persoonlijke aspecten evalueert (gebaseerd op geautomatiseerde verwerking), waaronder profilering en waarop besluiten worden gebaseerd waaraan rechtsgevolgen voor betrokkenen zijn verbonden.
- Op grote schaal bijzondere persoonsgegevens of strafrechtelijke gegevens verwerkt.
- Op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Voorts heeft de AP een lijst met soorten verwerkingen opgesteld waarvoor het uitvoeren van een PIA is verplicht vóórdat met het verwerken van persoonsgegevens wordt begonnen. Deze lijst is niet uitputtend en het pensioenfonds moet zelf beoordelen of de verwerking een hoog privacyrisico oplevert voor betrokkenen. Nu is de situatie dat het pensioenfonds nagenoeg alle processen waarbij persoonsgegevens worden verwerkt, heeft uitbesteed. De belangrijkste verwerker is AZL en deze uitvoerder voert standaard een PIA uit bij een gewijzigd of nieuw proces met een verwacht hoog risico voor de betrokkenen. Het pensioenfonds neemt, desgewenst, kennis van de ingevulde PIA's. Op deze wijze houdt het pensioenfonds zicht op processen met een hoog privacyrisico voor betrokkenen en krijgt het inzicht welke maatregelen er worden genomen om geconstateerde privacyrisico's te mitigeren.

5.3 Geautomatiseerde verwerkingen

Betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerkinggebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.
Het pensioenfonds maakt vooralsnog geen gebruik van geautomatiseerde beslissingen. Indien daarvan sprake zal zijn, dan zullen daar specifieke eisen aan worden gesteld.

5.4 Privacy by design & default

Het privacy by design- en defaultbeginsel houdt in dat de bij de verwerking gehanteerde mechanismen en systemen zo zijn ontworpen dat zoveel als mogelijk rekening wordt gehouden met de privacy van betrokkenen. Ook hiervoor geldt dat de belangrijke processen waarbij persoonsgegevens worden verwerkt, plaatsvinden bij de uitvoerder AZL. Bij projecten / programma's van AZL wordt door middel van onder meer de PIA, afgedwongen om rekening te houden met mogelijke risico's op het gebied van privacy en security.

5.5 Datalekken

Bij een datalek gaat het om in handen komen van persoonsgegevens bij ongeautoriseerde personen, als gevolg van een inbreuk op de beveiliging. Bij een datalek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking, hetgeen dus niet de bedoeling is van het pensioenfonds. Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop, een inbraak in een databestand door een hacker of post met een verkeerde adressering of open envelop versturen. De verantwoordelijke, dus het pensioenfonds, moet een geconstateerd datalek meteen doch in ieder geval binnen 72 uur melden aan de Autoriteit Persoonsgegevens. Als dat niet tijdig lukt, dan moet het pensioenfonds hiervoor een verklaring kunnen geven.

Als er wel een hoog risico is en het pensioenfonds geen maatregelen meer kan nemen om het risico te mitigeren, dan moeten naast de Autoriteit Persoonsgegevens ook de deelnemers zelf worden geïnformeerd, zodat die eventueel voorzorgsmaatregelen kunnen treffen. De Autoriteit Persoonsgegevens kan het pensioenfonds ook verplichten tot melding aan de deelnemers.
Zie voor de uitwerking van de melding de procedure meldingsplicht datalekken van het pensioenfonds.

6. Verwerkers

6.1 Uitbesteding aan een verwerker

Het pensioenfonds besteedt een groot deel van het verwerken van persoonsgegevens uit aan verwerkers. Deze verwerkers hebben een uitvoerende taak en geen zeggenschap over de wijze van verwerken uit hoofde van het privacybeleid. Essentieel is dat de gegevens alleen in opdracht van het pensioenfonds mogen worden verwerkt en niet voor eigen doeleinden door de verwerker. Het gaat om uitbestede / gedelegeerde verwerkingsactiviteiten, die een verantwoordelijke ook zelf had kunnen verrichten.
Indien het pensioenfonds persoonsgegevens laat verwerken door een verwerker, wordt de uitvoering van de verwerkingen geregeld in een schriftelijke overeenkomst tussen het pensioenfonds als de verantwoordelijke en de verwerker. Daarin worden in ieder geval de in 6.2 genoemde eisen opgenomen.

6.2 Eisen verwerkersovereenkomst

Algemene beschrijving

Een omschrijving van het onderwerp, de duur, de aard en het doel van de verwerking, het soort persoonsgegevens, de categorieën van betrokkenen en de rechten en verplichtingen als verwerkingsverantwoordelijke, dit kan het best in een bijlage worden vastgelegd.

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

Beveiliging
De verwerker garandeert passende technische en organisatorische maatregelen om de verwerking te beveiligen. Daarbij gelden de navolgende eisen:
- de verwerker werkt conform de maatregelen genoemd in de meest recente ISO 27001-norm of soortgelijke standaarden;
- het vermogen om op permanente basis de vertrouwelijkheid, de integriteit, de beschikbaarheid en de veerkracht van de verwerkingssystemen en diensten te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid en de toegang tot de persoonsgegevens tijdig te herstellen;
- een procedure voor het jaarlijks testen, beoordelen en evalueren van de doeltreffendheid van de technische maatregelen ter beveiliging van de verwerking en bij geconstateerde manco's zal de verwerker zo spoedig mogelijk voor eigen rekening aanvullende beveiligingsmaatregelen treffen;
- logische toegangscontrole, gebruik makend van wachtwoorden;
- fysieke maatregelen voor toegangsbeveiliging;
- automatische logging van alle handelingen rond de persoonsgegevens;
- pseudonimisering en encryptie (versleuteling) van digitale bestanden met persoonsgegevens;
- organisatorische maatregelen voor toegangsbeveiliging;
- beveiliging van netwerkverbindingen via Secure Socket Layer (SSL) technologie;
- doelgebonden toegangsbeperkingen;
- controle op toegekende bevoegdheden;
- maatregelen ter preventie van top 10 bedreigingen zoals geformuleerd door OWASP;
- een procedure met betrekking tot melden van datalekken.

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

Subverwerkers
De verwerker schakelt geen subverwerker(s) in zonder voorafgaande schriftelijke toestemming van het pensioenfonds. De verwerker legt aan een subverwerker in een verwerkersovereenkomst dezelfde verplichtingen op als het pensioenfonds aan de verwerker.

Andere verplichtingen
De verwerker faciliteert het pensioenfonds om te voldoen aan zijn plichten zoals privacyrechten van aanspraak- en pensioengerechtigden en ook om de overige verplichtingen na te komen, zoals het melden van datalekken, het uitvoeren van een privacy impact assessment (PIA) en het voorafgaand raadplegen van de Autoriteit Persoonsgegevens in geval van een hoog risicovolle PIA. De verwerker hanteert ook ISAE 3402 als raamwerk om in control te zijn aantoonbaar te maken. Voorts draagt de verwerker zorg voor voldoende kwaliteit van de persoonsgegevens.

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

Het pensioenfonds zorgt ervoor dat de verwerkersovereenkomsten minimaal voldoen met betrekking tot bovengenoemde aspecten en ziet ook toe op de naleving daarvan. Daartoe wordt een monitoringsproces ingericht en jaarlijks wordt daarover gerapporteerd.

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

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

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

7. Non-Compliance & Klachten

7.1 Non-Compliance
De AP heeft tot taak de naleving van de verplichtingen ingevolge de AVG te monitoren en te handhaven. De AP beschikt daartoe over verschillende bevoegdheden, zoals het doen van onderzoeken, het verkrijgen van toegang tot alle bedrijfsruimten en middelen van gegevens-verwerkingen. In geval van een onderzoek door de AP zal het pensioenfonds daaraan zijn medewerking verlenen. Voorts heeft de AP de bevoegdheid tot het opleggen van corrigerende maatregelen, oplopend van een waarschuwing, last om betrokkenen te

informeren, tot een verwerking te beperken, tijdelijk dan wel definitief. Tenslotte afhankelijk van de aard, ernst en duur van de overtreding, kan de AP forse boetes opleggen oplopend tot 20 miljoen euro. Het is derhalve van belang dat het pensioenfonds, betrokken gremia, de uitvoerders en alle anderen de AVG naleven. Voorts bij vragen over de toepassing van de AVG direct contact opnemen met de privacy officer van het pensioenfonds.

7.2 Klachten & Schadevergoeding

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

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

7.3 Vragen

Bij vragen over de toepassing van de AVG, andere privacyregelgeving of dit beleid, neem dan contact op met de privacy officer van het pensioenfonds.

8. Riscobeheersing

In het kader van het three-lines-of-defencemodel voor het beheersen van privacyrisico‘s is het bestuur binnen de eerste lijn verantwoordelijk voor het voldoen aan het privacybeleid. Daarbij zijn door de eerste lijn een aantal belangrijke kaders vastgesteld om te beoordelen of het pensioenfonds dan wel een partij, waaraan de belangrijkste processen zijn uitbesteed, voldoet aan een beheerste IT-beheeromgeving en informatiebeveiliging, waardoor ook privacyrisico’s worden gemitigeerd. Zo maakt het pensioenfonds gebruik van de Good Practice Informatiebeveiliging 2019/2020, DNB Cloud computing Assessment en de Cobit-controls. Voorts wordt jaarlijks het rapport van AZL bestudeerd met betrekking tot de naleving van de AVG op de uitbestede verwerkingen aan AZL. Daarnaast vindt om de twee jaar een privacy check bij de overige uitbestede partijen plaats, alwaar op veel bescheidener schaal verwerking van gegevens plaatsvindt.
De tweede lijn wordt gevormd door de privacy officer en de risicomanagementfunctie. Deze hebben als taak te adviseren omtrent de privacyrisico’s dan wel de IT-security risico’s en rapportages te beoordelen dan wel na te gaan of aan de privacywet- en regelgeving wordt voldaan.
De derde lijn wordt gevormd door de auditfunctie die zorgt voor een periodieke toetsing naar de opzet, het bestaan en de werking van de interne beheersmaatregelen op het gebied van privacy.

9. Inwerkingtreding

Dit privacy beleid is van kracht per 16 juli 2020 en wordt periodiek door het pensioenfonds geëvalueerd. Laatste update september 2022.