BedrijfstakPensioenfonds
voor de Zuivel

Privacybeleid

Stichting Bedrijfstakpensioenfonds voor de Zuivel en aanverwante industrie

Definitieve versie

12 juni 2018

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

Uit naam van Stichting Bedrijfstakpensioenfonds voor de Zuivel en aanverwante industrie (BPZ) worden dagelijks persoonsgegevens verwerkt. Om de privacy van de betrokken personen te beschermen vinden wij het van groot belang dat de verwerking van persoonsgegevens zorgvuldig gebeurt en dat wordt voldaan aan de wet- en regelgeving die wij op het gebied van de bescherming van persoonsgegevens in Nederland kennen. BPZ wil compliant zijn met deze wet- en regelgeving.

1.2 Doel van dit document

Dit Privacybeleid geldt vanaf 25 mei 2018. BPZ is de verwerkingsverantwoordelijke in de zin van de AVG. Dit houdt in dat BPZ de zeggenschap heeft over de data en het doel en de middelen voor de gegevensverwerkingen vaststelt. Dit Privacybeleid geeft de kaders aan die BPZ stelt en die compliant zijn met wet- en regelgeving. Die wet- en regelgeving betreft:

- De Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming of 'AVG'). De AVG is van kracht per 25 mei 2018;
- Naast de AVG is in Nederland ook de Uitvoeringswet AVG van belang.

1.3 Opbouw van dit document

Dit Privacybeleid is verdeeld in een aantal onderdelen. In hoofdstuk 2 worden de begrippen, reikwijdte en uitgangspunten beschreven en is de privacy cyclus binnen BPZ beschreven. In hoofdstuk 3 zijn de daadwerkelijke beleidsonderwerpen beschreven.

2. Begrippen, uitgangspunten, privacycyclus

2.1 Inleiding

In dit hoofdstuk wordt nadere uitleg gegeven over een aantal begrippen die in dit Privacybeleid voorkomen en worden de uitgangspunten beschreven die betrekking hebben op het beleid omtrent de bescherming van persoonsgegevens binnen BPZ. Tevens wordt de Privacycyclus beschreven die door BPZ wordt doorlopen.

2.2 Begrippen

De algemene omschrijving van de begrippen sluit aan bij de definities in de AVG (Artikel 4). In bijlage 1 zijn deze nader omschreven.

2.3 Uitgangspunten

Verwerkingsverantwoordelijke: BPZ

BPZ is verantwoordelijk voor de verwerkingen van persoonsgegevens in de zin van de AVG. Indien BPZ verwerkingen uitbesteed aan een derde partij (verwerker) worden deze opgenomen in het verwerkingsregister van BPZ en wordt een verwerkersovereenkomst opgesteld tussen BPZ en de derde partij. Zie verder paragraaf 3.3.

Informatieverplichting

Op basis van de informatieverplichting zal richting een betrokkene duidelijk gecommuniceerd moeten worden over de wijze waarop persoonsgegevens worden verwerkt. De verwerkingsverantwoordelijke dient onder andere haar identiteit kenbaar te maken. Zie verder paragraaf 3.5.

Informatiebeveiliging

Op de persoonsgegevens die onder verantwoordelijkheid van BPZ worden verwerkt is in het kader van de beveiliging het BPZ Informatiebeveiligingsbeleid van toepassing en zijn afspraken gemaakt met de derde partijen (verwerkers). Zie verder paragraaf 3.7.

Functionaris voor gegevensbescherming

BPZ moet rondom de verwerking van persoonsgegevens een beheerste en integere bedrijfsvoering organiseren. Onder de AVG is het voor BPZ niet verplicht een Functionaris voor gegevensbescherming (FG) aan te stellen. BPZ kiest er echter wel voor om een FG aan te stellen. De FG ondersteunt BPZ bij het opereren binnen de wettelijke kaders en zorgt er voor dat privacy-aangelegenheden uniform en gecoördineerd worden opgepakt, ook naar derde partijen (verwerkers).

De FG heeft vanuit het bestuur de verantwoordelijkheid om het Privacybeleid actueel te houden, te coördineren en te monitoren. In bijlage 2 is een nadere toelichting aangegeven over de rol van de FG binnen het fonds.

2.4 Privacycyclus

Verantwoordelijkheden & Privacy organisatie

BPZ is verantwoordelijk voor het in control zijn met betrekking tot privacy. De kaders en uitgangspunten zijn hierbij beschreven in dit beleid.

Door BPZ worden in het kader van de dienstverlening en het risicomanagement rapportages gevraagd aan uitbestedingspartners. Voor derde partijen (verwerkers) (zie paragraaf 3.3) worden aanvullende eisen gesteld die volgen uit dit beleid.

Voor deze rapportages geldt dat de totstandkoming van deze rapportages een integraal onderdeel uitmaakt van het risicomanagement proces van BPZ. Aan de uitbestedingspartners (waaronder verwerkers) worden normen gesteld ten aanzien van de rapportages, die aan BPZ worden verstrekt, en de periodiciteit hiervan. Het bestuur van BPZ beoordeelt de kwaliteit van deze rapportages en bespreekt deze met derde partijen (verwerkers).

3. Beleidsonderwerpen

3.1 Inleiding

In dit Privacybeleid hebben wij onderstaande beleidsonderwerpen opgenomen en uitgewerkt. Een aantal onderwerpen zijn in de bijlagen 3 – 10 nader toegelicht en uitgewerkt.

Paragraaf	Beleidsonderwerp
3.2	**(Bijzondere) Persoonsgegevens en BSN** • Persoonsgegevens • Bijzondere Persoonsgegevens • Burger Service Nummers (BSN) Bijlage 3 Nadere toelichting (Bijzondere) persoonsgegevens
3.3	**Verwerkingsverantwoordelijke, verwerker en verwerkersovereenkomst** • Derde partijen Bijlage 4 Nadere toelichting Verwerkingsverantwoordelijke, verwerker en verwerkersovereenkomst
3.4	**Verwerkingsregister** • Administratie en proces Bijlage 5 Nadere toelichting Verwerkingsregister
3.5	**Beginselen voor verwerking** • Rechtmatige grondslag, behoorlijkheid en transparantie • Doelbinding • Minimale gegevensverwerking • Juistheid • Opslagbeperking • Integriteit en vertrouwelijkheid Bijlage 6 Nadere toelichting Beginselen voor verwerking Bijlage 7 Nadere toelichting Privacyverklaring
3.6	**Rechten betrokkenen** • Identificatie als voorwaarde • Recht op inzage • Recht op correctie/rectificatie • Recht op gegevenswissing/vergetelheid • Recht op beperking van de verwerking • Recht op overdraagbaarheid van gegevens (dataportabiliteit) • Recht van bezwaar • Profilering en geautomatiseerde besluitvorming Bijlage 8 Nadere toelichting Rechten betrokkenen
3.7	**Technische en organisatorische maatregelen (waaronder beveiliging)** • Technische en organisatorische maatregelen • Beveiliging: passend beschermingsniveau • Privacy by design and by default • Anonimiseren, Pseudonimiseren en Hashing • Verwerkers en passende maatregelen Bijlage 9 Beleidsregels Beveiliging Persoonsgegevens
3.8	**Datalekken**
3.9	**Privacy Impact Assessment (PIA)** Bijlage 10 Nadere toelichting Privacy Impact Assessment (PIA)

3.2 (Bijzondere) Persoonsgegevens en BSN

BPZ verwerkt gegevens in overeenstemming met wet- en regelgeving. Hieronder is een nadere toelichting gegeven.

Persoonsgegevens

Bijlage 3 geeft nadere toelichting aan het begrip persoonsgegeven inclusief de elementen:

1. Alle informatie over een persoon;
2. Geïdentificeerde of identificeerbare;
3. Natuurlijk persoon.

Voor BPZ gaat het hierbij met name om:
- aanspraak- en pensioengerechtigden;
- (ex)leden van fondsgremia.

Gegevens van overleden personen zijn geen persoonsgegevens in de zin van de AVG. BPZ gaat uiteraard wel zorgvuldig met deze gegevens om.

Bijzondere Persoonsgegevens

De aard van sommige gegevens brengt mee dat de verwerking ervan een grotere inbreuk kan maken op de persoonlijke levenssfeer van de betrokkene omdat die gegevens gevoelige informatie over iemand verschaffen. In de AVG worden deze gegevens 'bijzondere persoonsgegevens' genoemd. Voor de verwerking van deze bijzondere gegevens geldt een verbod, tenzij er een wettelijke uitzondering van toepassing is. Die uitzondering kan in de AVG staan of in een wet van de lidstaten. BPZ hanteert het uitgangspunt dat het geen Bijzondere Persoonsgegevens verwerkt, tenzij noodzakelijk voor de uitvoering. Bijlage 3 geeft nadere toelichting op het begrip Bijzondere Persoonsgegevens.

Burger Service Nummer (BSN)

Het nationaal identificatienummer is een apart persoonsgegeven dat benoemd wordt in de AVG. De AVG ziet een nationaal identificatienummer in beginsel als een ''gewoon'' persoonsgegeven. Lidstaten kunnen echter specifieke voorwaarden stellen voor een nationaal identificatienummer of enige andere identificator van algemene aard (art 87 AVG).

Nederland houdt vast aan de lijn die ook onder de Wbp gold. Dat betekent dat voor gebruik van het BSN er een expliciete wettelijke grondslag moet zijn die verwerking toestaat.

De hoofdregel is dus: gebruik van het BSN is verboden, tenzij het expliciet bij wet is toegestaan. Ook al geeft iemand een bedrijf bijvoorbeeld toestemming, dan nog is het verwerken van het BSN niet toegestaan als er geen wettelijke grondslag voor is.

Gebruik van het BSN is toegestaan in de gevallen genoemd in het 'Besluit gebruik burgerservice-nummer Wbp'. Hierin is o.a. bepaald dat een Pensioenfonds voor zover hij is belast met de uitvoering van pensioenregelingen overeenkomstig de Pensioenwet, het BSN mag gebruiken voor zover dat noodzakelijk is voor de uitvoering van zijn taken of voor een juiste uitvoering van wettelijke voorschriften. Ook in de Pensioenwet (art. 94 PW) is een grondslag opgenomen.

De overige regels van de AVG blijven gewoon van toepassing. Tenzij de wet gebruik van BSN verplicht stelt, is het dus nog steeds de vraag of gebruik van BSN ook noodzakelijk is gezien het doel, ook al staat in de wet dat BSN gebruikt mag worden. Als op andere wijze of met een minder gevoelig gegeven hetzelfde doel gediend kan worden, zal daar in beginsel voor gekozen worden.

3.3 Verwerkingsverantwoordelijke, verwerker en verwerkersovereenkomst

De verwerkingsverantwoordelijke (BPZ) is de entiteit die het doel van en de middelen voor de verwerking van persoonsgegevens bepaalt. De verwerker (artikelen 4 en 28 AVG) is de partij die ten behoeve van de verwerkingsverantwoordelijke (BPZ) persoonsgegevens verwerkt.

Derde partijen

BPZ heeft werkzaamheden uitbesteed aan derde partijen. Hieronder is aangegeven welke derde partijen BPZ ziet als verwerker en waarbij een verwerkersovereenkomst is opgesteld.

	Derde partijen (verwerker)
1	Achmea Pensioenservices

De vermogensbeheerder en custodian zijn door BPZ niet aangeduid als verwerker, aangezien zij van BPZ geen Persoonsgegevens zullen ontvangen. Ook de adviserend actuaris beschikt niet over Persoonsgegevens van het fonds en is daarmee geen verwerker. De accountant en waarmerkend (certificerend) actuaris hebben een wettelijke taak en zijn daarmee ook niet aan te merken als verwerker. De herverzekeraar voor de arbeidsongeschiktheids- en overlijdensrisico's geldt als verwerkingsverantwoordelijke.

Het is verplicht met een verwerker een overeenkomst te sluiten. BPZ mag alleen zaken doen met betrouwbare verwerkers die voldoende garanties bieden (art 28 lid 1 AVG). Om die reden dient er een overeenkomst gesloten te worden met de verwerker die bindende aanspraken geeft aan BPZ en waarvan BPZ zich kan vergewissen dat de beveiliging van de verwerker op orde is door hieraan eisen te stellen (zoals, certificering door een derde). Dat leggen wij vervolgens ook vast in de overeenkomst.

Een nadere toelichting over het begrip "verwerkingsverantwoordelijke", "verwerker" en de "verwerkersovereenkomst" hebben wij in bijlage 4 opgenomen.

3.4 Verwerkingsregister

Conform Artikel 30 lid 1 AVG dient BPZ als verwerkingsverantwoordelijke een register bij te houden met verwerkingsactiviteiten. Conform Artikel 30 lid 2 AVG dient de verwerker een register bij te houden van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht. Dit mag schriftelijk en/of elektronisch. Het verwerkingsregister kan opgevraagd worden door de Autoriteit Persoonsgegevens (AP).

Het verwerkingsregister dient actueel te zijn. Aangezien BPZ een deel van de bewerkingen heeft uitbesteed aan derden stelt het eisen aan derde partijen (verwerkers). In bijlage 5 zijn deze aspecten nader uiteengezet en is een nadere beschrijving gegeven van de eisen die BPZ stelt aan het verwerkingsregister en hoe deze wordt ingevuld.

Administratie en proces

Het opstellen en onderhoud van het verwerkingsregister voor BPZ als verwerkingsverantwoordelijke is namens het bestuur belegd bij Achmea Pensioenservices. Om te beoordelen of de administratie actueel en volledig is, wordt het verwerkingsregister jaarlijks vervaardigd (afgestemd met de verwerkingsregisters van eventuele andere verwerkers) en voorgelegd aan het bestuur van BPZ met het verzoek de inhoud te accorderen.

3.5 Beginselen voor verwerking

De artikelen 5 en 6 van de AVG bevatten diverse algemene beginselen voor de verwerking van persoonsgegevens, dat wil zeggen het verzamelen en vervolgens verwerken, archiveren en vernietigen van persoonsgegevens. Voor BPZ vormen dit uitgangspunten voor dit beleid.

Rechtmatige grondslag, behoorlijkheid en transparantie

De AVG schrijft voor dat persoonsgegevens moeten worden verwerkt op een wijze die rechtmatig, behoorlijk en transparant is. Voor aanspraak- en pensioengerechtigden moet inzichtelijk zijn waarom en op welke manier persoonsgegevens worden verwerkt. BPZ moet hier helder en toegankelijk over communiceren in een zogenoemde privacyverklaring.

Rechtmatige grondslag

De verwerking van persoonsgegevens moet gebaseerd zijn op een van de zes in de AVG limitatief genoemde grondslagen (art. 6 AVG). Zie verder bijlage 6 Nadere toelichting Beginselen voor verwerking: Rechtmatige grondslag. Voor BPZ is een rechtmatige grondslag aanwezig door het uitvoeren van de pensioenovereenkomst (grondslag b). De vastlegging of sprake is van rechtmatige verwerking BPZ vindt plaats in het verwerkingsregister.

Behoorlijkheid en transparantie

Om behoorlijke en transparante verwerking te waarborgen dient BPZ de volgende aspecten vast te stellen:

a) Bewaartermijngegevens (of criteria om bewaartermijnen te bepalen);
b) Dat de betrokkene recht heeft op inzage, correctie, vergeten te worden, beperking (‘bevriezing’), bezwaar en gegevens overdraagbaarheid, zie hiervoor de volgende paragraaf;
c) Het recht om een klacht in te dienen bij de toezichthouder;
d) of sprake is van geautomatiseerde besluitvorming (waaronder profilering) en zo ja, wat de onderliggende logica is en welke gevolgen er zijn voor de betrokkene.

Informatieplicht en Privacyverklaring

Transparantie is een van de belangrijkste verplichtingen als persoonsgegevens verwerkt worden. Om de betrokkene in staat te stellen zijn rechten te verwezenlijken, moet hij van de verwerking van hem betreffende gegevens op de hoogte zijn. Het niet voldoen aan de informatieplicht leidt, tenzij er een wettelijke uitzondering is, tot een onrechtmatige verwerking van persoonsgegevens. Transparant zijn wat BPZ doet met gegevens en de verplichte informatie verstrekken aan betrokkenen staat daarom voorop.

Dit betekent niet dat BPZ moet zorgen dat een betrokkene de informatie ook daadwerkelijk leest, maar wel dat die mogelijkheid expliciet wordt geboden. BPZ heeft dit opgenomen in de Privacyverklaring.

Deze verklaring moet in duidelijke en eenvoudige taal worden opgesteld en mag dus niet lezen als een juridische disclaimer. BPZ heeft een privacyverklaring op haar website staan die voldoet aan de criteria van de AVG. De vereiste inhoud van de privacyverklaring is nader toegelicht in bijlage 7.

Doelbinding

Gegevensverwerking mag alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden gebeuren. BPZ heeft die doeleinden concreet vastgesteld, omschreven en vastgelegd in het verwerkingsregister. Verdere verwerking van persoonsgegevens, voor een ander doel dan waarvoor ze oorspronkelijk werden verzameld, moet separaat gerechtvaardigd kunnen worden als de verdere verwerking niet berust op toestemming of een wettelijke verplichting. In bijlage 6 hebben is een toelichting gegeven over doelbinding.

Minimale gegevensverwerking

BPZ streeft minimale gegevensverwerking na. Dataminimalisatie betekent dat verwerking moet worden beperkt tot wat noodzakelijk is om de vastgestelde doeleinden te bereiken. Hiermee hangt samen dat persoonsgegevens ook zo snel mogelijk moeten worden geaggregeerd (als daarmee ook het doel kan worden gerealiseerd), geanonimiseerd en gewist. De opslagperiode van de persoonsgegevens moet tot een strikt minimum worden beperkt en er dienen termijnen te zijn voor het wissen of periodiek toetsen van de persoonsgegevens. BPZ bespreek deze termijnen met de derde partijen (verwerkers).

Juistheid

BPZ zorgt er actief voor dat dat de verwerkte gegevens juist en actueel zijn en stelt hierbij eisen aan de uitbestedingspartners die vervolgens worden gemonitord.

Opslagbeperking

Het beginsel van opslagbeperking betekent dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het bereiken van de gestelde doeleinden. BPZ bewaart gegevens conform wet- en regelgeving en aanwijzingen DNB. Met de derde partijen (verwerkers) zijn hierover afspraken gemaakt.

Integriteit en vertrouwelijkheid

Het beginsel van integriteit en vertrouwelijkheid brengt met zich mee dat BPZ ervoor zorgt dat door middel van passende technische en organisatorische beveiligingsmaatregelen ongeoorloofde toegang tot c.q. ongeoorloofd gebruik van persoonsgegevens wordt voorkomen. BPZ is verantwoordelijk voor de naleving van deze beginselen en moet dat ook kunnen aantonen (de zogenoemde verantwoordingsplicht). Dit betekent dat BPZ eisen stelt aan de derde partijen (verwerkers) en dit periodiek monitort door en namens het bestuur.

3.6 Rechten betrokkenen

Een belangrijke voorwaarde voor het verwerken van Persoonsgegevens is dat de verwerking rechtmatig, behoorlijk en transparant is. Om daarvoor te zorgen moeten de betrokkenen op een heldere en volledige wijze worden geïnformeerd over het verwerken van hun persoonsgegevens. Dit betekent ook dat zij goede en volledige informatie krijgen over hun rechten en hoe zij die kunnen uitoefenen.

Identificatie

BPZ moet zeker weten wie een recht uitoefent. Daarom gelden de volgende voorwaarden:

1. De verantwoordelijke moet kunnen vaststellen dat de betrokkene de persoon is op wie de persoonsgegevens betrekking hebben. Het vaststellen van de identiteit van de verzoeker is noodzakelijk om te voorkomen dat iemand door het gebruik van de naam van een ander diens gegevens kan inzien (artikelen 11, lid 2, 12, leden 1, 2, 6 AVG);
2. De betrokkene kan alleen een inzageverzoek doen als hij ouder is dan 16 jaar en indien hij niet onder curatele is gesteld. Anders moet het verzoek door de wettelijke vertegenwoordiger van de betrokkene worden gedaan.

De AVG geeft de betrokkenen de volgende rechten:

- Recht op inzage (artikel 15 AVG);
- Recht op correctie/rectificatie (artikel 16 AVG);
- Recht op gegevenswissing/vergetelheid (artikel 17 AVG);
- Recht op beperking van de verwerking (artikel 18 AVG);
- Recht op overdraagbaarheid van gegevens (dataportabiliteit) artikel 20 AVG);
- Recht van bezwaar (artikel 21 AVG);
- Niet te worden onderworpen aan volledige geautomatiseerde besluitvorming (waaronder profileren) met rechtsgevolgen of wanneer de betrokkene daardoor in aanmerkelijke mate wordt getroffen (artikel 22 AVG).

Recht op inzage

Een betrokkene heeft het recht om aan BPZ te vragen of die persoonsgegevens van hem of haar verwerkt. Wanneer dat het geval is moet er een overzicht komen met de volgende informatie:

- De doeleinden waarvoor de persoonsgegevens worden verwerkt;
- De categorieën van persoonsgegevens;
- De specifieke persoonsgegevens die van de betrokkene worden verwerkt;
- De (categorieën) van ontvangers waaraan persoonsgegevens zijn of kunnen worden doorgegeven ook van ontvangers in landen buiten de EER en internationale organisaties;
- Bewaartermijnen of criteria die gebruikt worden om de bewaartermijnen te bepalen;
- Het recht op rectificatie, gegevenswissing, beperking en bezwaar;
- Het recht om een klacht in te dienen bijeen toezichthoudende autoriteit;
- Bronnen van persoonsgegevens die niet van de betrokkene zelf verkregen zijn;
- Het bestaan van geautomatiseerde besluitvorming en/of profilering.

In bijlage 8 is een nadere detaillering opgenomen van het Recht op inzage.

Recht op correctie/rectificatie

Op basis van inzage in zijn gegevens kan een betrokkene BPZ verzoeken de gegevens te verbeteren of aan te vullen. Daarbij zijn de doeleinden van de verwerking bepalend.

BPZ informeert degenen aan wie persoonsgegevens zijn verstrekt over de correctie/rectificatie van de betreffende gegevens.

In bijlage 8 is een nadere detaillering opgenomen van het Recht op correctie/rectificatie.

Recht op gegevenswissing/vergetelheid

Het recht op gegevenswissing houdt in dat een betrokkene het recht heeft om gegevens die van hem of haar worden verwerkt te laten wissen. Het recht staat ook bekend als “Het recht om vergeten te worden”. Het is geen absoluut recht, maar aan voorwaarden gebonden, Het recht is vastgelegd in artikel 17 AVG.

Een betrokkene kan BPZ vragen om zijn of haar persoonsgegevens te wissen, hieraan wordt gevolg gegeven wanneer:

- De gegevens niet meer nodig zijn voor het doel waarvoor ze zijn verzameld en verder verwerkt;
- Wanneer de verwerking is gebaseerd op toestemming en die wordt ingetrokken en er is geen andere grondslag;
- De betrokkene terecht bezwaar heeft gemaakt tegen de verwerking;
- De gegevensverwerking niet rechtmatig is;
- Wissen verplicht is om te kunnen voldoen aan een wettelijke verplichting.

Wanneer de betrokkene het recht heeft zijn/haar gegevens te laten wissen, moeten we ook bekijken of het gaat om gegevens die wij verder openbaar hebben gemaakt, bijvoorbeeld door deze door te geven aan het Nationaal Pensioen Register. Is dat zo dan zullen wij redelijke maatregelen treffen om hen (andere verwerkingsverantwoordelijken) te informeren over het feit dat de betrokkene deze gegevens heeft laten wissen. Daarbij mogen we wel rekening houden met uitvoeringskosten en beschikbare technologie. Met andere woorden we hoeven niet alles te doen wat mogelijk is, we moeten van geval tot geval bekijken wat dan redelijk is.

BPZ informeert degenen aan wie persoonsgegevens zijn verstrekt over de wissing van de betreffende gegevens.

Recht op beperking van de verwerking

In een aantal gevallen heeft de betrokkene het recht om BPZ te verplichten de verwerking van diens gegevens te beperken. Dit is een ander recht dan het recht van bezwaar. Dat betekent dan dat de gegevens waar het over gaat alleen verwerkt mogen worden:

- Met toestemming van de betrokkene;
- Om ze op te slaan;
- Om ze te gebruiken bij een rechtsvordering of voor de bescherming van rechten van een andere natuurlijke- of rechtspersoon;
- Om ze te gebruiken voor om belangrijke redenen van algemeen belang voor de Europese Unie of een lidstaat.

Het recht kan worden ingeroepen in de volgende gevallen:

- De juistheid van de gegevens wordt betwist. De beperking geldt dan voor een periode die nodig is om de juistheid te controleren. De verantwoordelijke heeft zo invloed op de periode van de beperking;
- De verwerking is onrechtmatig, maar de betrokkene verzet zich tegen wissing;
- De verantwoordelijke heeft de gegevens niet meer nodig, maar de betrokkene wel in het kader van een rechtsvordering;
- Wanneer bezwaar gemaakt is tegen de verwerking. De beperking geldt dan voor de periode die nodig is om vast te stellen dat de gerechtvaardigde gronden voor de verwerking van de verwerkingsverantwoordelijke zwaarder wegen dan de belangen van de betrokkene.

BPZ informeert degenen aan wie persoonsgegevens zijn verstrekt over de beperking van de verwerking van de betreffende gegevens. Wordt de beperking opgeheven dan informeert BPZ eerst degene die een beroep op dit recht heeft gedaan.

Recht op overdraagbaarheid van gegevens (dataportabiliteit)

Wanneer een betrokkene persoonsgegevens aan BPZ heeft verstrekt en de verwerking van die gegevens is gebaseerd op toestemming of is noodzakelijk voor de uitvoering van een overeenkomst met de betrokkene en het gaat om automatische verwerking van die gegevens, dan heeft de betrokkene het recht om die gegevens in een gestructureerde, gangbare en machine leesbare vorm terug te krijgen. De betrokkene mag deze gegevens dan zonder meer overdragen aan een andere verwerkingsverantwoordelijke (artikel 20 AVG).

Recht van bezwaar

Een betrokkene kan in enkele gevallen bezwaar maken tegen het verwerken van zijn persoonsgegevens in verband met bijzondere omstandigheden. Bezwaar kan dan worden gemaakt tegen verwerking van gegevens die is gebaseerd op noodzakelijkheid voor het vervullen van een taak van openbaar belang of openbaar gezag (artikel 6, lid 1, onder e, AVG) of op noodzakelijkheid voor de behartiging van een gerechtvaardigd belang (artikel 6, lid 1, onder f, AVG), ook wanneer er sprake is van profilering op basis van deze bepalingen. Ook kan een betrokkene bezwaar maken wegens bijzondere omstandigheden bij wetenschappelijk of historisch onderzoek of het verzamelen voor statistische doeleinden, behalve wanneer de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang.

Profilering en geautomatiseerde besluitvorming

In de AVG is ‘Profilering’ als volgt gedefinieerd: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen (Artikel 4 lid 4 AVG).

Persoonsgegevens gebruiken voor het opstellen van profielen en het toepassen van die profielen valt onder de ‘normale’ regels van de AVG. De verschillende onderwerpen uit dit privacy beleid zijn van toepassing.

BPZ heeft niet de intentie tot de opbouw van klantprofielen. Mocht BPZ de intentie hebben tot de opbouw van klantprofielen zullen wij toestemming vragen van betrokkene en toegang tot profielen geven.

Bij BPZ is er geen sprake van volledig geautomatiseerde besluitvorming. Mocht deze plaats vinden dan kan een betrokkene het recht uitoefenen om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming, waaronder profilering, in overeenstemming met art 22 AVG indien deze besluiten rechtsgevolgen voor hem hebben.

3.7 Technische en organisatorische maatregelen (waaronder beveiliging)

Persoonsgegevens moeten goed beveiligd worden door passende technische en/of organisatorische maatregelen zodat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (art 5 lid 1 sub f AVG).

De verantwoordelijke heeft meer algemeen de verplichting om passende technische en organisatorische maatregelen te treffen om aan te kunnen tonen dat de verwerking van persoonsgegevens in overeenstemming met de AVG wordt uitgevoerd. Maatregelen dienen geëvalueerd en indien nodig geactualiseerd te worden.

Op de persoonsgegevens die onder verantwoordelijkheid van BPZ worden verwerkt is in het kader van de beveiliging het Achmea Informatiebeveiligingsbeleid van toepassing en zijn afspraken gemaakt met derde partijen (verwerkers).

Technische en organisatorische maatregelen

Technische maatregelen zijn de logische en fysieke maatregelen in en rondom de informatiesystemen (bijvoorbeeld toegangscontroles/autorisatie management, logging van handelingen, back ups, versleuteling van persoonsgegevens, beveiliging van transport van persoonsgegevens, databases gescheiden houden omdat gegevens ingezet worden voor diverse doelen zodat verdere verwerking voorkomen wordt).

Organisatorische maatregelen zijn maatregelen voor de inrichting van de organisatie en voor het verwerken van de persoonsgegevens (bijvoorbeeld het toekennen van verantwoordelijkheden en bevoegdheden, instructies, trainingen en calamiteitplannen).

Beveiliging: Passend beschermingsniveau

Beveiliging is een inspanningsverplichting, maar wel met een ondergrens. Maatregelen die in de wereld van informatievoorziening als minimaal noodzakelijk worden gezien moeten ook minimaal getroffen zijn.

Criteria daarbij van belang zijn (art 24 en 34 AVG):

- De stand der techniek: allereerst wordt vastgesteld welke technische maatregelen op dat moment beschikbaar zijn; achterhaalde technieken worden niet langer als passend geclassificeerd; de verantwoordelijke zal bij het bepalen van de te nemen technische maatregelen een afstemming moeten vinden tussen de technische faciliteiten die in gebruik zijn bij de verwerking en die in gebruik zijn bij de beveiliging van persoonsgegevens; de verantwoordelijke zal deze analyse periodiek herhalen.
- De uitvoeringskosten: de verantwoordelijke maakt een keuze tussen de mogelijke technische en organisatorische maatregelen; in alle redelijkheid moet worden afgewogen of er een evenredigheid bestaat tussen de kosten van de beveiliging en het effect daarvan voor de beveiliging van persoonsgegevens.
- Aard van de gegevens: Daarbij is er een onderscheid tussen:
  - Persoonsgegevens: alle direct en indirect herleidbare gegevens (zie bijlage 3);
  - Gevoelige persoonsgegevens;*
  - Bijzondere persoonsgegevens (zie bijlage 3).
- De risico's die de verwerking met zich meebrengen: vastgesteld wordt welk risico de betrokkene en de verantwoordelijke lopen bij verlies of onrechtmatige verwerking van persoonsgegevens: naarmate het risico toeneemt zullen de maatregelen evenredig verzwaard moeten worden. Denk bij risico's voor de betrokkene bijvoorbeeld aan uitsluiting, identiteitsfraude, verlies van controle over gegevens, discriminatie, identiteitsdiefstal of –fraude, reputatieschade, financiële schade en evt. ander economisch nadeel.

- Omvang van de verwerking: de gegevens van enkele betrokkenen verwerken is wat anders dan het stelselmatig en op grote schaal verwerken van de persoonsgegevens van vele betrokkenen.
- Context van de verwerking: Zorg is bijvoorbeeld een andere context waar vertrouwelijkheid over het algemeen hoger zal zijn, dan bij Schade met name daar waar het gaat om materiële schade.
- Verwerkingsdoeleinden.

Maatregelen zijn, waar passend, o.a. (benoemd in art 34 AVG):

a) De pseudonimisering en versleuteling van persoonsgegevens;
b) Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen.
c) Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen. Dit betreft het Business Continuiteitsmanagement proces (BCM). Vanuit BCM worden er eisen gesteld aan de beschikbaarheid van processen, systemen en data.
d) Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

*Gevoelige persoonsgegevens

Gevoelige persoonsgegevens zijn door de AP geïntroduceerd als een categorie tussen persoonsgegevens en bijzondere persoonsgegevens voor het bepalen van een passend beschermingsniveau. Dit betreft:

- Gegevens over de financiële of economische situatie van de betrokkene.
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene.
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude. Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het burgerservicenummer (BSN).

Bij gevoelige gegevens dient een hoger beveiligingsniveau gehanteerd te worden.

Informatiebeveiliging en de Beleidsregels beveiliging 2013 vanuit de AP

De AP heeft in 2013 beleidsregels vastgesteld betreffende de beveiliging van persoonsgegevens. Deze leggen uit hoe de AP bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens de beveiligingsnormen uit voorheen de Wbp toepast en nu de AVG. Hoewel deze beleidsregels geen status van ‘wet’ hebben komt er wel groot belang aan toe omdat het weergeeft hoe de toezichthouder aankijkt tegen de open norm van de wet. De beleidsregels vormen de schakel tussen het juridisch domein en het domein van de informatiebeveiliging, waarin de noodzakelijke kennis en kunde aanwezig is om daadwerkelijk aan die eisen te voldoen. In bijlage 9 is nadere informatie opgenomen over de beleidsregels.

Privacy by design and by default

Gegevensbescherming door ontwerp (design) en door standaardinstellingen (by default).

Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst van uiteenlopende risico’s voor de rechten en vrijheden van de betrokkene(n) moeten bij de bepaling van de verwerkingsmiddelen en bij de verwerking zelf passende technische en organisatorische maatregelen getroffen worden (art. 25 AVG). De maatregelen hebben als doel de gegevensbeschermingsbeginselen zoals minimale gegevensverwerking op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen om de naleving van de AVG te

borgen en ter bescherming van de rechten van betrokkenen. Daarbij dient o.a. rekening gehouden te worden met:

- Alleen persoonsgegevens verwerken die nodig zijn voor het doel;
- Minimaliseren van de hoeveelheid verzamelde gegevens;
- De mate waarin zij worden verwerkt zoveel mogelijk beperken;
- De termijn van opslag definiëren en vervolgens gegevens verwijderen of anonimiseren;
- Toegankelijkheid van de gegevens (autorisaties en beveiliging);
- Pseudonimiseren als beschermingsmaatregel wordt expliciet benoemd in de wet.

Bij het ontwerpen van processen, producten en diensten kan door privacy vanaf het begin stadium (ontwerp) mee te nemen en requirements te definiëren vanuit privacy perspectief de nakoming van de verplichtingen uit de AVG geborgd worden. Zo kan bijvoorbeeld, als een product of dienst de betrokkene rechtstreeks raakt, in een interface rekening worden gehouden met rechten van de betrokkene door ruimte te geven aan zinvolle informatie en daar waar mogelijk / nodig controle over zijn persoonsgegevens voor een betrokkene.

Anonimiseren en Pseudonimiseren

- **Anonimiseren**
  Als gegevens geanonimiseerd worden dan vallen deze niet meer onder de AVG. Alle identificerende kenmerken moeten dan ontdaan zijn van de gegevens (zowel directe als indirecte persoonsgegevens).
- **Pseudonimisering**
  Als sprake is van pseudonimiseren blijft het pseudoniem een persoonsgegeven. Pseudonimiseren is een beveiligingsmaatregel. Deze wordt vaak in de AVG benoemd. Als een doel bereikt kan worden door gegevens te pseudonimiseren is dat een gewenste beveiligingsmaatregel. In de AVG is pseudonimisering als volgt gedefinieerd. Art 4 lid 5 AVG ‘pseudonimisering’: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

Verwerkers en passende maatregelen

In een aantal gevallen zal de verwerking van persoonsgegevens geheel of gedeeltelijk worden uitbesteed aan een derde partij verwerker (en evt. sub-verwerkers). Voor de beveiliging van persoonsgegevens geldt dat dit niet mag afdoen aan de passende technische en organisatorische maatregelen. BPZ blijft daar als uitbestedende partij verantwoordelijk voor. In art. 28 AVG is zelfs expliciet opgenomen dat uitsluitend wordt samengewerkt met verwerkers die afdoende garanties bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking aan de wet voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.

In de contracten met verwerkers moet de beveiliging van de persoonsgegevens opgenomen worden. Zie hierover Paragraaf 3.3 en bijlage 9.

3.8 Datalekken

Een datalek is een ‘’inbreuk in verband met persoonsgegevens’’. Dat is een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (art. 4 lid 12 AVG).

Datalek binnen 72u melden

Een datalek moet door de verantwoordelijke zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72u na kennis name aan de toezichthoudende autoriteit worden gemeld. In Nederland is dat de AP. Daarbij moet ten minste het volgende omschreven / meegedeeld worden (art 33 lid 1 en 3 AVG):

a) de aard van de inbreuk, waar mogelijk o.v.v. categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
b) de naam en contactgegevens van de FG of een ander contactpunt;
c) waarschijnlijke gevolgen van de inbreuk;
d) de maatregelen die de verantwoordelijke heeft voorgesteld of genomen om de inbreuk aan te pakken, waaronder in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen.

Wanneer het niet mogelijk is alle informatie gelijktijdig te verstrekking kan dat in fases. (Voorlopig) melden is dan belangrijker dan volledig zijn (art 33 lid 4 AVG).

Geen risico, dan niet melden bij de toezichthouder

Als het niet waarschijnlijk is dat een inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen hoeft niet gemeld te worden bij de toezichthouder (art. 33 lid 1 AVG).

Alle datalekken intern administreren

Ongeacht of een datalek gemeld wordt bij de toezichthouder, moeten alle datalekken door de verantwoordelijke gedocumenteerd worden met daarbij (art 33 lid 5 AVG):

- de feiten;
- de gevolgen;
- de genomen corrigerende maatregelen.

Verwerker moet alles melden bij BPZ

Een verwerker moet BPZ zonder onredelijke vertraging op de hoogte stellen van ieder datalek (art. 33 lid 2 AVG). Om die reden is in de standaard verwerkersovereenkomst opgenomen dat een verwerker direct (in elk geval binnen 48 uur), aan de contactpersoon van BPZ een datalek meldt als zij ontdekt of redelijkerwijs vermoedt dat die heeft plaatsgevonden.

Bij hoog risico ook melden aan de betrokkene(n)

Als een datalek waarschijnlijk een hoog risico inhoudt voor de betrokkene(n) moet het datalek ook onverwijld aan betrokkene(n) worden gemeld in duidelijke en eenvoudige taal (art. 34 lid 1 en 2 AVG):

- een omschrijving van het datalek;
- de naam en contactgegevens van de FG of een ander contactpunt;
- waarschijnlijke gevolgen van de inbreuk;
- de maatregelen die de verantwoordelijke heeft voorgesteld of genomen om de inbreuk aan te pakken, waaronder in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen.

Wanneer hoeft er niet gemeld te worden aan betrokkene(n) (art 34 lid 3 AVG)

- als er maatregelen zijn getroffen die de persoonsgegevens onbegrijpelijk maken voor onbevoegden (zoals encryptie);
- door achteraf genomen maatregelen die zorgen dat het datalek waarschijnlijk geen hoog risico meer is voor de betrokkene;
- als een mededeling onevenredige inspanning vergt. Dan moet er een openbare mededeling of soortgelijke maatregelen getroffen worden waarbij betrokkenen even doeltreffend worden geïnformeerd.

Een toezichthouder kan verplichten om alsnog te melden aan betrokkene(n) ook al is een uitzondering van toepassing (art 34 lid 4 AVG).

3.9 Privacy Impact Assessment (PIA)

Met een PIA (in de AVG een 'gegevensbeschermingseffectbeoordeling' genoemd) kan aangetoond worden dat bij hoog risico verwerkingen aan de wet voldaan wordt.

Een PIA is een proces gemaakt om een verwerking te omschrijven, de noodzakelijkheid en proportionaliteit van een verwerking te onderzoeken en de risico's en rechten en vrijheden van betrokkenen te managen (door deze te onderzoeken en passende maatregelen te bepalen).

Wanneer is een PIA verplicht?

Een PIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacy risico oplevert voor de betrokkenen. De wet noemt drie omstandigheden waarbij een PIA verplicht is:

- systematisch en uitvoerig persoonlijke aspecten evalueren, waaronder profiling;
- op grote schaal bijzondere persoonsgegevens verwerken;
- op grote schaal en systematisch mensen volgen in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Naast deze drie situaties geeft de AVG geen overzicht van verwerkingen met een hoog risico. De werkgroep van Europese privacytoezichthouders (WP 29) heeft criteria opgesteld om het risico te bepalen. In bijlage 10 zijn deze nader toegelicht.

Wanneer is een PIA niet verplicht?

- Als een verwerking geen hoog risico is;
- Als de aard, reikwijdte, context en doelen van een verwerking overeen komen met een andere verwerking waar al een PIA voor uitgevoerd is. Dan kunnen de resultaten daarvan gebruikt worden;
- Als de verwerking op grond van de wet is voorgeschreven en er al een PIA is uitgevoerd door de overheid;
- Als de toezichthouder een lijst publiceert met verwerkingen waarvoor geen PIA nodig is.

Functionaris Gegevensbescherming

BPZ heeft een FG aangesteld. Namens BPZ wordt vastgesteld of derde partijen (verwerkers) de PIA's afdoende verrichten.

PIA iedere 3 jaar herijken

Een PIA dient iedere drie jaar herijkt te worden of eerder als het risico verandert (art 35 lid 11 AVG).

Boetes voor niet uitvoeren PIA

Het niet aantoonbaar uitvoeren van een PIA wanneer deze verplicht is of het niet vooraf raadplegen van de toezichthouder als er een hoog risico overblijft voor betrokkenen, kan resulteren in een boete.

Hoog risico blijft? Voorafgaande raadpleging AP

Wanneer uit een PIA blijkt dat de verwerking een hoog risico zou opleveren en er gezien (on)beschikbare technologie en uitvoeringskosten geen goede maatregelen mogelijk zijn om het risico te beperken (de verwerking blijft een hoog risico), moet de AP voorafgaand aan de verwerking geraadpleegd worden.

4. Bijlagen

Bijlagen	
	Bijlage 1 Begrippen Bijlage 2 Nadere toelichting FG en Privacy Organisatie BPZ Bijlage 3 Nadere toelichting (Bijzondere) persoonsgegevens Bijlage 4 Nadere toelichting Verwerkingsverantwoordelijke, verwerker en verwerkersovereenkomst Bijlage 5 Nadere toelichting Verwerkingsregister Bijlage 6 Nadere toelichting Beginselen voor verwerking Bijlage 7 Nadere toelichting Privacyverklaring Bijlage 8 Nadere toelichting Rechten betrokkenen Bijlage 9 Beleidsregels Beveiliging Persoonsgegevens Bijlage 10 Nadere toelichting Privacy Impact Assessment (PIA)

Bijlage 1 Begrippen

Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

Persoonsgegeven

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Identificeerbaar wil zeggen direct- of indirect identificeerbaar aan de hand van bijvoorbeeld een naam, nummer, of locatiegegevens (identificatoren, al dan niet on line) of aan de hand van een aantal elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van de betreffende natuurlijke persoon.

Betrokkene

Een betrokkene is degene op wie een persoonsgegeven betrekking heeft. Bijvoorbeeld de verwerkingen van gegevens van deelnemers.

Verwerkingsverantwoordelijke

De natuurlijke persoon, of rechtspersoon die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Dit is BPZ.

Verwerker

Een verwerker is degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Bij een verwerker gaat het altijd om een persoon of organisatie buiten BPZ.

Toestemming van de betrokkene

Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting, waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.

Verwerken van persoonsgegevens

Dit is in feite elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd via **geautomatiseerde** processen. Deze handelingen kunnen bestaan uit verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden, of op een andere wijze ter beschikking stellen, aligneren, combineren, afschermen wissen, of vernietigen.

Bijlage 2 Nadere toelichting FG en Privacy Organisatie BPZ

Onder AVG geen verplichte FG voor BPZ

BPZ is onder AVG niet verplicht een FG aan te stellen. Een FG is wettelijk verplicht in drie situaties:

1. Bij overheidsinstanties en publieke organisaties;
2. Voor organisaties die vanuit hun kernactiviteiten (de processen die essentieel zijn om de doelen van de organisatie te bereiken of die tot de hoofdtaken van de organisatie horen) op grote schaal individuen volgen. Het kan hierbij gaan om bijvoorbeeld profilering van mensen voor het maken van risico-inschattingen. Relevant hierbij zijn onder meer het aantal betrokkenen en aantal gegevens en de tijdsduur van het volgen.
3. Als op grote schaal bijzondere persoonsgegevens verwerkt worden als kernactiviteit. Bijvoorbeeld gezondheidsgegevens, ras, politieke opvatting, geloofsovertuiging of strafrechtelijke verleden.

BPZ heeft wel een FG aangesteld omdat er wel op grote schaal persoonsgegevens worden verwerkt. Daarnaast beschikt BPZ voor de arbeidsongeschikte deelnemers over gegevens om de premievrije voortzetting bij invaliditeit te kunnen vaststellen. Hieronder staan de eisen voor de FG opgenomen.

Onafhankelijkheid en geen belangenverstrengeling

De FG moet zijn functie in onafhankelijkheid kunnen uitvoeren en geen instructies ontvangen over het uitvoeren van zijn taken. Hij heeft ook ontslagbescherming die gerelateerd is aan de uitvoering van die taken.

FG mag binnen de organisatie niet (ook) een functie hebben waarin hij het doel en middelen van een gegevensverwerking bepaalt. Een FG mag andere taken vervullen maar het mag niet leiden tot een belangenconflict. De FG brengt rechtstreeks verslag uit aan de hoogste leidinggevende van de organisatie. Dit is bij BPZ het bestuur.

Privacy kennis en bedrijfskennis vereist

Van een FG wordt verwacht dat hij of zij bovengemiddelde vakkennis heeft van privacywetgeving en de praktijk van gegevensbescherming. Waaronder:

- kennis van nationale en Europese privacywet- en regelgeving over gegevensbescherming;
- begrip van de gegevensverwerkingen die de organisatie uitvoert;
- begrip van IT en informatiebeveiliging;
- kennis van de organisatie en de sector waarin die actief is;
- het kunnen promoten van een cultuur van gegevensbescherming binnen de organisatie.

Taken FG

- Het informeren en adviseren over verplichtingen die voortvloeien uit de AVG, de Uitvoeringswet AVG en andere regelgeving op het gebied van de bescherming van persoonsgegevens;
- Toezien op de naleving van de AVG en de aanpalende regelgeving;
- Toezien op naleving en monitoring van het Privacybeleid (incl. verwerkers);
- Toewijzen van verantwoordelijkheden op het gebied van het verwerken van persoonsgegevens;
- Adviseren, monitoren en betrokkenheid bij Privacy Impact Analyses (incl. verwerkers);
- Samenwerken met de AP;
- Fungeren als contactpunt voor de AP. Contacten met de AP lopen altijd via de FG.
- Fungeren als contactpunt voor betrokkenen (bijvoorbeeld deelnemers) wanneer dat relevant is wanneer zij gebruik willen maken van de rechten die zij op grond van de AVG hebben;

- Rapporteren en bespreken naar het bestuur van het fonds;
- Advisering en monitoring van het verwerkingsregister (incl. verwerkers);
- Advisering en actueel houden van het Privacy Beleid.

De contactgegevens van de FG moeten bekend worden gemaakt bij de AP.

Bijlage 3 Nadere toelichting (Bijzondere) persoonsgegevens

Begrip Persoonsgegeven inclusief elementen

Hieronder is het begrip **Persoonsgegeven** gedefinieerd:

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Identificeerbaar wil zeggen direct- of indirect identificeerbaar aan de hand van bijvoorbeeld een naam, nummer, of locatiegegevens (identificatoren, al dan niet on line) of aan de hand van een aantal elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van de betreffende natuurlijke persoon.

Het begrip persoonsgegevens bestaat uit een aantal elementen:

1. Alle informatie over een persoon;
2. Geïdentificeerde of identificeerbare;
3. Natuurlijk persoon.

1. Alle informatie over een persoon

Een aantal elementen zijn bepalend voor de vraag of een gegeven ook een persoonsgegeven is:

a. Inhoud: bijvoorbeeld naam, adres;
b. (beoogd) doel: bijvoorbeeld fraude onderzoek, bijhouden van logging om wijzigingen te kunnen traceren naar een persoon of voor fraude onderzoek, een identificatienummer;
c. Resultaat: bijvoorbeeld toepassen van gerichte communicatie op een deelpopulatie.

De vorm van de informatie maakt niet uit. Het kan gaan om geschreven tekst maar ook bijvoorbeeld beeld, geluid, spraak.

Het moet wel gaan om informatie over een persoon of informatie die relateert aan een persoon. Een postcode zonder nadere aanduiding (nummer, pand) op zich is geen persoonsgegeven.

Of een gegeven iets zegt over een persoon is context afhankelijk, waarbij ook het (maatschappelijk) gebruik van gegevens meegewogen moet worden. Bijvoorbeeld gegevens die niet direct betrekking hebben op een bepaalde persoon, maar op een product of een proces, kunnen soms over een bepaalde persoon informatie verschaffen. Bijvoorbeeld wanneer daarmee de productiviteit of het aantal fouten van een specifieke werknemer van een uitbestedingspartners gemakkelijk in kaart kan worden gebracht.

Gegevens die uitsluitend voorwerpen aanduiden als daar geen persoon aan gekoppeld kan worden, zijn geen persoonsgegevens (maar zuivere objectgegevens).

2. Geïdentificeerde of identificeerbare

Criterium voor ‘identificeerbare’ is of een natuurlijk persoon redelijkerwijs geïdentificeerd zou kunnen worden. Dat kan door BPZ zijn als verantwoordelijke maar ook door een willekeurig ander bedrijf / derde (door selectie, koppelen).

Iets wat nu geen persoonsgegeven is, zou dat in de toekomst kunnen worden (door technologische ontwikkeling). Of identificatie ‘’redelijkerwijs’’ mogelijk is (en een gegeven daarmee een persoonsgegeven is), hangt af van de kosten en tijd benodigd voor eventuele identificatie en de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen. Dat is ‘gezien de markt’ en dus niet enkel op basis van de bij BPZ of uitbestedingspartners beschikbare middelen. Als identificatie van personen vele dagen rekenen door computer(s) in beslag neemt, kan gezegd worden dat identificatie ‘redelijkerwijs niet mogelijk is’ en dus de wet niet van toepassing is.

Niet elk technisch of toevallig verband tussen een gegeven en een persoon is dus voldoende om dat gegeven een persoonsgegeven te doen zijn. Is de mogelijkheid weliswaar theoretisch aanwezig maar is het ondenkbaar dat dit ook daadwerkelijk gebeurt, dan kan ervan worden uitgegaan dat de gegevens niet als persoonsgegevens worden aangemerkt.

Een geanonimiseerd gegeven is geen persoonsgegeven. Het gegeven moet dan van alle identificerende kenmerken zijn ontdaan.

Bij encryptie of pseudonimiseren zegt dat wat over de beveiligingsmaatregelen die zijn getroffen, maar het maakt niet uit voor de beoordeling of het een persoonsgegevens is.

3. Natuurlijk persoon:

a. Overledenen vallen niet onder de reikwijdte van de wet;
b. Rechtspersonen vallen niet onder de reikwijdte van de wet, tenzij daar een individu uit afgeleid kan worden. Denk aan een ZZP'er of bijvoorbeeld een éénmanszaak.

Bijzondere persoonsgegeven

1. Begripsvorming.

Art. 9 lid 1 AVG: Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

De aard van sommige gegevens brengt mee dat de verwerking ervan een grotere inbreuk kan maken op de persoonlijke levenssfeer van de betrokkene omdat die gegevens gevoelige informatie over iemand verschaffen. In de AVG worden deze gegevens 'bijzondere persoonsgegevens' genoemd. Voor de verwerking van deze bijzondere gegevens geldt een verbod, tenzij er een wettelijke uitzondering van toepassing is. Die uitzondering kan in de AVG staan of in een wet van de lidstaten.

In het AVG artikel worden een aantal verschillende woorden gebruikt zoals ''waaruit blijkt'', ''over'' en ''met betrekking tot''.

- Gegevens waaruit blijkt:
  - Ras of etnische afkomst;
  - Politieke opvattingen;
  - Religieuze of levensbeschouwelijke overtuigingen;
  - Lidmaatschap vakbond.
- Genetische gegevens;
- Biometrische gegevens met het oog op de unieke identificatie van een persoon;
- Gegevens over gezondheid;
- Gegevens met betrekking tot: seksueel gedrag of seksuele gerichtheid.

In artikel 9 AVG worden een aantal algemene uitzonderingen genoemd tot het verbod van bijzondere persoonsgegevens. Deze hebben wij in dit beleid niet limitatief opgenomen.

2. Gegevens over gezondheid

Art. 4 lid 15 ‘’gegevens over gezondheid’’: persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.

Conform overweging 35 AVG betreft gegevens over de gezondheid:

Alle gegevens die betrekking hebben op de gezondheidstoestand van een betrokkene (lichamelijk en geestelijk) in het verleden, het heden en de toekomst. Dit betreft onder andere:

- informatie die is verzameld in het kader van de registratie voor of de verlening van gezondheidszorgdiensten die aan patiënten worden verstrekt om de gezondheidstoestand te beoordelen, te behouden of te herstellen, waaronder begrepen het voorschrijven en het verstrekken van geneesmiddelen en medische hulpmiddelen;
- een aan een natuurlijke persoon toegekend cijfer, symbool of kenmerk dat als unieke identificatie van die natuurlijke persoon geldt voor gezondheidsdoeleinden;
- informatie die voortkomt uit het testen of onderzoeken van een lichaamsdeel of lichaamseigen stof, met inbegrip van genetische gegevens en biologische monsters;
- informatie over bijvoorbeeld ziekte, handicap, ziekterisico, medische voorgeschiedenis, klinische behandeling of de fysiologische of biomedische staat van de betrokkene (ongeacht de bron, zoals bijvoorbeeld een arts of een andere gezondheidswerker, een ziekenhuis, een medisch hulpmiddel of een in-vitrodiagnostiek).

In de Uitvoeringswet AVG (art. 23 lid 1) is opgenomen dat de volgende partijen gezondheidsgegevens mogen verwerken en voor welk doel:

f. bestuursorganen, pensioenfondsen, werkgevers of instellingen die te hunnen behoeve werkzaam zijn voor zover dat noodzakelijk is voor:

1°. een goede uitvoering van wettelijke voorschriften, pensioenregelingen of collectieve arbeidsovereenkomsten die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene of

2°. de re-integratie of begeleiding van werknemers of uitkeringsgerechtigden in verband met ziekte of arbeidsongeschiktheid.

Geheimhouding

Lid 2 van art 23 Uitvoeringswet AVG geeft aan dat deze gegevens alleen verwerkt mogen worden door personen die uit hoofde van ambt, beroep of wettelijk voorschrift, dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht. Als de verantwoordelijke gegevens persoonlijk verwerkt en op hem niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht rust, is hij verplicht tot geheimhouding van de gegevens, behoudens voor zover de wet hem tot mededeling verplicht of uit zijn taak de noodzaak voortvloeit dat de gegevens worden meegedeeld aan andere die krachtens het eerste lid bevoegd zijn tot verwerking daarvan.

Bijlage 4 Nadere toelichting Verwerkingsverantwoordelijke, verwerker en verwerkersovereenkomst

Verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke (BPZ) is de entiteit die het doel van en de middelen voor de verwerking van persoonsgegevens bepaalt. De verwerker (artikelen 4 en 28 AVG) is de partij die ten behoeve van de verwerkingsverantwoordelijke (BPZ) persoonsgegevens verwerkt.

Verwerker

Een verwerker verwerkt persoonsgegevens uitsluitend op basis van schriftelijke instructies van BPZ als verantwoordelijke (art 28 lid 3 sub a AVG en art. 29) , dat wil zeggen overeenkomstig diens instructies en onder diens uitdrukkelijke verantwoordelijkheid. Een verwerker houdt er geen eigen doelen op na met persoonsgegevens!

Verwerkersovereenkomst

Het is verplicht met een verwerker een overeenkomst te sluiten. BPZ mag alleen zaken doen met betrouwbare verwerkers die voldoende garanties bieden (art 28 lid 1 AVG). Om die reden dient er een overeenkomst gesloten te worden met de verwerker die bindende aanspraken geeft aan BPZ en waarvan BPZ zich kan vergewissen dat de beveiliging van de verwerker op orde is door hieraan eisen te stellen (zoals, certificering door een derde). Dat leggen we vervolgens ook vast in de overeenkomst.

In de (verwerkers)overeenkomst met de leverancier dienen tenminste de volgende punten opgenomen te zijn:

- BPZ als verantwoordelijke (of een andere verantwoordelijke entiteit als daar sprake van is);
- De entiteit van de verwerker;
- dat de verwerker alleen gegevensverwerkingen uitvoert volgens de instructies van BPZ;
- het onderwerp en de duur van de verwerking;
- de doeleinden van de gegevensverwerking;
- het soort persoonsgegevens dat verwerkt wordt;
- de categorieën van betrokkenen op wie de gegevens zien;
- geheimhouding voor de medewerkers die met persoonsgegevens in aanraking komen;
- het niet inschakelen van sub-verwerkers zonder (algemene of specifieke) toestemming;
- passende technische en organisatorische maatregelen (o.a. beveiliging);
- een audit recht voor BPZ of een gemachtigde controleur;
- het na afloop vernietigen of terug leveren van de gegevens;
- het onverwijld melden van datalekken bij BPZ, zodat BPZ indien nodig op tijd kan melden bij de toezichthouder;
- het bijhouden van een verwerkingsregister door de verwerker;
- geen persoonsgegevens verwerken buiten de EER of een wettelijke passende waarborg afspreken als er wel doorgifte is buiten de EER.

De verwerkingsverantwoordelijke (BPZ) is verantwoordelijk en aansprakelijk voor de gegevensverwerking door de verwerker.

Bijlage 5 Nadere toelichting Verwerkingsregister

Verwerkingsregister

Conform Artikel 30 lid 1 AVG dient BPZ als verwerkingsverantwoordelijke een register bij te houden met verwerkingsactiviteiten, conform Artikel 30 lid 2 AVG dient de verwerker een register van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht. Dit mag schriftelijk en/of elektronisch. Het verwerkingsregister kan opgevraagd worden door de AP.

Het verwerkingsregister dient actueel te zijn. Dat betekent dat voordat met een nieuwe verwerkingsactiviteit wordt gestart, deze:

- onder wordt gebracht bij een bestaande geregistreerde verwerking; of;
- opgevoerd moet worden in het verwerkingsregister.

Als een gegevensverwerking ten onrechte niet (juist en volledig) is geadministreerd kan de AP een boete opleggen.

Wijzigingen in verwerkingen

Wijzigingen in verwerkingen, zowel binnen BPZ, als bij verwerkers moeten worden doorgegeven aan BPZ. Om te beoordelen of de administratie actueel en volledig is, wordt het verwerkingsregister jaarlijks afgestemd met de verwerkingsregisters van de verwerkers en voorgelegd aan het bestuur van BPZ met het verzoek de inhoud te accorderen. Ook zal nagevraagd worden om na te gaan of er verwerkingen zijn ontstaan die nog niet zijn opgenomen in het verwerkingsregister van BPZ.

Inhoud van de administratie

De AVG schrijft niet voor in welke mate van detail verwerkingsactiviteiten geadministreerd moeten worden. Een te hoge mate van detail vergt veel tijd / geld qua onderhoud en brengt het risico met zich mee dat de administratie niet actueel is. BPZ zal het verwerkingsregister vullen in lijn met het meldingsprogramma van de AP gebaseerd op art 27-30 Wbp (oud). Hierbij wordt rekening gehouden met het verschil tussen de eisen uit Wbp en art. 30 AVG voor het vastleggen van verwerkingen:

- Gezamenlijke verwerkingsverantwoordelijken benoemen;
- Functionaris voor Gegevensbescherming contactgegevens benoemen;
- (categorieën) ontvangers in derde landen of internationale organisaties;
- Naast doorgifte naar derde land ook indien internationale doorgifte plaatsvindt het land en (indien geen adequaatheidsbesluit of passende waarborg) de uitzondering van art. 49 lid 1 tweede alinea;
- indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist.

Verwerkingsregister BPZ als verwerkingsverantwoordelijke

Hieronder is per wettelijke eis uitgeschreven hoe / in welke mate van detail het verwerkingsregister wordt ingevuld. Cursief is nadere toelichting voor invulling aangegeven.

Wettelijke eis art. 30 lid 1 AVG	Invulling BPZ
Verwerkingsactiviteiten die onder verantwoordelijkheid van de verwerkingsverantwoordelijke plaatsvinden.	Dit betreft alle processen die nodig zijn voor het uitvoeren van de pensioenovereenkomst. Te denken valt aan communicatie, mutatieverwerking, premieberekeningen en het verrichten van uitkeringen.

De naam en contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris van gegevensbescherming.	De contactgegevens van het verantwoordelijke bestuurslid en de functionaris voor de gegevensbescherming worden opgenomen in het verwerkingsregister.
De naam en contactgegevens van de andere verantwoordelijke(n) als er sprake is van een gezamenlijke verwerkingsverantwoordelijkheid en, in voorkomend geval, van de vertegenwoordiger van de andere verwerkingsverantwoordelijke en van de functionaris van gegevensbescherming indien aanwezig.	In verwerkingsregister is opgenomen: o voor welke specifieke verwerkingsdoeleinden er wordt samengewerkt met andere verantwoordelijken (herverzekeraar, accountant en certificerend actuaris alsmede UWV en belastingdienst'' (art 26 AVG); o Contactgegevens en FG contactgegevens van de andere verantwoordelijken.
Categorieën van betrokkenen	Dit betreft leden van fondsgremia, deelnemers, slapers en uitkeringsgerechtigden

Categorieën persoonsgegevens;	Gekoppeld aan de categorieën betrokkenen: welke categorieën persoonsgegevens worden verwerkt.
	
	Daar waar bijzondere persoonsgegevens worden verwerkt en/of BSN wordt een koppeling gemaakt met specifieke doeleinden.
	
	Ter illustratie voorbeelden voor BSN en Gegevens betreffende de gezondheid:
	o BSN
	  o Bij de uitvoering van Pensioenen wordt het BSN gebruikt in de communicatie met de deelnemer.
	  o Bij het verstrekken van gegevens aan de Belastingdienst.
	o Gegevens betreffende de gezondheid
	  o Verzameldoel: Het verwerken van Premievrije deelnemers, het berekenen van een toereikende voorziening voor het fonds.

Categorieën van ontvangers aan wie de persoonsgegevens worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;	Persoonsgegevens worden onder meer vertrekt aan de belastingdienst, de herverzekeraar en indien nodig aan accountant en certificerend actuaris voor controledoeleinden. Persoonsgegevens van deelnemers, slapers en uitkeringsgerechtigden worden niet verstrekt aan leden van fondsgremia. Ook een subverwerker van Achmea kan beschikken over mailadressen voor het doen van communicatie.
Indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49 lid 1 AVG, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen.	Nvt

Indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist	BPZ neemt dit niet specifiek op in het verwerkingsregister. BPZ verwijst hierbij naar de afspraken gemaakt met de derde partijen (verwerkers).
Indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.	BPZ neemt dit niet specifiek op in het verwerkingsregister. BPZ verwijst hierbij naar het Achmea informatiebeveiligingsbeleid en/of de afspraken gemaakt met de derde partijen (verwerkers).

Administratie

Het verwerkingsregister voor BPZ als verwerkingsverantwoordelijke wordt bijgehouden door Achmea Pensioenservices.

Bijlage 6 Nadere toelichting Beginselen voor verwerking

Rechtmatige grondslag

De verwerking van persoonsgegevens moet gebaseerd zijn op één van de zes in de AVG limitatief genoemde grondslagen (art. 6 AVG). Deze grondslagen zijn:

a) Toestemming voor een of meer specifieke doelen;
b) Noodzakelijk voor de uitvoering van de overeenkomst waarbij de betrokkene partij is of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
c) Noodzakelijk om aan een wettelijke verplichting te voldoen;
d) Noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene omdat deze fysiek of juridisch geen toestemming kan geven: Deze grond is niet snel van toepassing in de context van BPZ
e) Noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verantwoordelijke is opgedragen;
f) Noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verantwoordelijke (of derde), behalve wanneer de belangen of de grondrechten en fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen.

Is geen van deze grondslagen aanwezig, dan is de verwerking van persoonsgegevens niet toegestaan.

Het is belangrijk om de verwerkingsgrondslag vast te stellen, omdat de verwerking daar op ingericht moet worden. De verplichtingen als verantwoordelijke en de rechten van de betrokkene kunnen namelijk verschillen afhankelijk van de verwerkingsgrondslag. Voor zover relevant voor de dagelijkse praktijk van BPZ worden de eisen per verwerkingsgrondslag hieronder behandeld.

Doelen/Doelbinding

Doel

Een doel / doelen voor verzameling van Persoonsgegevens moeten voldoen aan de volgende eisen:

- Welbepaald;
- Uitdrukkelijk omschreven; en,
- Gerechtvaardigd.

Een doel moet omschreven zijn vóórdat de verzameling van gegevens plaatsvindt.

Vervolgens mogen persoonsgegevens niet verder op een met de verzamel doeleinden onverenigbare wijze worden verwerkt (doelbinding / verenigbaar gebruik) (art. 5 lid 1 sub b AVG).

Welbepaald

Dit houdt in dat een verantwoordelijke geen persoonsgegevens mag verzamelen zonder een precieze doelomschrijving. Het doel moet welbepaald zijn voordat persoonsgegevens verzameld worden. Welbepaald betekent dat de doelomschrijving duidelijk moet zijn en niet zo vaag of ruim dat de doelomschrijving tijdens het verzamelproces geen kader kan bieden waaraan getoetst kan worden of de gegevens nodig zijn voor dat doel of niet.

Uitdrukkelijk omschreven

Betekent dat de verantwoordelijke het doel waarvoor hij persoonsgegevens verwerkt, moet hebben omschreven. Doelen moeten altijd passen binnen de in het verwerkingsregister omschreven doelen.

Gerechtvaardigd

Gerechtvaardigd betekent dat het doel niet in strijd mag zijn met de wet, openbare orde of goede zeden. Het ziet op alle aspecten van het recht. Een gerechtvaardigd doel hangt nauw samen met artikel 6 AVG waarin een limitatieve opsomming wordt gegeven van gronden die een verwerking van persoonsgegevens rechtvaardigen (zie rechtmatige grondslag).

Doelbinding

Persoonsgegevens mogen niet op een wijze worden verwerkt die onverenigbaar is met het verzameldoel / de verzameldoelen (art. 5 lid 1 sub b AVG).

Bij de beoordeling of een verwerking onverenigbaar is met het oorspronkelijke doel zijn de volgende criteria van belang:

- de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen;
- de aard van de betreffende gegevens: hoe gevoeliger de gegevens voor de betrokkene hoe minder snel gebruik voor andere doeleinden is toegestaan;
- de gevolgen van de beoogde verwerking voor de betrokkene;
- de wijze waarop en context waarin de gegevens zijn verkregen: De relatie tussen betrokkene en verantwoordelijke en de diensten die worden geleverd spelen een belangrijke rol bij deze factor;
- de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen: Denk bijvoorbeeld aan pseudonimiseren als anonimiseren niet mogelijk is. Aggregeren, maar ook autorisatiebeheer en andere maatregelen.

Bijlage 7 Nadere toelichting Privacyverklaring

BPZ is verplicht om aanspraak- en pensioengerechtigden te informeren over de verwerking van hun persoonsgegevens (artikel 12 AVG). Op de website van BPZ is een privacyverklaring opgenomen. In de AVG worden scherpere eisen gesteld aan de informatieplicht en daarmee aan de privacyverklaring. Deze worden hieronder toegelicht. De privacyverklaring wordt gezien als een eenzijdige overeenkomst. BPZ kan door deelnemers en pensioengerechtigden worden gehouden aan hetgeen in die verklaring wordt beloofd.

Transparantie

Met de AVG wordt als gevolg van versterking en vernieuwing van de rechten van betrokkenen het transparantiebeginsel in de wet geïntroduceerd. Het beginsel dat persoonsgegevens op een manier worden verwerkt die transparant is, houdt in dat deelnemers duidelijk geïnformeerd moeten worden over dat en hoe hun persoonsgegevens verzameld, gebruikt, geraadpleegd of op een andere manier verwerkt worden, waarom en door wie. Voor de privacyverklaring betekent dit:

- in heldere taal; de informatie aan deelnemers en daarmee de privacyverklaring moet beknopt, begrijpelijk, duidelijk, eenvoudig en gemakkelijk toegankelijk zijn;
- onderwerpen; in de privacyverklaring wordt invulling gegeven aan de volgende informatie:

	Onderwerpen	Vragen
1	Contactgegevens Pensioenfonds	Hoe kunnen betrokkenen contact opnemen met het Pensioenfonds en de Functionaris Gegevensbescherming (FG)
2	Doel en rechtsgrond	Waarom worden persoonsgegevens verzameld en waarom mag dat?
3	Gerechtvaardigde belangen	Wat zijn de gerechtvaardigde belangen van het fonds voor de gegevensverwerking? Aan wie worden de persoonsgegevens verder nog verstrekt? (ontvangers of categorieën van ontvangers)
4	Noodzaak	Zijn betrokkenen verplicht om de gevraagde persoonsgegevens te verstrekken of niet? En wat zijn de gevolgen als een betrokkene de persoonsgegevens niet verstrekt?
5	Informatieverstrekking	Waar en hoe kan de betrokkene vragen om inzage, rectificatie, wissen of overdracht van persoonsgegevens, klachten indienen, bezwaar maken of een verwerking beperken?
6	Intrekken verleende toestemming	Hoe kan een betrokkene een verleende toestemming intrekken?
7	Bewaartermijnen	Hoe lang kan het fonds de persoonsgegevens bewaren?
8	Persoonsgegevens buiten EU	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?
9	Geautomatiseerde besluitvorming	Doet het fonds aan geautomatiseerde besluitvorming (computergestuurde verwerking van persoonsgegevens zonder menselijke tussenkomst, bijvoorbeeld profilering)? En zo ja, welke logica wordt daarvoor gebruikt? Het fonds maakt geen gebruik van geautomatiseerde besluitvorming.
10	Cookies	Maakt het fonds gebruik van zogenoemde cookies, welke persoonsgegevens worden dan verzameld, waarom en op welke wijze? Het fonds heeft de specifieke informatie hierover in een afzonderlijke cookieverklaring opgenomen en verwijst daarnaar in de privacyverklaring.

Bijlage 8 Nadere toelichting Rechten betrokkenen

Nadere detaillering Recht op inzage

- De betrokkene heeft recht op een kopie van de persoonsgegevens die worden verwerkt. Dat betekent niet per definitie dat een kopie van een volledig dossier moet worden verstrekt, maar een overzicht van de categorieën verwerkte persoonsgegevens is niet voldoende (art. 15, lid 3 AVG);
- Wanneer gegevens worden verstrekt aan landen buiten de EER of internationale organisaties mag de betrokkene vragen om aan te geven welke maatregelen zijn getroffen om deze verstrekking op een verantwoorde wijze te laten plaatsvinden. Bijvoorbeeld het hanteren van EU standaard clausules wanneer het betreffende land geen adequaat beschermingsniveau kent (artikel 15, lid 2 AVG);
- Wanneer er sprake is van geautomatiseerde besluitvorming en/of profilering die leidt tot een besluit met rechtsgevolgen of een besluit dat de betrokkene in aanmerkelijke mate treft moet niet alleen aangegeven worden dat sprake is van geautomatiseerde besluitvorming/profilering, maar ook zinvolle (voor “leken” begrijpelijke) informatie over de logica daar achter en wat de verwachte gevolgen zijn van zo’n verwerking (artikel 15, lid 1, onder h);
- De reactie is schriftelijk (ook elektronisch). Een mondelinge reactie is op verzoek van de betrokkene mogelijk, wanneer de identiteit voldoende is vastgesteld met andere middelen ,dus niet mondeling (artikel 12, lid 1 AVG);
- Een elektronisch verzoek, wordt ook in een gangbaar elektronische vorm beantwoord, mits de betrokkene niet anders verzoekt (artikel 15, lid 3). Een dergelijke uitwisseling moet dan wel veilig plaats kunnen vinden;
- De reactietermijn is een maand, met verlening van één maand in moeilijke gevallen. De verlenging moet dan binnen de eerste maand worden meegedeeld (artikel 12, lid 3 AVG);
- Een verzoek is principe kosteloos. Wanneer een verzoek buitensporig is of onredelijk vaak herhaald wordt, mogen wel kosten in rekening gebracht worden of mag het inzage verzoek geweigerd worden (artikel 12, lid 5 AVG);
- Wanneer er veel informatie wordt verwerkt van de betrokkene kunnen we vragen om het inzageverzoek te specificeren voor een reactie te geven (Overweging 63 AVG);

Uitzonderingen

Er zijn uitzonderingen. In een aantal gevallen kan het inzagerecht worden geweigerd. Bijvoorbeeld wanneer uitoefenen van het recht strijdt met openbare veiligheid , de opsporing en vervolging van strafbare feiten of de bescherming van rechten en vrijheden van anderen. Dit is verder uitgewerkt in artikel 39 van de Uitvoeringswet Algemene verordening gegevensbescherming.

Nadere detaillering Recht op correctie/rectificatie

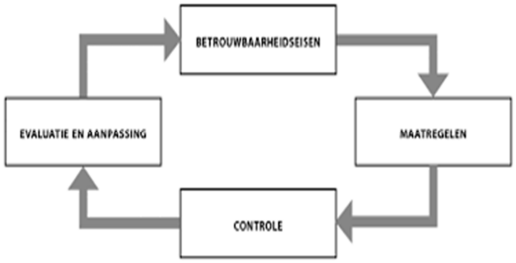
- De reactie is schriftelijk (ook elektronisch). Een mondelinge reactie is op verzoek van de betrokkene mogelijk, wanneer de identiteit voldoende is vastgesteld met andere middelen, dus niet mondeling (artikel 12, lid 1 AVG);
- De reactietermijn is een maand, met verlenging van één maand in moeilijke gevallen. De verlenging moet dan binnen de eerste maand worden meegedeeld (artikel 12, lid 3 AVG);
- Een verzoek is principe kosteloos. Wanneer een verzoek kennelijk ongegrond is mogen wel kosten in rekening gebracht worden of mag het rectificatieverzoek geweigerd worden (artikel 12, lid 5 AVG);

Bijlage 9 Beleidsregels Beveiliging Persoonsgegevens

De AP heeft in 2013 beleidsregels betreffende de beveiliging van persoonsgegevens vastgesteld. Deze leggen uit hoe de AP bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens de beveiligingsnormen uit voorheen de Wbp toepast en nu de AVG. Hoewel deze beleidsregels geen status van 'wet' hebben, zijn deze wel van groot belang omdat het weergeeft hoe de toezichthouder aankijkt tegen de open norm van de wet. De beleidsregels vormen de schakel tussen het juridisch domein en het domein van de informatiebeveiliging, waarin de noodzakelijke kennis en kunde aanwezig is om daadwerkelijk aan die eisen te voldoen

Het begint met een risicoanalyse. Vervolgens wordt op basis daarvan vastgesteld welke maatregelen noodzakelijk zijn zodat een bepaalde dreiging niet optreedt, danwel dat de gevolgen ervan wordt geminimaliseerd.

Eén van de kernpunten betreft de noodzaak van het inbedden van de zgn. "plan-do-check-act-cyclus" (ook genaamd: kwaliteitscirkel van Deming) in de dagelijkse praktijk van een organisatie:



Dat komt kort gezegd op het volgende neer:

1. Beoordeel de risico's

a. Beoordeel de risico's die de gegevens en de aard van de verwerking met zich meebrengen voor de betrokkenen. Inventariseer vervolgens de dreigingen die kunnen leiden tot een beveiligingsincident, de gevolgen die het beveiligingsincident kan hebben en de kans dat deze gevolgen zich voor zullen doen.

b. Classificeer de data: Voor persoonsgegevens is het daarbij belangrijk om niet sec het data attribuut te classificeren, maar dat te doen in de context van de verwerking. De algemene stelregel m.b.t persoonsgegevens is:

   i. Persoonsgegevens V (Vertrouwelijkheid) = 2;
   ii. Gevoelige persoonsgegevens V (Vertrouwelijkheid) = 3;
   iii. Bijzondere persoonsgegevens V (Vertrouwelijkheid) = 3.

   Wanneer het risico van ongewenste gevolgen en de schade die daaruit voortvloeit groot is, zal de classificatie van de vertrouwelijkheid hoger uitvallen en zullen hogere eisen worden gesteld aan de maatregelen die getroffen moeten worden.

c. Als de verwerking classificeert als een hoog risico: voer een Privacy Impact Assessment uit (Paragraaf 3.9).

De volgende stap is het vaststellen van de juiste maatregelen die het gewenste beveiligingsniveau kunnen waarborgen.

2. Maak gebruik van algemeen geaccepteerde beveiligingsstandaarden

Daar waar de risicoanalyse in kaart brengt welke beveiligingsrisico's er spelen, bieden beveiligingsstandaarden een handvat als het gaat om het mitigeren van deze beveiligingsrisico's zoals ISO/NEN normen. Het vakgebied informatiebeveiliging kent vele beveiligingsmethoden, -standaarden

en -maatregelen die zijn gebaseerd op ervaringen uit de dagelijkse beveiligingspraktijk. Deze standaarden geven houvast bij het daadwerkelijk treffen van passende maatregelen om de beveiligingsrisico's af te dekken. Correct gebruik van actuele beveiligingsstandaarden stelt de verantwoordelijke in staat om passende maatregelen te treffen en om tot een evenwichtig en effectief geheel aan technische en organisatorische maatregelen te komen.

De persoonsgegevens die onder verantwoordelijkheid van BPZ worden verwerkt is in het kader van de beveiliging het Achmea Informatiebeveiligingsbeleid van toepassing en zijn afspraken gemaakt met de derde partijen (verwerkers).

3 Controleer en evalueer regelmatig

Controleer met zekere regelmaat of de beveiligingsmaatregelen daadwerkelijk zijn getroffen en worden nageleefd. Beoordeel periodiek of het beveiligingsniveau nog steeds past bij de risico's die de verwerking en de aard van de te verwerken gegevens met zich meebrengen en of de beveiligingsmaatregelen nog steeds voldoen. Betrek daarbij ook de stand van de techniek en de nieuwste inzichten binnen het vakgebied informatiebeveiliging. Pas waar nodig de beveiligingsmaatregelen aan. Dit betreft zowel controle:

- op de (naleving van) maatregelen binnen de organisatie;
- op de technische maatregelen om te bepalen of die (nog) volstaan.

Bijlage 10 Nadere toelichting Privacy Impact Assessment (PIA)

Wanneer is er sprake van een hoog risico?

Naast de drie omstandigheden waarin een PIA verplicht is geeft de AVG geen overzicht van verwerkingen met een hoog risico. De werkgroep van Europese privacytoezichthouders (WP 29) heeft criteria opgesteld om het risico te bepalen. Advies is daarbij om bij twijfel een PIA uit te voeren omdat het een nuttig proces is om risico's in kaart te brengen en om aantoonbaarheid met het voldoen aan de AVG te borgen.

Art 29 WG criteria.
Aan hoe meer criteria de verwerking voldoet, hoe waarschijnlijker het is dat deze een hoog risico oplevert (en een PIA verplicht is):

1. Beoordelen of scoren van betrokkenen. Veelal op basis van persoonskenmerken (waaronder profileren). Zoals kredietwaardigheidsscores, klantbeeld op websites;
2. Geautomatiseerde beslissingen;
3. Stelselmatige (en grootschalige) monitoring;
4. Gevoelige gegevens verwerken;
5. Grootschalige gegevensverwerkingen: gezien de hoeveelheid betrokkenen, gegevens, tijdsduur en/of geografische reikwijdte;
6. Het koppelen van databases / datasets: koppelen of combineren van persoonsgegevens afkomstig uit verschillende gegevensverwerkingen met andere doelen en/of andere verantwoordelijken;
7. Gegevens over kwetsbare personen;
8. Gebruik van nieuwe technologieën:
9. Blokkering van een recht, dienst of contract: gegevensverwerkingen die tot gevolg hebben dat betrokkenen een recht niet kunnen uitoefenen, dat zij een dienst niet kunnen gebruiken of dat zij een contract niet kunnen afsluiten.

Als tenminste twee criteria geraakt worden is de stelregel dat er een hoog risico is en er dus een PIA uitgevoerd moet worden. Maar ook bij één kan dit al het geval zijn.

Als gezamenlijke verwerkingsverantwoordelijken een PIA uitvoeren moet daaruit specifiek een ieders verantwoordelijkheid blijken (wie doet wat en hoe zorgen we samen voor adequate bescherming).

Samenwerking met andere partijen? Dan samen de PIA uitvoeren.

Als een verwerking in het geheel of grotendeels door een verwerker wordt uitgevoerd moet de PIA samen met de verwerker uitgevoerd worden en moet die alle benodigde informatie verstrekken en de uitkomsten van de PIA bevestigen.

Inhoudelijke eisen PIA (minimaal):

Een PIA is een risicoanalyse vanuit privacy perspectief. Artikel 35 AVG vereist dat minimaal het volgende aan bod komt:

- een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden:
  - aard, reikwijdte, context, doelen;
  - persoonsgegevens, ontvangers, bewaartermijnen;
  - functionele beschrijving van de verwerking;
  - een dataflow incl. locaties (incl. assets waar gebruik van wordt gemaakt (hardware, software,
    netwerk, afdelingen, evt. fysieke dragers als papier).

- indien verwerkingsgrond ‘noodzakelijk voor de behartiging van een gerechtvaardigd belang’ is, een omschrijving van de gerechtvaardigde belangen van BPZ versus die van de betrokkene(n) om gevrijwaard te blijven van een inbreuk op privacy;
- een beoordeling van de noodzaak en de evenredigheid van de verwerking(en) met betrekking tot het doel / de doeleinden:
  - specifiek doel formuleren;
  - noodzakelijkheidstoets data t.o.v. doel;
  - rechtsgrondslag bepalen + evt. bijhorende verplichtingen (informeren, rechten betrokkene);
  - opslagbeperking.
- een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen (oorsprong, aard, specifieke karakter en ernst van de risico’s evalueren). In ieder geval meewegen: ongeautoriseerde toegang, ongewenste wijziging en het ongewenst verdwijnen van data;
- Gebaseerd op de risico’s, passende maatregelen vaststellen;
- Vaststellen van de beoogde maatregelen om de risico’s te mitigeren, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, inclusief het borgen van de rechten van de betrokkenen;
- Rekening houden met de ‘Code verwerking Persoonsgegevens Pensioenfondsen’ waar BPZ zich aan zal committeren zodra deze beschikbaar is (art 35 lid 8 jo. art. 40 AVG);
- De mening van betrokkenen vragen ‘’in voorkomend geval’’ (art 35 lid 9 AVG). Dit is geen verplichting, maar het helpt wel bij de onderbouwing richting betrokkenen en bijvoorbeeld een toezichthouder als het fonds de betrokkenen actief betrekt bij de vraag wat acceptabel wordt geacht.