

PF

Gedraglijn Verwerking Persoonsgegevens Pensioenfondsen

2023

Pensioenfederatie

De Pensioenfederatie is de overkoepelende belangenbehartiger van bijna alle Nederlandse pensioenfondsen. Zij vertegenwoordigt namens 166 pensioenfondsen de belangen van:

- 6 miljoen deelnemers
- 3,6 miljoen gepensioneerden
- 9,4 miljoen gewezen deelnemers.

Het overgrote deel van alle werkenden is aangesloten bij een collectief pensioenfonds.

De pensioenfondsen van de Pensioenfederatie beheren samen circa 1.800 miljard euro.

(Cijfers per 31-12-2021)

Contactinformatie

Prinses Margrietplantsoen 90
2595 BR Den Haag

Postbus 93158
2509 AD Den Haag

T + 31 (0)70 76 20 220
info@pensioenfederatie.nl
www.pensioenfederatie.nl

© Overname van tekst(delen) uit deze uitgave is mogelijk na toestemming van de Pensioenfederatie. Aan de inhoud van deze uitgave kunnen geen rechten worden ontleend.

Pensioenfederatie,
Den Haag, december 2022

Inhoudsopgave

	Inleiding	5
1	Overwegingen	6
2	Begripsbepalingen	7
3	De reikwijdte van de Gedraglijn	11
3.1	De sector	11
3.2	Toepassing	11
4	Beginselen van Verwerking van Persoonsgegevens	12
4.1	Wet en regelgeving	12
4.2	Doeleinden	12
5	Rechtmatigheid van de Verwerking	13
5.1	Rechtmatigheid	13
5.2	Noodzakelijkheid	13
6	Doeleinden voor de Verwerking van Persoonsgegevens	15
6.1	Inleiding	15
6.2	Persoonsgegevens in het kader van uitvoeren pensioenregeling	15
6.3	Persoonsgegevens in relatie tot historische, statistische en wetenschappelijke doeleinden	15
6.4	Persoonsgegevens in het kader van relatiemanagement en Direct Marketing activiteiten	16
6.5	Persoonsgegevens in verband met wettelijke voorschriften	16
6.6	Persoonsgegevens in verband met behartiging gerechtvaardigde belangen	17
6.7	Wijziging van doeleinden voor persoonsgegevens die reeds verwerkt worden	17
7	Verwerking van Bijzondere categorieën van en overige gevoelige Persoonsgegevens	18
7.1	Persoonsgegevens betreffende iemands gezondheid	18
7.2	Persoonsgegevens van strafrechtelijke aard	18
7.3	Kopie identiteitsbewijs	19
7.4	Gegevens van partners en kinderen van een deelnemer	19
7.5	Overige bijzondere Persoonsgegevens	19
7.6	Gevoelige Persoonsgegevens	19
7.7	BSN	19

8	Rechten van Betrokkene	20
8.1	Algemene bepalingen	20
8.2	Informatieplicht	21
8.3	Inzage	21
8.4	Correctie	22
8.5	Gegevenswissing (“recht op vergetelheid”)	22
8.6	Beperking van de Verwerking	23
8.7	Overdraagbaarheid van Persoonsgegevens	23
8.8	Bezwaar	23
8.9	Geautomatiseerde besluitvorming, waaronder profilering	24
9	Overige onderwerpen	25
9.1	Privacy by default en by design	25
9.2	Verwerkersovereenkomst	25
9.3	Register van Verwerkingen	26
9.4	Beleid bewaartermijnen	27
9.5	Beveiliging Verwerking	27
9.6	Datalekken	28
9.7	(Data) Privacy Impact Assessment/Gegevens- beschermingseffectbeoordeling	29
9.8	Functionaris	30
9.9	Doorgifte Persoonsgegevens	32
10	Beperkingen	35
11	Naleving van de Gedraglijn	36
12	Geschillen	37
	Toelichting en bijlage	38
	Bijlage Verwerkingsverantwoordelijke of Verwerker?	64

Inleiding

Pensioenfondsen streven sinds de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) naar een sector breed kader. Met dit kader laten pensioenfondsen zien op welke manier zij (Persoons)gegevens van (gewezen) deelnemers, pensioengerechtigden of andere aanspraakgerechtigden verwerken.

Dit sector brede kader is geen officiële gedragscode in de zin van artikel 40 van de AVG, met onafhankelijke monitoring in lijn met de voorschriften van de AVG. In plaats daarvan legt de pensioensector, na consultatie van de pensioenfondsen, een eigen Gedragslijn neer die recht doet aan het diverse karakter van pensioenfondsen en hun achterbannen. Deze Gedragslijn is geschreven door ervaringsdeskundigen werkzaam bij pensioenfondsen- en uitvoeringsorganisaties en sluit aan op de dagelijkse, actuele praktijk. In 13 hoofdstukken is een sector breed kader geschetst voor het verwerken van persoonsgegevens door pensioenfondsen.

Deze Gedragslijn stemt overeen met bepalingen uit de AVG. De Gedragslijn wordt periodiek getoetst op wijzigingen in de Uitvoeringswet AVG en nieuwe interpretaties. De Gedragslijn heeft een bindend karakter en pensioenfondsen leven deze Gedragslijn na. De bijlagen en toelichtingen geven sectorspecifieke voorbeelden weer. Deze voorbeelden kunnen worden gebruikt. Deze voorbeelden hebben geen bindend karakter.

De Autoriteit Persoonsgegevens (AP) kan vanwege de wettelijke taak de gedragslijn niet goedkeuren zoals bij een gedragscode, wel wordt de AP in kennis gesteld van de Gedragslijn.

Deze Gedragslijn is het sluitstuk op de eerder uitgebrachte servicedocumenten '[Gegevensbescherming](#)' en '[Guidance verwerking persoonsgegevens pensioenfondsen](#)'. De eerste Gedragslijn trad in werking per 1 juli 2019. Pensioenfondsen hebben daarna 6 maanden de tijd gehad om de Gedragslijn te implementeren. Per 1 januari 2020 rapporteren Pensioenfondsen over de naleving van de Gedragslijn. De "Gedragslijn verwerking persoonsgegevens pensioenfondsen 2023" geldt per 1 januari 2023 en werd vastgesteld in de algemene ledenvergadering van de Pensioenfederatie op 1 december 2022.

1

Overwegingen

Pensioenfondsen verwerken in het kader van hun bedrijfsvoering Persoonsgegevens en vinden het belangrijk dat met deze Persoonsgegevens zorgvuldig wordt omgegaan en dat deze vertrouwelijk worden behandeld.

De Algemene verordening gegevensbescherming (AVG) biedt waarborgen voor de bescherming van de persoonlijke levenssfeer van natuurlijke personen met betrekking tot het verwerken van Persoonsgegevens.

De Pensioenfederatie heeft in lijn met het bepaalde in de AVG de Gedragslijn Verwerking Persoonsgegevens Pensioenfondsen (hierna: Gedragslijn) opgesteld.

De Gedragslijn heeft tot doel:

- a uniforme en specifieke gedragslijnen te geven voor Pensioenfondsen voor het Verwerken van Persoonsgegevens;
- b inzicht geven aan personen van wie Persoonsgegevens door Pensioenfondsen verwerkt (zullen) worden;
- c bij te dragen aan de transparantie over de uitgangspunten die door de Pensioenfondsen worden gehanteerd met betrekking tot het Verwerken van Persoonsgegevens; en
- d een passende interpretatie te geven aan het wettelijk kader dat aansluit bij de strekking van de wetgeving en op de specifieke kenmerken van de pensioensector.

2

Begripsbepalingen

In deze Gedraglijn wordt verstaan onder:

- a AP: de Autoriteit Persoonsgegevens zoals bedoeld in artikel 6 van de Uitvoeringswet AVG.
- b AVG: Algemene Verordening Gegevensbescherming. Hieronder valt tevens de Uitvoeringswet Algemene Verordening Gegevensbescherming (Uitvoeringswet AVG).
- c Bestand: elk gestructureerd geheel van Persoonsgegevens dat volgens bepaalde criteria toegankelijk is, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid.
- d Betrokkene(n): degene op wie een Persoonsgegeven(s) betrekking heeft/hebben zoals (gewezen) deelnemer, pensioengerechtigde of andere aanspraakgerechtigde (onder andere nabestaande).
- e Bijzondere categorieën van persoonsgegevens: 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.
- f Biometrische gegevens: Persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen.
- g DPIA (Data Protection Impact Assessment): de gegevensbeschermings-effect-beoordeling zoals bedoeld in artikel 35 AVG.
- h Derde: eenieder, niet zijnde de Betrokkene, de Verwerkingsverantwoordelijke, de Verwerker, of enig persoon die onder rechtstreeks gezag van de Verwerkingsverantwoordelijke of de Verwerker gemachtigd is om Persoonsgegevens te verwerken.

- i Direct Marketing: digitaal, telefonisch dan wel per post overbrengen van (product)informatie anders dan de wettelijke verplichte pensioeninformatie door een Pensioenfonds aan een Betrokkene ten behoeve van commerciële of ideële doeleinden.
- j Functionaris: de functionaris voor gegevensbescherming, ook wel aangeduid als FG, zoals bedoeld in artikel 37 AVG.
- k Gedraglijn: de Gedraglijn Verwerking Persoonsgegevens Pensioenfondsen 2023.
- l Gegevens over gezondheid: Persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een Betrokkene, waaronder het arbeidsongeschiktheidspercentage en gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.
- m Inbreuk: een inbreuk op de beveiliging die per ongeluk en/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 Persoonsgegevens. Dit wordt een datalek genoemd.
- n Ontvanger: eenieder aan wie Persoonsgegevens worden verstrekt.
- o Pensioenfonds: een Pensioenfonds zoals bedoeld in artikel 1 van de Pensioenwet en een beroepspensioenfonds zoals bedoeld in artikel 1 van de Wet verplichte beroepspensioenregeling.
- p Pensioenregister: de website www.mijnpensioenoverzicht.nl, waar iedere burger aan de hand van zijn DigiD, of daarvoor in de plaats komende officiële internet legitimatiestandaard, (een indicatie van) zijn pensioenaanspraken of zijn pensioenrechten kan inzien, alsmede inzicht kan krijgen in de hoogte van het te bereiken pensioen, de keuzes ten aanzien van het pensioen en de gevolgen van deze keuzes en van belangrijke gebeurtenissen op het pensioen.
- q Pensioenuitvoeringsorganisatie: een derde partij die werkzaamheden verricht voor en namens het Pensioenfonds.
- r Pensioenwet: de Pensioenwet en de op deze wet gebaseerde regelingen en besluiten.

- s Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare levende natuurlijke persoon (de Betrokkene) aan de hand van een (online) identificator zoals een naam, een identificatienummer, locatiegegevens, of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
- t Persoonsgegevens van strafrechtelijke aard: persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen als bedoeld in artikel 10 van de verordening, alsmede persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag.
- u Profilering: 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.
- v Privacy by default: de standaardinstellingen van systemen zijn zo ingericht dat deze zo privacy-vriendelijk mogelijk staan. Dat houdt onder meer in dat de persoonsgegevens niet openbaar zichtbaar zijn.
- w Privacy by design: bij het ontwerp van producten en diensten worden privacy waarborgen getroffen zodat de gehanteerde mechanismen en systemen zoveel mogelijk rekening houden met de privacy van de Betrokkene.
- x Pseudonimisering: het verwerken van Persoonsgegevens op een zodanige wijze dat de Persoonsgegevens niet meer aan een specifieke Betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens moeten worden gebruikt, mits deze aanvullende gegevens separaat 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.
- y Stichting Pensioenregister: de rechtspersoon die is aangewezen ter uitvoering van het bepaalde in artikel 51 Pensioenwet, artikel 62 Wet verplichte beroepspensioenregeling en artikel 164a lid 1 Algemene pensioenwet politieke ambtsdragers (Pensioenregister) en die als Verwerker geldt.
- z Toestemming: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de Betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende Verwerking van Persoonsgegevens aanvaardt.

- aa Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de Verwerking van Persoonsgegevens vaststelt.
- bb Verwerker: eenieder die ten behoeve van en in opdracht van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt.
- cc Verwerking: elke bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van Persoonsgegevens.
- dd Wet verplichte beroepspensioenregeling: de Wet verplichte beroepspensioenregeling en de op deze wet gebaseerde regelingen en besluiten.

3

De reikwijdte van de Gedragslijn

3.1 De sector

3.1.1 De Gedragslijn is van toepassing op Pensioenfondsen die lid zijn van de Pensioenfederatie. Pensioenfondsen die geen lid zijn van de Pensioenfederatie kunnen vrijwillig verklaren dat zij zich aansluiten bij deze Gedragslijn en dat zij deze Gedragslijn naleven.

3.1.2 Pensioenfondsen kunnen bij de Verwerking van Persoonsgegevens gebruik maken van een Verwerker. Indien gebruik wordt gemaakt van de diensten van een Verwerker zal met deze Verwerker een (verwerkers)overeenkomst worden gesloten, waarin schriftelijk of in een andere, gelijkwaardige vorm onder meer wordt vastgelegd dat passende technische en organisatorische maatregelen ter beveiliging van die Persoonsgegevens moeten worden genomen. Pensioenfondsen zullen bij uitbesteding van taken aan Verwerkers in de pensioensector naleving van de AVG of naleving van deze Gedragslijn opleggen.

3.2 Toepassing

3.2.1 De Gedragslijn is in de eerste plaats van toepassing op de (gedeeltelijk) geautomatiseerde Verwerking van Persoonsgegevens door een Pensioenfonds in het kader van de pensioenuitvoering. De Gedragslijn is ook van toepassing op de fysieke Verwerking van Persoonsgegevens door een Pensioenfonds in het kader van de pensioenuitvoering, op voorwaarde dat de Persoonsgegevens zijn opgenomen in een Bestand of bestemd zijn om daarin te worden opgenomen.

3.2.2 Verwerkingen van Persoonsgegevens in de hoedanigheid van een Pensioenfonds als werkgever vallen buiten de reikwijdte van deze Gedragslijn.

3.2.3 Het Pensioenfonds legt het doel en de wijze van de Verwerking van Persoonsgegevens vast.

4

Beginnelsen van Verwerking van Persoonsgegevens

4.1

Wet- en regelgeving

4.1.1

Pensioenfondsen verwerken Persoonsgegevens in overeenstemming met geldende wet- en regelgeving. Zij respecteren de beginselen van proportionaliteit, subsidiariteit en vertrouwelijkheid en verwerken Persoonsgegevens op een transparante, behoorlijke en zorgvuldige wijze.

4.1.2

Pensioenfondsen baseren iedere Verwerking van Persoonsgegevens op een in geldende wet- en regelgeving opgenomen grondslag. De Gedragslijn bevat een nadere uitwerking van rechtmatige grondslagen uit wet- en regelgeving voor Verwerkingen van Persoonsgegevens door Pensioenfondsen.

4.2

Doeleinden

4.2.1

Pensioenfondsen verzamelen Persoonsgegevens voor welbepaalde en uitdrukkelijk omschreven doeleinden. De Gedragslijn werkt deze doeleinden verder uit in artikel 6. Daarnaast mogen Pensioenfondsen in overeenstemming met geldende wet- en regelgeving Persoonsgegevens verder verwerken mits dit verenigbaar is met het oorspronkelijke doel waarvoor de Persoonsgegevens zijn verzameld. Dat zijn de doeleinden waarvoor de Persoonsgegevens oorspronkelijk verzameld zijn. Pensioenfondsen omschrijven de doeleinden van Verwerkingen en de bronnen van Persoonsgegevens respectievelijk in het privacy beleid en het verwerkingsregister.

4.2.2

Pensioenfondsen doen uitsluitend Verwerkingen van Persoonsgegevens die toereikend zijn, ter zake dienend en beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ("minimale gegevensverwerking"), en juist zijn en zo nodig worden geactualiseerd of gewist. Zij voeren een beleid ten aanzien van de juistheid van Persoonsgegevens, de bewaartermijnen, het vastleggen van Verwerkingen in een daartoe bestemd verwerkingsregister en de verwijdering van Persoonsgegevens.

4.2.3

Pensioenfondsen geven invulling aan de rechten van de Betrokkene ten aanzien van de Verwerking van Persoonsgegevens. De Gedragslijn werkt de rechten nader uit in artikel 8.

4.2.4

Bijzondere situaties en omstandigheden kunnen de beginselen van Verwerking van Persoonsgegevens beperken. Dit is nader uitgewerkt in artikel 10 van de Gedragslijn.

5

Rechtmatigheid van de Verwerking

5.1 Rechtmatigheid

5.1.1 Elke Verwerking door een Pensioenfonds moet rechtmatig zijn. Om rechtmatig te zijn moet de Verwerking te baseren zijn op tenminste één van de in artikel 5.1.2 vastgelegde rechtsgrondslagen. Het gaat hier om voor een Pensioenfonds relevante en in de AVG vastgelegde rechtsgrondslagen. Of een rechtsgrondslag van toepassing is, hangt onder meer af van het doel dat met de Verwerking wordt beoogd.

5.1.2 De voor een Pensioenfonds relevante rechtsgrondslagen voor een Verwerking zijn:

- a de Betrokkene heeft Toestemming gegeven voor de Verwerking voor een of meer specifieke doeleinden;
- b de Verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de Betrokkene partij is, of om op verzoek van de Betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
- c de Verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op het Pensioenfonds rust (deze wettelijke plicht moet een grondslag hebben in het recht van de Europese Unie dan wel een unierechtelijke lidstaat); of
- d de Verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van het Pensioenfonds of van een Derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de Betrokkene die tot bescherming van de Persoonsgegevens nopen, zwaarder wegen dan die belangen.

5.2 Noodzakelijkheid

5.2.1 Bij de *noodzakelijkheidsgrondslagen* (5.1.2 b – d) maakt het Pensioenfonds de afweging of de Verwerking noodzakelijk en daarmee gerechtvaardigd is voor de in deze grondslagen genoemde doeleinden. Hierbij wordt getoetst of de Verwerking voldoet aan de vereisten van proportionaliteit en subsidiariteit.

- 5.2.2 De vraag of de Verwerking proportioneel is, beoordeelt het Pensioenfonds aan de hand van de criteria van *effectiviteit* en *evenredigheid*. Een Verwerking is effectief als met de Verwerking het gestelde doel kan worden bereikt of als dat zeer waarschijnlijk is.
Een Verwerking is evenredig als het doel dat met de Verwerking wordt nagestreefd in verhouding staat tot het feit dat Persoonsgegevens worden verwerkt.
- 5.2.3 Bij de vraag of de Verwerking subsidiair is, kijkt het Pensioenfonds of de Pensioenuitvoeringsorganisatie het doel niet op een andere, minder ingrijpende wijze kan bereiken.
- 5.2.4 Alleen als de Verwerking niet te baseren valt op een van de *noodzakelijkheidsgrondslagen*, is Toestemming van de Betrokkene voor de gegevensverwerking nodig.

6

Doeleinden voor de Verwerking van Persoonsgegevens

6.1

Inleiding

Bij de Verwerking van Persoonsgegevens baseert het Pensioenfonds zich op doeleinden die gebaseerd zijn op één van de in hoofdstuk 5 vermelde grondslagen.

Het Pensioenfonds legt deze doelstellingen vast in het register van verwerkingen (zie 9.2.3.b) en informeert de Betrokkenen over deze doelstelling (zie 8.2), bijvoorbeeld via de privacyverklaring op de website van het Pensioenfonds.

Pensioenfondsen verwerken uitsluitend Persoonsgegevens waarvoor zij, voordat zij met de Verwerking beginnen, de doeleinden voor Verwerking hebben bepaald. Deze doeleinden zijn welbepaald, uitdrukkelijk omschreven en gerechtvaardigd.

6.2

Persoonsgegevens in het kader van uitvoeren pensioenregeling

Pensioenfondsen verwerken Persoonsgegevens voor het uitvoeren van de pensioenregeling, uitvoeringsreglement dan wel uitvoeringsovereenkomst die zij hiervoor zijn aangegaan.

6.3

Persoonsgegevens in relatie tot historische, statistische en wetenschappelijke doeleinden

6.3.1

Pensioenfondsen kunnen (bijzondere) Persoonsgegevens verwerken voor historische, statistische of wetenschappelijke doeleinden.

6.3.2

Ingeval van verwerking van bijzondere persoonsgegevens dient de Verwerking noodzakelijk te zijn voor het verrichten van een specifieke analyse en te voldoen aan de overige voorwaarden van artikel 7 van de Gedragslijn.

6.4 Persoonsgegevens in het kader van relatiemanagement en Direct Marketing activiteiten

6.4.1 Pensioenfondsen kunnen Persoonsgegevens voor relatiemanagement en marketingactiviteiten verwerken. Bij Verwerking van Persoonsgegevens voor relatiemanagement en marketingdoeleinden die Pensioenfondsen niet direct bij Betrokkene hebben verzameld, informeren zij de Betrokkene. Het versterken van bewustwording en pensioenbewustzijn van de (gewezen) deelnemers, pensioengerechtigden of andere aanspraakgerechtigden valt binnen de wettelijke taak van het Pensioenfonds (zie 6.5.1).

6.4.2 Bij het Verwerken van Persoonsgegevens voor direct marketing doeleinden vragen de Pensioenfondsen uitdrukkelijke toestemming aan de Betrokkene. Het Pensioenfonds beëindigt de Verwerking voor direct marketing activiteiten als de Betrokkene kenbaar maakt dat de hem betreffende Persoonsgegevens hiervoor niet gebruikt mogen worden (zie ook 8.8). Pensioenfondsen houden bij Direct Marketing activiteiten rekening met overige ter zake geldende wet- en regelgeving, zoals artikel 11.7 van de Telecommunicatiewet.

6.5 Persoonsgegevens in verband met wettelijke voorschriften

6.5.1 Pensioenfondsen moeten in bepaalde gevallen Persoonsgegevens van een Betrokkene, verwerken en in bepaalde gevallen verstrekken aan bevoegde autoriteiten op grond van voorschriften uit wet- en regelgeving en van sectortoezichthouders.

6.5.2 Pensioenfondsen dienen Persoonsgegevens aan het Pensioenregister van de Stichting Pensioenregister (www.mijnpensioenoverzicht.nl) te verstrekken conform het wettelijk kader. De gegevensverwerking via deze website vindt plaats op grond van de Pensioenwet en Wet verplichte beroepspensioenregeling. Informatie over de werking van het pensioenregister is te vinden op www.pensioenregister.nl.

6.5.3 Pensioenfondsen verwerken Persoonsgegevens op grond van de Pensioenwet en de Wet verplichte beroepspensioenregeling voor de wettelijk verplichte pensioencommunicatie naar Betrokkenen. Hierbij geeft de wetgever aan dat Pensioenfondsen bij voorkeur vanuit kosten oogpunt zoveel mogelijke elektronisch moeten communiceren. De Pensioenfondsen verwerken daarom de hiervoor benodigde Persoonsgegevens als e-mailadressen en indien noodzakelijk mobiele telefoonnummers.

6.6 Persoonsgegevens in verband met behartiging gerechtvaardigde belangen

Pensioenfondsen kunnen persoonsgegevens in verband met de behartiging van gerechtvaardigd belangen verwerken. Het Pensioenfonds maakt een gedegen belangenafweging met de grondrechten en fundamentele vrijheden van de Betrokkene. Een belangrijke factor hierbij is in hoeverre de Betrokkene redelijkerwijs mag verwachten dat verwerking met dat doel kan plaatsvinden.

6.7 Wijziging van doeleinden voor persoonsgegevens die reeds verwerkt worden

De verdere Verwerking van Persoonsgegevens is alleen geoorloofd als het nieuwe doel verenigd is aan het oorspronkelijke doel van de Verwerking en als de aard van de Persoonsgegevens en de gevolgen voor de Betrokkene zich niet tegen verdere Verwerking verzetten. Pensioenfondsen informeren de Betrokkene ingeval van een nieuwe Verwerking van Persoonsgegevens in overeenstemming met hoofdstuk 9 van de Gedragslijn.

7

Verwerking van Bijzondere categorieën van en overige gevoelige Persoonsgegevens

7.1 Persoonsgegevens betreffende iemands gezondheid

7.1.1 Het is Pensioenfondsen, of instellingen die voor hen werkzaam zijn, toegestaan Persoonsgegevens betreffende iemands gezondheid (Gegevens over gezondheid) te verwerken, voor zover:

- a de Verwerking noodzakelijk is voor een goede uitvoering van wettelijke voorschriften of pensioenregelingen die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van de Betrokkene; of
- b de Betrokkene uitdrukkelijke Toestemming heeft verleend voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden; of
- c dit noodzakelijk is voor historische, statistische of wetenschappelijke doeleinden en het Pensioenfonds passende waarborgen treft ter bescherming van de persoonlijke levenssfeer van de Betrokkene en de voorwaarden en de vereisten uit artikel 24 UAVG heeft getoetst; of
- d dit noodzakelijk is voor de vaststelling, uitoefening of de verdediging bij een rechtsvordering; of
- e naleving van wet- en regelgeving dit vereist.

7.1.2 De Gegevens omtrent iemands gezondheid worden alleen verwerkt door personen die tot geheimhouding zijn verplicht, tenzij de wet hem tot mededeling verplicht.

7.2 Persoonsgegevens van strafrechtelijke aard

7.2.1 Persoonsgegevens van strafrechtelijke aard mogen worden verwerkt door de Verwerkingsverantwoordelijke die deze gegevens ten eigen behoeve verwerkt:

- a ter beoordeling van een verzoek van Betrokkene om een beslissing over hem te nemen of aan hem een prestatie te leveren; of
- b ter bescherming van zijn belangen, voor zover het gaat om strafbare feiten die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd jegens hem of jegens personen die in zijn dienst zijn.

7.2.2 Onverminderd het bepaalde in artikel 7.2.1. van deze Gedragslijn is het een Pensioenfonds toegestaan om Persoonsgegevens van strafrechtelijke aard te verwerken indien de Verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

7.3 Kopie identiteitsbewijs

Het is een Pensioenfonds toegestaan om kopieën van identiteitsbewijzen te verwerken indien dat nodig is ter verificatie van de Betrokkene. Voorafgaand aan de identificatie geeft het Pensioenfonds aan welke Persoonsgegevens nodig zijn voor identificatie van de Betrokkene. In de beoordeling of een kopie identiteitsbewijs moet worden gevraagd moeten de verwerkingsprincipes van proportionaliteit en subsidiariteit meegewogen worden.

7.4 Gegevens van partners en kinderen van een deelnemer

Het is een Pensioenfonds toegestaan om gegevens omtrent (ex-)partners en kinderen te verwerken daar waar dat nodig is voor de uitvoering van het Pensioenreglement.

7.5 Overige bijzondere Persoonsgegevens

Het is een Pensioenfonds niet toegestaan om andere bijzondere Persoonsgegevens te verwerken tenzij er sprake is van een van de uitzonderingen genoemd in artikel 9 AVG.

7.6 Gevoelige Persoonsgegevens

Het is Pensioenfondsen, of instellingen die voor hen werkzaam zijn, toegestaan gevoelige Persoonsgegevens te verwerken, zoals financiële gegevens, voor zover dit noodzakelijk is voor de uitvoering van hun werkzaamheden.

7.7 BSN

Het Pensioenfonds mag het Burgerservicenummer verwerken voor de uitvoering van taken die horen bij de uitvoering van de pensioenwetgeving. In de beoordeling of het Burgerservicenummer verwerkt mag worden, dient ook het verwerkingsbeginsel van minimale gegevensverwerking meegenomen te worden.

8

Rechten van Betrokkene

8.1

Algemene bepalingen

Het Pensioenfonds draagt er zorg voor dat Betrokkene in beginsel kosteloos hun rechten kunnen uitoefenen. Voorafgaand aan de informatieverstrekking kan het Pensioenfonds vragen om te preciseren op welke informatie of welke verwerkingsactiviteit het verzoek betrekking heeft.

Het Pensioenfonds stelt de identiteit van de Betrokkene vast. Indien het onvoldoende duidelijk is dat de Betrokkene het verzoek heeft gedaan vraagt het Pensioenfonds aanvullende informatie op om de identiteit van de Betrokkene vast te stellen.

Het Pensioenfonds reageert binnen een maand inhoudelijk op het door de Betrokkene ingestelde verzoek. De termijn van een maand wordt opgeschort zolang de Betrokkene niet heeft voldaan aan het verzoek tot aanvullende informatie.

Indien het Pensioenfonds niet in staat is naar zekerheid de identiteit van Betrokkene vast te stellen, neemt het Pensioenfonds het verzoek niet in behandeling en wijst op de mogelijkheid om bij de AP of de rechter een klacht in te dienen.

Het Pensioenfonds heeft de mogelijkheid om de termijn van een verzoek door Betrokkene met 2 maanden te verlengen. Indien er sprake is van i) een complex verzoek of ii) een grote hoeveelheid verzoeken. Het Pensioenfonds bericht de Betrokkene daarover uiterlijk binnen een maand met redenen omkleed.

Indien het Pensioenfonds van mening is dat een verzoek kennelijk ongegrond is of buitensporig van aard, mag het Pensioenfonds weigeren het verzoek in behandeling te nemen. Het Pensioenfonds zal Betrokkene hierover schriftelijk informeren met toelichting op het besluit en de mogelijkheid voor Betrokkene om een klacht bij de AP in te dienen of beroep bij de rechter in te stellen.

Het Pensioenfonds stelt partijen met wie de Persoonsgegevens gedeeld zijn en die worden gerectificeerd, gewist of beperkt, op de hoogte van de wijzigingen binnen redelijke termijn. Dit informeren blijft achterwege wanneer:

- dit onmogelijk blijkt; of
- een onevenredige inspanning vergt.

8.2 Informatieplicht

- 8.2.1 Het Pensioenfonds informeert de Betrokkene over de Verwerking van Persoonsgegevens op een transparante wijze en in begrijpelijke taal, zodat de Betrokkene de Verwerking kan beoordelen en zijn rechten afdoende kan uitoefenen.
- 8.2.2 Indien de Persoonsgegevens worden opgevraagd bij de Betrokkene zelf wordt de Betrokkene bij de verkrijging van de persoonsgegevens geïnformeerd over de verwerkingsdoeleinden, de rechtsgrond, wie de Ontvangers zijn of sprake is van doorgifte van persoonsgegevens alsmede de contactgegevens van de Functionaris Gegevensbescherming.
- 8.2.3 Indien Persoonsgegevens worden verkregen van een derde dan informeert het Pensioenfonds de Betrokkene binnen een redelijke termijn die afhangt van de omstandigheden van het geval. Na verkrijging van de persoonsgegevens of indien mogelijk voorafgaand in de privacyverklaring op de website van het Pensioenfonds en informeert over de in 8.2.2 genoemde zaken.
- 8.2.4 De informatieplicht is niet van toepassing als de Betrokkene reeds geïnformeerd is, het informeren in de praktijk onmogelijk is of onevenredige inspanningen vergt. In dat geval zorgt het Pensioenfonds voor passende maatregelen waaronder het openbaar maken van de informatie.

8.3 Inzage

De Betrokkene is gerechtigd om het Pensioenfonds schriftelijk te vragen om een overzicht van de verwerkte Persoonsgegevens. Indien van toepassing zal het Pensioenfonds een overzicht van de Persoonsgegevens verstrekken aan de Betrokkene. Als het Pensioenfonds geen Persoonsgegevens van de Betrokkene verwerkt, stelt het Pensioenfonds de Betrokkene daarvan op de hoogte.

Het Pensioenfonds verstrekt informatie aan de Betrokkene over welke Persoonsgegevens verwerkt worden. Het Pensioenfonds mag voorafgaand aan de informatieverstrekking vragen om te preciseren op welke informatie of welke verwerkingsactiviteit het verzoek betrekking heeft.

Als het Pensioenfonds gebruik maakt van Persoonsgegevens in een deelnemersportaal, kan het Pensioenfonds Betrokkene verwijzen naar de plaatsen op het portaal waar Betrokkene de verwerkte Persoonsgegevens kan terugvinden. Tevens zal het Pensioenfonds aangeven of er nog op andere plaatsen Persoonsgegevens worden verwerkt en welk soort gegevens het betreft. Indien Betrokkene alsnog inzage wil hebben in de betreffende gegevens, heeft het Pensioenfonds de verplichting deze gegevens te leveren. Hierbij wordt rekening gehouden met hetgeen in artikel 8.1 is bepaald.¹

¹ Eventuele wijzigingen en/of aanvullingen op basis van de Richtlijnen over Inzage opgesteld door de Europese toezichthouder (EDPB), zullen gepubliceerd worden op de website van de Pensioenfederatie.

8.4 Correctie

Indien een Betrokkene een terecht beroep doet op het recht op correctie zal het Pensioenfonds deze Persoonsgegevens onverwijld corrigeren en de Betrokkene hiervan op de hoogte stellen.

8.5 Gegevenswissing ("recht op vergetelheid")

8.5.1 Persoonsgegevens worden door een Pensioenfonds gewist wanneer:

- i de Persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
- ii de Betrokkene zijn Toestemming intrekt waarop de Verwerking berust en er geen andere rechtsgrond is voor de Verwerking;
- iii de Betrokkene bezwaar maakt tegen de gegevensverwerking en dit bezwaar gegrond is verklaard op grond van de klachten- en de geschillenregeling en mits dit niet ingaat tegen de eerder genoemde noodzaak tot verwerking in het kader van de uitvoering van het uitvoeringsreglement;
- iv de Persoonsgegevens onrechtmatig zijn verwerkt; en
- v dient te worden voldaan aan een in het Unierecht of lidstatelijke recht neergelegde wettelijke verplichting die op het Pensioenfonds rust.

8.5.2 Het Pensioenfonds is niet verplicht de Persoonsgegevens te wissen wanneer de Verwerking nodig is voor:

- i het nakomen van een in een het Unierecht of het lidstatelijke recht neergelegde wettelijke verwerkingsverplichting die op het Pensioenfonds rust;
- ii (het voorkomen van) de instelling, uitoefening of onderbouwing van een rechtsvordering;
- iii met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden; of
- iv uitvoering te geven aan een overeenkomst.

8.5.3 Het Pensioenfonds draagt er zorg voor dat de betreffende Persoonsgegevens uit de administratie worden verwijderd. Indien verwijdering technisch niet mogelijk is of slechts tegen hoge kosten schermt het Pensioenfonds de gegevens afdoende af.

8.6 Beperking van de Verwerking

De Betrokkene heeft het recht om van het Pensioenfonds de beperking van de Verwerking te verkrijgen indien:

- i de juistheid van de Persoonsgegevens wordt betwist door de Betrokkene, gedurende een periode die het Pensioenfonds in staat stelt de juistheid van de Persoonsgegevens te controleren;
- ii de verwerking onrechtmatig is en de Betrokkene zich verzet tegen het wissen van Persoonsgegevens en in de plaats daarvan om beperking van het gebruik ervan verzoekt;
- iii het Pensioenfonds de Persoonsgegevens niet meer nodig heeft voor de verwerkingsdoeleinden, maar de Betrokkene deze nodig heeft voor de instelling of onderbouwing van een rechtsvordering; of
- iv de Betrokkene bezwaar heeft gemaakt tegen de verwerking en in afwachting is van het antwoord op de vraag of de gerechtvaardigde gronden van het Pensioenfonds zwaarder wegen dan die van de Betrokkene.

8.7 Overdraagbaarheid van Persoonsgegevens

8.7.1 De Betrokkene heeft het recht de hem betreffende Persoonsgegevens die hij aan het Pensioenfonds heeft verstrekt, in een gestructureerde, gangbare en machine leesbare vorm te verkrijgen, en hij heeft het recht die gegevens aan een andere Verwerkingsverantwoordelijke over te dragen, zonder dat hij daarbij wordt gehinderd door het Pensioenfonds, indien (i) de verwerking berust op toestemming, (ii) op een overeenkomst en (iii) de verwerking geschiedt geautomatiseerd.

8.7.2 Het Pensioenfonds draagt er zorg voor dat, indien dit technisch mogelijk is, de gegevens rechtstreeks naar de andere Verwerkingsverantwoordelijke worden doorgezonden.

8.8 Bezwaar

Wanneer het Pensioenfonds Persoonsgegevens verwerkt op grond van het gerechtvaardigd belang, heeft de Betrokkene te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende Persoonsgegevens.

8.9 Geautomatiseerde besluitvorming, waaronder profilering

8.9.1 De Betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft, tenzij dit besluit:

- i noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de Betrokkene en het Pensioenfonds;
- ii is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de Betrokkene;
- iii berust op de uitdrukkelijke Toestemming van de Betrokkene.

8.9.2 Geautomatiseerde besluiten worden niet gebaseerd op de in artikel 9 lid 1 AVG bedoelde bijzondere categorieën van Persoonsgegevens, tenzij artikel 9 lid 2 sub a of g AVG van toepassing is en er passende maatregelen ter bescherming van de gerechtvaardigde belangen van de Betrokkene zijn getroffen.

9

Overige onderwerpen

9.1 Privacy by default en by design

9.1.1 Privacy by default

Het Pensioenfonds richt de standaardinstellingen van systemen in volgens het principe van Privacy by default (artikel 25 AVG) zodat deze zo privacy-vriendelijk mogelijk staan, dat betekent onder andere dat de persoonsgegevens niet openbaar zichtbaar zijn.

9.1.2 Privacy by design

Het Pensioenfonds treft bij het ontwerp van producten en diensten privacy waarborgen zodat de gehanteerde mechanismen en systemen zoveel mogelijk rekening houden met de privacy van de Betrokkenen volgens het principe Privacy by design (artikel 25 AVG). De aandacht voor privacy blijft tijdens de gehele levensduur van het systeem bestaan en gedurende de periode dat de Betrokkene rechten kan ontleen aan de pensioenovereenkomst. Onderdeel hiervan is het minimaliseren van gegevens van Betrokkene (alleen de gegevens verwerken die nodig zijn voor de pensioenuitvoering) en het goed beveiligen van de gegevens.

9.2 Verwerkersovereenkomst

9.2.1 Wanneer een verwerking namens een Verwerkingsverantwoordelijke wordt verricht, doet de Verwerkingsverantwoordelijke uitsluitend een beroep op een verwerker die afdoende garanties biedt met het toepassen van passende technische en organisatorische maatregelen.

9.2.2 De Verwerking door een verwerker wordt geregeld in een (verwerkers)overeenkomst. Daarin worden de vereisten genoemd in artikel 28, lid 3, AVG uitgewerkt.

9.2.3 Wanneer de verwerker een andere verwerker (subverwerker) contracteert om voor rekening van de verwerkingsverantwoordelijke een verwerkingsactiviteit te verrichten, worden aan deze andere verwerker dezelfde verplichtingen opgelegd die door de verwerkingsverantwoordelijke zijn opgelegd aan de eerste verwerker.

9.2.4 Bij niet nakomen van verplichtingen door de andere verwerker, blijft de eerste verwerker verantwoordelijk voor het nakomen van de verplichtingen van die andere verwerker.

9.2.5 Samenwerking tussen Pensioenfondsen en dienstverleners.
Uitbesteding door het Pensioenfonds aan opdrachtnemers/dienstverleners vindt plaats op basis van een verwerkersovereenkomst indien er in het kader van de uitbesteding sprake is van verwerking van Persoonsgegevens. Het Pensioenfonds bepaalt of een Verwerkersovereenkomst nodig is.

9.2.6 Contractuele afspraken tussen Verwerkingsverantwoordelijken.
Indien er sprake is van meerdere verwerkingsverantwoordelijken dienen Partijen conform het bepaald in artikel 26 AVG hun verantwoordelijkheden voortvloeiende uit de AVG vast te leggen.

De vorm waarin deze afspraken worden vastgelegd is niet in de AVG geregeld. De afspraken kunnen worden vastgelegd in bijvoorbeeld een Service Level Agreement (SLA) of een overeenkomst van opdracht.

9.3 Register van verwerkingen

9.3.1 De Verwerkingsverantwoordelijke(n) en, in voorkomend geval, de vertegenwoordiger van de Verwerkingsverantwoordelijke houdt een schriftelijk register bij, ook verwerkingsregister genoemd, bij voorkeur in elektronische vorm, van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden.

9.3.2 Dat register bevat de volgende gegevens:

- a de naam en de contactgegevens van de Verwerkingsverantwoordelijke en de eventuele gezamenlijke Verwerkingsverantwoordelijken, en, in voorkomend geval, van de vertegenwoordiger van de Verwerkingsverantwoordelijke en van de FG;
- b. de verwerkingsdoeleinden;
- c. een beschrijving van de categorieën van Betrokkene en van de categorieën van Persoonsgegevens;
- d. de categorieën van Ontvangers aan wie de Persoonsgegevens zijn of zullen worden verstrekt, onder meer Ontvangers in derde landen of internationale organisaties;
- e. 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, de documenten inzake de passende waarborgen;
- f. indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist; en
- g. indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

9.3.3 Het register van Verwerkingen moet ter beschikking worden gesteld aan de AP indien hier om wordt verzocht.

9.4 Beleid bewaartermijnen

Pensioenfondsen voeren een beleid ten aanzien van het bewaren van Persoonsgegevens. Zij bewaren Persoonsgegevens voor specifieke doeleinden en totdat de in het bewaarbeleid vastgestelde bewaartermijnen zijn verstreken. Na het verstrijken van de bewaartermijn zullen Pensioenfondsen de Persoonsgegevens vernietigen, anonimiseren, pseudonimiseren of overbrengen naar een bestemming ten behoeve van archiefbeheer en ter waarborging van geschillenbeslechting. Pensioenfondsen kunnen gearchiveerde Persoonsgegevens analyseren voor het verrichten van historische, statistische of wetenschappelijke analyse. Wat betreft bewaartermijnen wordt aangesloten bij het eerder uitgebrachte servicedocument van de Pensioenfederatie.²

² Het servicedocument bewaartermijnen is beschikbaar voor leden van de Pensioenfederatie.

9.5 Beveiliging Verwerking

9.5.1 Algemeen

Bij het Verwerken van Gegevens dienen door de verwerkingsverantwoordelijke of de verwerker passende technische en organisatorische maatregelen getroffen te zijn opdat de persoonsgegevens beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

9.5.2 Beveiliging van Persoonsgegevens

Het beveiligen van Persoonsgegevens heeft betrekking op i) de persoonsgegevens die worden verzameld, verwerkt en verwijderd, ii) de systemen waarin de persoonsgegevens worden verwerkt en iii) de medewerkers die toegang hebben tot de persoonsgegevens.

9.5.3 Cameratoezicht

Het gebruik van cameratoezicht op basis van eigen beleid vindt met name plaats met het oog op:

- de beveiliging van gebouwen, terreinen, medewerkers, goederen, informatie en andere gerechtvaardigde belangen;
- het voorkomen, vaststellen en onderzoeken van strafbare feiten en overtredingen van bedrijfsregels;
- het voeren van juridische procedures en slechts voor zover dat voor het doel onvermijdelijk is.

9.5.4 Telefoon- en chatgesprekken

Het vastleggen van telefoon- en chatgesprekken waarin persoonskenmerken voorkomen gebeurt op een zorgvuldige wijze.

9.5.5 Vastlegging elektronische communicatie
Ook voor de overige vormen van elektronische communicatie, zoals e-mail verkeer, zullen regels ten aanzien van zorgvuldigheid en beveiliging gelden, die zijn opgenomen in het eigen beleid.

9.6 Datalekken

9.6.1 Datalekken

De Verwerkingsverantwoordelijke registreert en beoordeelt elk datalek (inbreuk op de beveiliging van Persoonsgegevens). Daarbij wordt tenminste vastgelegd:

- de aard van het datalek met vermelding van de categorieën van Betrokkenen en van Persoonsgegevens alsook het aantal Betrokkenen en persoonsgegevenregisters;
- de naam en contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt;
- de waarschijnlijke gevolgen van het datalek;
- de te nemen of getroffen maatregelen om de eventuele nadelige gevolgen van het datalek te beperken of op te heffen.

9.6.2 Melden datalekken aan AP

Tenzij het niet waarschijnlijk is dat het datalek een risico voor Betrokkenen inhoudt, meldt de Verwerkingsverantwoordelijke zonder onredelijke vertraging en, indien mogelijk, uiterlijk binnen 72 uur na het ontdekken van het datalek door de Verwerkingsverantwoordelijke, aan de AP.

Indien het datalek foutieve postverzending betreft, d.w.z.:

- een poststuk dat geopend retour ontvangen wordt;
- een poststuk dat bij de verkeerde Ontvanger aankomt; of
- een poststuk dat niet aankomt,

mogen deze datalekken in bulk en uiterlijk op de overeenkomstige dag van de eerstvolgende maand na de dag van ontdekking door de Verwerkingsverantwoordelijke aan de AP gemeld worden.

9.6.3 Melding door (sub)Verwerker

De Verwerker informeert de Verwerkingsverantwoordelijke zo snel mogelijk nadat hij een datalek ontdekt heeft bij de Gegevensverwerking voor de Verwerkingsverantwoordelijke, dit datalek bij de Verwerkingsverantwoordelijke. Hierover worden afspraken vastgelegd in de verwerkersovereenkomst, de dienstverleningsovereenkomst of de SLA.

Indien de Verwerker voor de gegevensverwerking voor de Verwerkingsverantwoordelijke gebruik maakt van een subverwerker meldt de subverwerker een bij hem plaatsgevonden hebbend datalek zo snel mogelijk bij de Verwerker die het datalek dan weer op zijn beurt meldt bij de Verwerkingsverantwoordelijke. De afspraken tussen de Verwerker en de subverwerker worden vastgelegd in een verwerkersovereenkomst.

9.6.4 Melden datalek aan Betrokkene

Indien een datalek gemeld wordt aan de AP, wordt indien het datalek waarschijnlijk een hoog risico voor de Betrokkene inhoudt, ook gemeld aan de Betrokkene.

Betrokkene wordt in ieder geval over volgende geïnformeerd:

- de aard van het datalek;
- de naam en contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt;
- de waarschijnlijke gevolgen van het datalek;
- de te nemen of getroffen maatregelen om de eventuele nadelige gevolgen van het datalek te beperken of op te heffen.

Melden aan de Betrokkene kan achterwege blijven indien:

- er vooraf dan wel achteraf maatregelen genomen zijn die het risico voor Betrokkene mitigeren, met name het versleutelen van de persoonsgegevens;
- er onevenredige inspanningen gemoeid zijn met zo'n melding en met een openbare mededeling kan worden volstaan.

9.7 (Data) Protection Impact Assessment/ Gegevensbeschermingseffectbeoordeling

9.7.1 Uitvoeren DPIA's

Pensioenfondsen moeten een DPIA (laten) uitvoeren indien sprake is van een Verwerking dat een hoog risico inhoudt voor de rechten en vrijheden van Betrokkenen. In dat geval mag de voorgenomen Verwerking pas plaatsvinden als de DPIA is uitgevoerd, inclusief een inschatting van de risico's voor Betrokkenen en de te treffen beheersmaatregelen.

9.7.2 Indien voor een verwerkingsactiviteit een nieuwe technologie wordt toegepast en er waarschijnlijk sprake is van een hoog risico voor de rechten en vrijheden van natuurlijke personen, dient een DPIA uitgevoerd te worden. Indien er al een DPIA is uitgevoerd, dient deze geactualiseerd te worden waarin een nieuwe afweging is gemaakt over het risico.

9.7.3 De DPIA wordt om de 3 jaar geactualiseerd. De termijn van herijking is neergelegd in het privacy beleid.

9.8 Functionaris

9.8.1 Aanwijzing van een Functionaris

³ In de Guidance van de PF is onder paragraaf 11 overwegingen en scenario's opgenomen op grond waarvan het Pensioenfonds of de Pensioenuitvoeringsorganisatie kunnen bepalen of zij al dan niet een FG zullen aanwijzen.

Het Pensioenfonds of de Pensioenuitvoeringsorganisatie vallen niet onder de in artikel 37, eerste lid, van de AVG opgenomen verplichting tot het aanwijzen van een FG.

Wel kan het voor het Pensioenfonds of de Pensioenuitvoeringsorganisatie zinvol zijn om vrijwillig een FG aan te wijzen.³

Als een FG is aangewezen, wordt deze functionaris aangemeld bij de AP en worden zijn contactgegevens gepubliceerd op de website.

9.8.1.1 Vanuit elke vestiging makkelijk te contacteren

Het Pensioenfonds of de Pensioenuitvoeringsorganisatie die als concern uit meerdere (bedrijfs)onderdelen bestaan, mogen een gezamenlijke FG aanwijzen, mits deze vanuit elke vestiging makkelijk te contacteren is. Om ervoor te zorgen dat de FG bereikbaar is, is het belangrijk dat diens contactgegevens beschikbaar zijn voor zowel de Betrokkenen als de toezichthouder.⁴

9.8.1.2 Deskundigheid en vaardigheden van de FG

De FG wordt aangewezen op grond van zijn professionele kwaliteiten, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen zijn taken te vervullen.

9.8.1.3 Publicatie en communicatie van de contactgegevens van de FG

Het Pensioenfonds of de Pensioenuitvoeringsorganisatie zijn verplicht de contactgegevens van de FG:

- te publiceren; en
- aan de relevante toezichthouder te communiceren
- de contactgegevens van de FG dienen informatie te bevatten die personen en toezichthouder in staat stellen de FG gemakkelijk te bereiken (postadres, speciaal telefoonnummer en/of een speciaal e-mailadres of contactformulier; de persoonlijke naam is tenzij voor de bekendheid binnen het Pensioenfonds of de Pensioenuitvoeringsorganisatie niet noodzakelijk).

9.8.2 Positie FG

9.8.2.1 Betrokkenheid van de FG bij alle aangelegenheden die de bescherming van Persoonsgegevens betreffen

Het is van cruciaal belang dat de FG zo vroeg mogelijk betrokken wordt bij alle aangelegenheden die de bescherming van Persoonsgegevens betreffen. Wat betreft DPIA's zijn het Pensioenfonds of de Pensioenuitvoeringsorganisatie verplicht bij het uitvoeren van deze assessments het advies van de FG in te winnen. De FG dient toe te zien op de uitvoering van de assessments. Daarnaast is het belangrijk dat de FG als gesprekspartner voor privacy vraagstukken binnen de organisatie wordt gezien.

⁴ In de Guidance van de PF is onder het kopje 'Algemeen' in paragraaf 11 de mogelijkheid genoemd dat in de verwerkersovereenkomst bepaald kan worden dat de FG van het Pensioenfonds ook als FG van de Pensioenuitvoeringsorganisatie op kan treden. Zaak is dan wel om contractueel goed te borgen dat de FG niet in een situatie van een belangenconflict tussen Pensioenfonds en Pensioenuitvoeringsorganisatie terecht kan komen.

- 9.8.2.2 Benodigde middelen**
Het Pensioenfonds of de Pensioenuitvoeringsorganisatie ondersteunen de FG door hem toegang te verschaffen tot Persoonsgegevens en Verwerkingen en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van deze taken en het in stand houden van zijn deskundigheid.
- 9.8.2.3 Onafhankelijk handelen**
Het Pensioenfonds of de Pensioenuitvoeringsorganisatie dienen er voor te zorgen dat de FG zijn taken met voldoende autonomie kan uitvoeren.
- 9.8.2.4 Ontslag of sancties voor het uitvoeren van FG-taken**
Een FG mag niet ontslagen of gestraft worden voor het te goeder trouw uitvoeren van zijn taken.
Als het Pensioenfonds of de Pensioenuitvoeringsorganisatie het niet eens is met de wijze waarop de FG uitvoering geeft aan zijn (wettelijke) taken, terwijl de FG zijn functie uitvoert op een wijze die in overeenstemming is met deze (wettelijke) taken, mag het Pensioenfonds of de Pensioenuitvoeringsorganisatie de FG niet bestraffen of ontslaan uitsluitend op de uitvoering van diens taken. Dit artikel waarborgt dat de FG zijn taken met autonomie kan uitvoeren.
- 9.8.2.5 Belangenconflicten**
Een FG mag andere taken en plichten vervullen, mits deze taken of plichten niet tot een belangenconflict leiden. De positie van de FG, bijvoorbeeld in de 2e lijn, is afhankelijk van de gekozen organisatiestructuur.
- 9.8.3 Taken van de FG**
- 9.8.3.1 Toezicht op naleving van de AVG**
De FG dient erop toe te zien dat de AVG nageleefd wordt. Daartoe kan de FG:
- informatie verzamelen om verwerkingswerkzaamheden te identificeren;
 - analyseren en controleren in hoeverre verwerkingswerkzaamheden aan de AVG voldoen; en
 - het Pensioenfonds of de Pensioenuitvoeringsorganisatie informeren, adviseren of aanbevelingen geven.
- 9.8.3.2 Risico gebaseerde benadering**
De FG dient bij de uitvoering van zijn taken rekening te houden met het aan verwerkingen verbonden risico en met de aard, de omvang, de context en de verwerkingsdoeleinden.
- 9.8.3.3 De rol van de FG in het voeren van een administratie**
Niet de FG, maar het Pensioenfonds of de Pensioenuitvoeringsorganisatie zijn verplicht een register van (alle categorieën van) de verwerkingsactiviteiten bij te houden.

9.9

Doorgifte Persoonsgegevens

De AVG stelt strikte regels aan het laten Verwerken van Persoonsgegevens buiten de Europese Economische Ruimte (EER). Voor landen binnen de Europese Economische Ruimte (EER, d.w.z. de EU plus Liechtenstein, Noorwegen en IJsland) geldt de AVG. Als een Pensioenfonds echter de Persoonsgegevens in een land buiten de EER laat verwerken, een zogenaamd derde land, dan gelden er striktere regels. Uitgangspunt bij het Verwerken van Persoonsgegevens buiten de EER is dat het land waar de Persoonsgegevens aan worden verstrekt beschikt over een passend beschermingsniveau. Dit houdt in dat het betreffende land minimaal dezelfde waarborgen moet bieden die de AVG biedt.

9.9.1

Doorgifte van Persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER)

De doorgifte van Persoonsgegevens buiten de EER, en daarmee aan een 'derde land', is slechts toegestaan in de volgende gevallen:

- doorgifte op basis van een adequaatheidsbesluit;
- doorgifte op basis van passende waarborgen;
- doorgifte in afwijkende situaties.

9.9.1.1

Doorgifte op basis van een adequaatheidsbesluit

Doorgifte naar derde landen is mogelijk indien de Europese Commissie hiervoor een adequaatheidsbesluit heeft genomen conform artikel 45 AVG. Met een dergelijk besluit geeft de Europese Commissie aan dat een derde land over een passend beschermingsniveau beschikt en dat doorgifte van Persoonsgegevens is toegestaan als wordt voldaan aan de algemene eisen uit de AVG.

9.9.1.2

Doorgifte op basis van passende waarborgen

Doorgifte naar een derde land dat niet beschikt over een adequaatheidsbesluit is alleen mogelijk indien er sprake is van het hebben afgesproken van passende waarborgen en Betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken. Deze waarborgen zijn in art. 46 AVG beschreven. In de volgende gevallen is sprake van 'passende waarborgen'⁵:

⁵ https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_nl

- 1 In het geval van een concern of groep van ondernemingen die een gezamenlijke economische activiteit beoefenen, dan mogen Persoonsgegevens overgedragen worden op basis van zogeheten "bindende bedrijfsvoorschriften" ofwel "binding corporate rules" (BCR) welke in overeenstemming dienen te zijn met de AVG. Hiervan kan enkel gebruik worden gemaakt indien de BCR door de Europese privacytoezichthouders en de European Data Protection Board (EDPB) zijn goedgekeurd.
- 2 Het tussen het Pensioenfonds en de ontvangende partij in een derde land overeenkomen van een modelcontract ofwel 'standard contractual clauses' (SSC's) dat door de Europese Commissie is vastgesteld. Op deze wijze is de contractspartij in het derde land verplicht aan een passend beschermingsniveau conform de AVG te voldoen. Indien partijen een eigen contract wensen overeen te komen is dit uitsluitend na toestemming van de AP geldig.

- 3 Het aansluiten van het Pensioenfonds bij een Gedragscode of certificeringsmechanisme, samen met het verkrijgen van een bindende en afdwingbare toezeggingen van de Ontvanger in het derde land om passende waarborgen toe te passen om de overgedragen Persoonsgegevens te beschermen.

9.9.1.3

Doorgifte in afwijkende situaties

Indien een land buiten de EER niet beschikt over een adequaatheidsbesluit en er is ook geen sprake van passende waarborgen kunnen Persoonsgegevens door een Pensioenfonds mogelijk onder één van de volgende voorwaarden verstrekt worden:

- het Pensioenfonds heeft de uitdrukkelijke Toestemming van de Betrokkene gekregen, waarbij de Betrokkene van tevoren duidelijk is geïnformeerd over eventuele met de Verwerking samenhangende risico's;
- de doorgifte is noodzakelijk voor de uitvoering van een overeenkomst tussen Betrokkene en het Pensioenfonds of voor de uitvoering van op verzoek van Betrokkene genomen precontractuele maatregelen;
- de doorgifte is noodzakelijk voor de sluiting of de uitvoering van een in het belang van Betrokkene tussen Pensioenfondsen een ander natuurlijke of rechtspersoon gesloten overeenkomst;
- de doorgifte is noodzakelijk wegens gewichtige redenen van algemeen belang;
- de doorgifte is noodzakelijke voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- de doorgifte is van vitaal belang voor de Betrokkene of andere personen indien de Betrokkene lichamelijk of juridisch niet in staat is zijn toestemming te geven;
- de doorgifte heeft toestemming van de AP verkregen; of
- de doorgifte naar een land buiten de EER berust op een wettelijke verplichting zoals vanuit een bij wet ingesteld register dat is bedoeld om het publiek voor te lichten.

Indien de doorgifte van Persoonsgegevens niet onder een van de voornoemde afwijkende situaties valt, mogen Persoonsgegevens toch worden doorgegeven aan een derde land als:

- de doorgifte niet repetitief is;
- de doorgifte een beperkt aantal Betrokkenen betreft;
- de doorgifte noodzakelijk is voor dwingende, gerechtvaardigde belangen, die niet ondergeschikt zijn aan de belangen of rechten en vrijheden van de Betrokkenen;
- na beoordeling van alle omstandigheden en op basis daarvan passende waarborgen heeft geboden voor de bescherming van persoonsgegevens.

Elke doorgifte waarbij geen beroep kan worden gedaan op een van de voornoemde mogelijkheden is onrechtmatig en dus niet toegestaan. De AP houdt hierop toezicht.

9.9.2

Gegevensverkeer met landen binnen de Europese Economische Ruimte (EER)

Verwerkingen die binnen de EER plaatsvinden dienen te voldoen aan de vereisten die de AVG stelt. Indien de Verwerking door een derde partij binnen de EER wordt uitgevoerd, die aangemerkt kan worden als Verwerker, dan gelden de bepalingen uit in art. 28 AVG. Indien het Pensioenfonds zelf de Verwerkingen in een land binnen de EER uitvoert dan gelden de bepalingen uit art. 24 AVG.

10

Beperkingen

Het Pensioenfonds kan de uitvoering ten aanzien van verplichtingen en rechten van Betrokkenen en van de beginselen van Verwerking van Persoonsgegevens beperken conform de AVG alleen in geval van:

- a het voorkomen, opsporen, onderzoeken en vervolgen van strafbare feiten of de tenuitvoerlegging van straffen waaronder inbegrepen de bescherming tegen en het voorkomen van gevaren voor de openbare veiligheid of
- b het beschermen en verdedigen van de rechten en vrijheden, met name:
 - i de veiligheid van personen, Pensioenfondsen en Pensioenuitvoeringsorganisaties, de sector alsook de nationale veiligheid;
 - ii de continuïteit en integriteit van de dienstverlening van Pensioenfondsen en Pensioenuitvoeringsorganisaties alsmede de sector;
 - iii de inning van civielrechtelijke vorderingen, bv. bij pensioenbeslag.

11

Naleving van de Gedragslijn

11.1

Maatregelen

Het Pensioenfonds verantwoordt zich over de naleving van de Gedragslijn.

11.2

Verantwoording

De verantwoording over de naleving van de Gedragslijn volgt de naleving van de overige wet- en regelgeving. Dit betreft de verantwoording door het bestuur van het Pensioenfonds. Het Pensioenfonds verantwoordt jaarlijks over de mate waarin zij zich heeft gehouden aan deze Gedragslijn, waarbij het Pensioenfonds besluit/bepaalt op welke wijze zij zich hierover verantwoordt en in welke mate hierover verantwoording wordt afgelegd in het bestuursverslag. Het gaat hierbij over het beoordelen van de mate waarin de belangrijkste risico's worden beheerst.

12

Geschillen

- 12.1 Het Pensioenfonds heeft een interne klachten- en geschillenprocedure in lijn met de Code Pensioenfondsen. Betrokkenen kunnen conform de klachten- en geschillenregeling een klacht indienen over het handelen van een Pensioenfonds bij een mogelijke strijdigheid met deze Gedragslijn of geldende wet- en regelgeving.
- 12.2 Als een Betrokkene de interne klachten- en geschillenprocedure heeft doorlopen en zich op het standpunt stelt dat het Pensioenfonds de klacht ontoereikend heeft behandeld, kan de Betrokkene zich rechtstreeks wenden tot de AP of de bevoegde rechter.

Toelichting en bijlage

3 De reikwijdte van de Gedragslijn

3.1.2 De sector

Het Pensioenfonds is met betrekking tot de Verwerking van Persoonsgegevens voor de uitvoering van de pensioenregeling Verwerkingsverantwoordelijke. De werkgever bepaalt of en welke pensioenregeling hij de werknemers aanbiedt en is verplicht om dit buiten de eigen onderneming onder te brengen. De werkgever is met betrekking tot de Verwerking van Persoonsgegevens voor de uitvoering van de arbeidsvoorwaarde pensioen Verwerkingsverantwoordelijke. Er hoeft geen verwerkersovereenkomst te worden gesloten tussen de werkgever en het Pensioenfonds voor het verstrekken van data voor de uitvoering van de pensioenregeling.

Bij een verplichtgesteld pensioenfonds (bedrijfstak- of beroepspensioenfonds) worden afspraken opgenomen over de Verwerking van de Persoonsgegevens in (aanvulling op) het uitvoeringsreglement. Bij een ondernemingspensioenfonds, een vrijwillig bedrijfstakpensioenfonds of een algemeen pensioenfonds kunnen afspraken worden gemaakt over de verwerking van de Persoonsgegevens in (aanvulling op) de uitvoeringsovereenkomst.

Pensioenfondsen zullen bij uitbesteding van taken aan Verwerkers vastleggen dat deze Gedragslijn wordt toegepast. Indien dit niet mogelijk is, dan zal de naleving van de AVG worden opgelegd aan de Verwerkers. Dit gebeurt bij voorkeur in een onderlinge overeenkomst, zoals een verwerkersovereenkomst maar kan ook op een andere wijze worden vormgegeven. Als de Gedragslijn van kracht wordt, wordt dit toegepast bij de eerstvolgende herziening van de (verwerkers)overeenkomst.

3.2.2 Toepassing

In de hoedanigheid van een Pensioenfonds verwerkt een Pensioenfonds Persoonsgegevens van natuurlijke personen. Voor het uitvoeren van een pensioenregeling zijn veel Persoonsgegevens nodig van een redelijk tot groot aantal natuurlijke personen. Om deze reden dient een Pensioenfonds in de bedrijfsvoering zorgvuldig en vertrouwelijk om te gaan met de Persoonsgegevens van de Betrokkenen. Onder Betrokkenen in de zin van deze Gedragslijn wordt verstaan: (gewezen) deelnemers, pensioengerechtigden, andere aanspraakgerechtigden (zoals ex-partners met aanspraak op bijzonder partnerpensioen en nabestaanden) en werkgevers. Daarnaast verwerkt het Pensioenfonds ook Persoonsgegevens van bijvoorbeeld medewerkers van het Pensioenfonds. De verwerking van deze Persoonsgegevens verricht het Pensioenfonds in de hoedanigheid van een werkgever. Deze Verwerking verschilt van de Verwerking van de Persoonsgegevens in het kader van de uitvoering van de pensioenregeling en valt daarom buiten de scope van deze gedragslijn. Uiteraard gelden hiervoor ook de vereisten van de AVG.

4 Beginselen verwerking van Persoonsgegevens

4.2.1

Pensioenfondsen moeten in een privacybeleid onder meer vastleggen met welk doel zij Persoonsgegevens verwerken, hoe lang ze de gegevens bewaren en hoe de gegevens beveiligd worden. Met een privacybeleid brengt een Pensioenfonds in beeld welke maatregelen het heeft genomen om de Persoonsgegevens te beschermen. Daarnaast is het een manier waarmee een organisatie aan zowel de (gewezen) deelnemers en pensioengerechtigden als aan de AP kan laten zien dat het compliant zijn aan de AVG belangrijk vindt. Daarnaast dient een organisatie te beschikken over een privacyverklaring. Alle organisaties die Persoonsgegevens verwerken, moeten mensen heldere informatie geven over de Persoonsgegevens die zij verwerken en voor welk(e) doel(en) zij deze gegevens verwerken. De meest aangewezen manier hiervoor is het opstellen van een (online) privacyverklaring. Het servicedocument 'guidance verwerking persoonsgegevens pensioenfondsen' van de Pensioenfederatie meldt in paragraaf 7 welke onderdelen in een privacyverklaring (zie voor dit begrip artikel 6.1) worden opgenomen.⁶

⁶ Het servicedocument Guidance Verwerking Persoonsgegevens Pensioenfondsen geeft praktische handvatten voor de implementatie van de AVG en voor de aanpassing van processen en systemen en is beschikbaar voor leden van de Pensioenfederatie.

4.2.2

Het Pensioenfonds moet een gerechtvaardigd belang hebben voor de Verwerking van Persoonsgegevens. Een Pensioenfonds kan zich op deze grondslag baseren als aan drie voorwaarden wordt voldaan: (1) het Pensioenfonds heeft een gerechtvaardigd belang, (2) de Verwerking is noodzakelijk om dit gerechtvaardigde belang te behartigen en (3) het Pensioenfonds heeft een afweging gemaakt tussen het belang van het Pensioenfonds en die van de personen van wie de Persoonsgegevens worden verwerkt.

Ten eerste moet het gaan om een gerechtvaardigd belang. Dit belang moet rechtmatig, voldoende duidelijk verwoord en ook echt aanwezig zijn. Dat is zo wanneer een verwerking aantoonbaar noodzakelijk is om de bedrijfsactiviteiten te verrichten. Het voeren van een pensioenadministratie is een noodzakelijk onderdeel van de bedrijfsactiviteiten van een Pensioenfonds.

Ten tweede moet de Verwerking van de Persoonsgegevens noodzakelijk zijn voor de behartiging van het gerechtvaardigde belang. Een pensioenfonds moet de verwerking daarom toetsen aan de eisen van (1) proportionaliteit en (2) subsidiariteit.

Dat betekent dat een Pensioenfonds moet nagaan of (1) het doel van de Verwerking in verhouding staat tot de inbreuk voor de personen van wie de Persoonsgegevens worden verwerkt en (2) of een Pensioenfonds het doel niet op een voor de betrokken personen minder nadelige manier kan bereiken.

Ten derde moet een Pensioenfonds een afweging maken tussen de belangen van een Pensioenfonds en de belangen van de personen van wie het Pensioenfonds de Persoonsgegevens verwerkt. Ook moet een Pensioenfonds hierbij eventueel maatregelen treffen om ervoor te zorgen dat de rechten en vrijheden van deze personen niet zwaarder wegen dan het gerechtvaardigd

belang van een Pensioenfonds. Dit betekent onder meer dat de gegevens niet langer bewaard worden dan nodig is voor het doel van de verwerking.

De kwaliteit van data van een Pensioenfonds wordt bepaald door de mate waarin deze data geschikt, volledig en accuraat is. Tekortkomingen in bijvoorbeeld pensioengegevens van deelnemers kunnen ertoe leiden dat een deelnemer later niet het pensioen ontvangt waar hij recht op heeft en/of ertoe leidt dat de deelnemer onjuist wordt geïnformeerd over zijn pensioen. Ook kunnen tekortkomingen in de data leiden tot inefficiënte processen en financiële of reputatieschade voor het Pensioenfonds. Een deelnemer is bij de uitvoering van de pensioenregeling gebaat bij een juiste en volledige pensioenadministratie.

Het Pensioenfonds moet er actief voor zorgen dat de verwerkte gegevens juist en actueel zijn en neemt daar alle redelijke maatregelen voor. Het is onvolledige als een pensioenfonds een afwachtende houding aanneemt, waarbij foutieve gegevens alleen worden gecorrigeerd na klachten van deelnemers.

Het servicedocument 'Guidance verwerking persoonsgegevens pensioenfondsen' van de Pensioenfederatie meldt in paragraaf 8 welke onderdelen in een verwerkingsregister worden opgenomen.⁷

⁷ Het servicedocument [Guidance Verwerking Persoonsgegevens Pensioenfondsen](#) geeft praktische handvatten voor de implementatie van de AVG en voor de aanpassing van processen en systemen en is beschikbaar voor leden van de Pensioenfederatie.

5

Rechtmatigheid van de Verwerking

5.1.2

Rechtmatigheid

Er is een aantal rechtsgrondslagen voor de Verwerking van Persoonsgegevens voor pensioenfondsen.

- a De Betrokkene heeft Toestemming gegeven voor de Verwerking voor een of meer specifieke doeleinden. Voor pensioenfondsen gaat het hier om Persoonsgegevens die niet strikt noodzakelijk zijn voor de uitvoering van de pensioenovereenkomst/-pensioenregeling.
- b De Verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de Betrokkene partij is, of om op verzoek van de Betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen. Deze grondslag is van toepassing voor niet-verplichtgestelde pensioenfondsen.
- c De Verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op het Pensioenfonds rust (deze wettelijke plicht moet een grondslag hebben in het recht van de Europese Unie dan wel een unierechtelijke lidstaat). Verplicht gestelde pensioenfondsen verwerken Persoonsgegevens van Betrokkene op basis van deze rechtsgrond.
- d De Verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van het Pensioenfonds of van een Derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de Betrokkene die tot bescherming van de Persoonsgegevens nopen, zwaarder wegen dan die belangen.

Dit betekent dat het Pensioenfonds altijd een aantoonbare afweging zal moeten maken waarbij de rechten en verwachtingen van Betrokkene worden afgewogen tegen het gerechtvaardigde belang van het Pensioenfonds. Indien Persoonsgegevens verwerkt worden op basis van deze grondslag, zal Betrokkene tevens moeten worden gewezen op het recht van bezwaar. Indien de Verwerking is gebaseerd op gerechtvaardigde belangen dient het Pensioenfonds de Betrokkene te informeren over welke deze gerechtvaardigde belangen zijn. In dit kader wordt ook verwezen naar artikel 7.2.2 die betrekking heeft op Persoonsgegevens van strafrechtelijke aard, waaronder de sanctieregelgeving.⁸

⁸ Zoals de Sanctiewet 1977, Verordening (EU) 268/2014, Council Decision (CFSP) 2016/1693, Council regulation (EU) 2016/1686, Verordening (EU) 2019/452(2) ("verordening screening BDI") en eind 2022 bijvoorbeeld Verordening (EU) 2022/1903 t/m 1906 en de Besluiten GBVB 2022/1907 t/m 1909.

In de pensioensector worden in bepaalde gevallen persoonsgegevens verwerkt op basis van de rechtsgrondslag "gerechtvaardigd belang". Onder voorwaarde dat de verwerking van ex-partnergegevens voldoet aan de beginselen "behoorlijk, transparant, dataminimalisatie, juistheid, opslagbeperking, integriteit en vertrouwelijkheid", kan deze verwerking worden gezien als rechtmatig op basis van gerechtvaardigd belang. Enkele voorbeelden waarin er sprake kan zijn van gerechtvaardigd belang zijn:

- Het pensioenfonds verwerkt de gegevens van partners van deelnemers
- Verwerken van ex-partnergegevens
- Gegevens die via UPA aan het pensioenfonds worden aangeleverd
- Gegevensverwerking van aspirant-deelnemers

6 Doeleinden voor de Verwerking van Persoonsgegevens

6.1

Inleiding

Het Pensioenfonds verwerkt geen Persoonsgegevens als de doeleinden voor verwerking van de Persoonsgegevens niet op één van de wettelijke grondslagen gebaseerd is. Het Pensioenfonds heeft in haar privacybeleid de gehanteerde grondslagen opgenomen. In een privacyverklaring deelt het Pensioenfonds met Betrokkenen de doeleinden en grondslagen van de Verwerking (op hoofdlijnen). Deze verklaring staat op de website van het Pensioenfonds en andere communicatiemiddelen.

Bij elk nieuw proces dan wel wijziging in een proces waar de Verwerking van Persoonsgegevens onderdeel van uitmaakt, maakt het Pensioenfonds een initiële inschatting van de risico's die gepaard gaan met de Verwerking. Ingeval het risico als hoog ingeschat wordt, dan voert het Pensioenfonds een (aanvullende) DPIA uit om passende technische en organisatorische beheersmaatregelen te treffen die deze risico's voldoende mitigeren.

- 6.2 Persoonsgegevens in het kader van uitvoeren van pensioenregeling**
Deze doelstelling is de belangrijkste doeleinde voor een Pensioenfonds en moet ruim uitgelegd worden. Om voor actuele gegevens te zorgen is periodieke verificatie van de Persoonsgegevens belangrijk. Bij beëindiging van de actieve relatie met het Pensioenfonds (slaper) zal het Pensioenfonds passende aanvullende werkzaamheden verrichten om de Persoonsgegevens actueel te houden.
- 6.3 Persoonsgegevens in relatie tot historische, statistische en wetenschappelijke doeleinden**
Pensioenfondsen kunnen de uitkomst van historische, statistische en wetenschappelijke analyse gebruiken om onder meer scenario's voor de waardering van de pensioenverplichtingen en kasprojecties op te stellen. Pensioenfondsen zullen de Persoonsgegevens ten grondslag aan de analyse waar mogelijk anonimiseren of pseudonimiseren. Dit betreft bijvoorbeeld Persoonsgegevens in relatie tot sterfte analyses, portefeuille verdeling op leeftijd.
- 6.4 Persoonsgegevens in het kader van relatiemanagement en Direct Marketing activiteiten**
De Verwerkingen in het kader van relatiemanagement en marketingactiviteiten zullen met name gericht zijn op het versterken van bewustwording en pensioenbewustzijn van de deelnemers (Betrokkenen). Pensioenfondsen die deze Verwerkingen verrichten onder de grondslag "met Toestemming van Betrokkenen", nemen dit expliciet in het privacybeleid en gepubliceerde privacyverklaring op. Verder worden de Betrokkenen hierover expliciet geïnformeerd. Het gebruik van e-mailadressen voor pensioencommunicatie valt onder artikel 6.5.3 en niet onder dit artikel.
- 6.5 Persoonsgegevens in verband met wettelijke voorschriften**
- 6.5.1** Persoonsgegevens kunnen worden verstrekt aan bevoegde autoriteiten. Hierbij kan gedacht worden aan de het verstrekken van Persoonsgegevens in het kader van de sanctieregeling.
- 6.5.2** De Sociale Verzekeringsbank en de Pensioenfondsen zijn verantwoordelijk voor het aanleveren van juiste en volledige gegevens bij Stichting Pensioenregister voor mijnpensioenoverzicht.nl, zodat in technische zin de raadpleegfuncties accuraat werkend worden gehouden.
- 6.5.3** Het Pensioenfonds kan (verplichte) pensioencommunicatie elektronisch of schriftelijk verstrekken. Er kan gewisseld worden tussen schriftelijke verstrekking en elektronische verstrekking van de informatie. Daarbij kan gedacht worden aan een gemiddelde frequentie van eenmaal per jaar uit kostenoverwegingen. Het voornemen om de (verplichte) pensioencommunicatie elektronisch te verstrekken mag het Pensioenfonds schriftelijk of elektronisch communiceren. Dit betekent dat als het Pensioenfonds beschikt over het e-mailadres van de (gewezen) deelnemer of andere pensioengerechtigden, dit e-mailadres zonder

Toestemming van de (gewezen) deelnemer of andere pensioengerechtigden gebruikt mag worden voor het communiceren van dit voornemen. Het vervolgens gebruiken van het e-mailadres voor de (verplichte) pensioencommunicatie mag alleen als de (gewezen) deelnemer of andere pensioengerechtigden bij dit elektronisch vragen heeft ingestemd met elektronische verstrekking d.w.z. hiervoor Toestemming heeft gegeven.

Als de (gewezen) deelnemer of andere pensioengerechtigden schriftelijk zijn geïnformeerd over het voornemen mag het Pensioenfonds het e-mailadres gebruiken voor de (verplichte) pensioencommunicatie, tenzij de (gewezen) deelnemer of andere pensioengerechtigden hiertegen bezwaar heeft gemaakt.

Ingeval van het elektronisch informatie verstrekken is het Pensioenfonds verplicht de elektronisch verstrekte informatie te bewaren tot zeven jaar na het overlijden van de pensioengerechtigde dan wel tot één jaar na het aflopen van de uitkering aan de nabestaanden. De (gewezen) deelnemer of andere pensioengerechtigden kunnen ten hoogste eenmaal per jaar de elektronisch verstrekte informatie opvragen.

6.6

Persoonsgegevens in verband met behartiging gerechtvaardigde belangen Fraudepreventie en gegevensverstrekking aan verenigingen van pensioengerechtigden of belanghebbendenverenigingen zijn goede voorbeelden van gebruik van Persoonsgegevens met dit doeleinde.

Fraudepreventie

Vertrouwen is essentieel voor het draagvlak van burgers van de pensioensector. Onderdeel hiervan is dat het Pensioenfonds de integriteit van de sector hoog in het vaandel heeft staan. Daarnaast is het Pensioenfonds verplicht een integere en beheerste bedrijfsvoering te hebben. Hiervoor moet het Pensioenfonds maatregelen nemen. Zo neemt het Pensioenfonds maatregelen om fraude te voorkomen.

Cameratoezicht

Cameratoezicht kan de privacy van burgers ernstig aantasten. De AP vindt het daarom belangrijk dat iedereen voorzichtig omgaat met cameratoezicht. De AP heeft zelf voor verschillende vormen van cameratoezicht voorlichtingsmateriaal opgesteld.⁹

⁹ Het voorlichtingsmateriaal van de AP met het oog op cameratoezicht is onder de titel 'film en foto' te vinden.

Gegevensverstrekking aan verenigingen

Er dient sprake te zijn van een evenredige vertegenwoordiging in een paritair bestuur.

In het paritaire bestuur van een Pensioenfonds zijn de belanghebbenden op een zo evenwichtig mogelijke wijze vertegenwoordigd. In het verantwoordingsorgaan zijn de deelnemers en de pensioengerechtigden evenredig op basis van onderlinge getalsverhoudingen vertegenwoordigd. Dit brengt met zich mee dat pensioengerechtigden in het bestuur en het verantwoordingsorgaan deelnemen.

De benoeming van de vertegenwoordigers van pensioengerechtigden in het paritaire bestuur van een Pensioenfonds vindt plaats:

- a na verkiezing van de vertegenwoordigers door de pensioengerechtigden; of
- b op voordracht van de vertegenwoordigers van de pensioengerechtigden in het verantwoordingsorgaan, mits deze vertegenwoordigers na verkiezing zijn benoemd.

De benoeming van leden van het verantwoordingsorgaan en een belanghebbendenorgaan door pensioengerechtigden gebeurt door het voordragen van kandidaten door verenigingen of door individuele pensioengerechtigden.

Voor het bereiken van pensioengerechtigden voor het houden van verkiezingen en het verstrekken van informatie hieromtrent moet de vereniging de pensioengerechtigden weten te bereiken. In dit geval is het toegestaan om naam-, adres- en woonplaatsgegevens te verstrekken aan deze verenigingen, tenzij Betrokkene hiertegen bezwaar aantekent.

Dergelijke verenigingen behartigen de belangen van de Betrokkenen bij een pensioenfonds. In verband met de behartiging van gerechtvaardigd belangen van pensioengerechtigden, kan het tevens toegestaan zijn om naam-, adres- en woonplaatsgegevens te verstrekken aan deze verenigingen.

In artikel 6, lid 2 Wet betreffende verplichte deelneming in een bedrijfstakpensioenfonds 2000 is in verband met de taakafbakening van bedrijfstakpensioenfonds expliciet vastgelegd dat naam-, adres-, en woonplaatsgegevens mogen worden verstrekt door Pensioenfondsen aan verenigingen met volledige rechtsbevoegdheid die als statutair doel of mede als statutair doel hebben het behartigen van de belangen van de Betrokkenen bij een bedrijfstakpensioenfonds (lees: vereniging van pensioengerechtigden of verenigingen die de belangen van haar leden als belanghebbenden bij een bedrijfstak-/beroepspensioenfonds behartigen). Maar op basis van het behartigen van de gerechtvaardigde belangen kan het voor Ondernemingspensioenfondsen, algemene pensioenfondsen en Beroepspensioenfondsen tevens toegestaan zijn om naam-, adres-, en woonplaatsgegevens te verstrekken aan deze verenigingen, onder de waarborgen van de AVG.

Voor Pensioenfondsen bestaat de mogelijkheid een voorzichtiger benadering te kiezen en geen Persoonsgegevens te verstrekken. Ter invulling van de verplichtingen uit de Pensioenwet en de Wet verplichte beroepspensioenregeling kan ervoor worden gekozen om informatie over verkiezingen via het Pensioenfonds te verstrekken. Pensioenkranten en verkiezingskranten waarin kandidaten zich voorstellen zijn goed gebruik om invulling te geven aan de rechten van de bedoelde verenigingen zodat de achterban wordt bereikt.

7 Verwerking van Bijzondere categorieën van en overige gevoelige Persoonsgegevens

7.1.2 Persoonsgegevens betreffende iemands gezondheid

Dit hoofdstuk bevat specifieke regels met betrekking de Verwerking van Bijzondere categorieën van Persoonsgegevens en overige gevoelige Persoonsgegevens. Voor Bijzondere Persoonsgegevens gelden zwaardere vereisten waaraan voldaan moet worden bij de Verwerking. Tegelijkertijd geeft de geldende wet- en regelgeving Pensioenfondsen meer ruimte om Gegevens over gezondheid te verwerken dan andere sectoren. Dit hangt samen het maatschappelijke belang van Pensioenfondsen, waardoor Pensioenfondsen genoodzaakt zijn deze Gegevens over gezondheid te verwerken.

Het arbeidsongeschiktheidspercentage (AO%) vormt een Gegeven betreffende iemands gezondheid. Pensioenuitvoerders zijn gerechtigd het AO% te verwerken omdat dit noodzakelijk is voor een goede uitvoering van de pensioenregelingen.¹⁰

¹⁰ Zie artikel 30 lid 1 AVG

7.2.2 Persoonsgegevens van strafrechtelijke aard

Een Pensioenfonds kan gegevens van strafrechtelijke aard verwerken om de integriteit en veiligheid van de bedrijfsvoering en de sector te waarborgen.¹¹ Onder Persoonsgegevens van strafrechtelijke aard verstaat de pensioensector in het kader van deze Gedraglijn ook de geconsolideerde lijst van personen en organisaties waarvan de tegoeden op grond van Europese regelgeving zijn bevroren.¹² Dergelijke tegoeden (pensioenaanspraken of pensioenuitkeringen) worden bevroren en als zodanig verwerkt.

¹¹ Zie artikel 33 AVG

¹² Zie <http://www.consilium.europa.eu/nl/policies/fight-against-terrorism/terrorist-list/>

7.3 Kopie identiteitsbewijs

Het is Pensioenfondsen toegestaan kopieën van identiteitsbewijzen op te vragen. Identificatie van Betrokkene is onder andere noodzakelijk indien Betrokkene een beroep doet op één of meerdere rechten vanuit de AVG. Ook is het toegestaan om een kopie identiteitsbewijs te verwerken om op juiste wijze invulling te kunnen geven aan de pensioenrechten van Betrokkene (bijv. i.g.v. afkoop). In het kader van dataminimalisatie geldt dat het Pensioenfonds niet alle informatie nodig heeft die op het kopie identiteitsbewijs staat. Het Pensioenfonds vraagt daarom in dat geval de Betrokkene de pasfoto, het Burgerservicenummer en de MRZ-code onleesbaar te maken of op een andere manier zorg te dragen voor dataminimalisatie.

7.5 Gevoelige Persoonsgegevens

Naast de categorieën “strafrechtelijke” en “bijzondere” Persoonsgegevens onderscheidt deze Gedraglijn ook de categorie “gevoelige Persoonsgegevens”. Hoewel de AVG de term Gevoelige Persoonsgegevens niet kent, zijn dit gegevens die bij verlies of onrechtmatige Verwerking ongunstige gevolgen kunnen hebben voor de persoonlijke levenssfeer. Denk hierbij aan BSN, bankrekeningnummer of financiële gegevens. Betrokkenen kunnen door het

verlies, onrechtmatig gebruik of misbruik in hun belangen worden geschaad. Daarbij kan gedacht worden aan misbruik van een kwetsbare positie, aantasting in eer en goede naam, (identiteits)fraude, de financiële positie of discriminatie van Betrokkene.

7.6

Nationaal identificatienummer

Het Pensioenfonds mag op grond van artikel 94 Pensioenwet het Burgerservicenummer uitsluitend gebruiken:

- a in het verkeer met de persoon op wie het nummer betrekking heeft; of
- b in contacten met personen en instanties voor zover deze zelf gemachtigd zijn tot het opnemen van het Burgerservicenummer in een persoonsregistratie, zoals de belastingdienst, het UWV, de SVB en binnen de wettelijke kaders, de werkgever.

8

Rechten van Betrokkene

8.1

Algemene bepalingen

Deze paragraaf beschrijft de rechten van Betrokkene met betrekking tot de Verwerking van de Persoonsgegevens bij het Pensioenfonds, conform artikel 15 tot en met 20 AVG. De gedachte achter het toekennen van deze rechten is dat de Betrokkene weet welke Persoonsgegevens voor welke doeleinden worden verwerkt en zo het Pensioenfonds kan aanspreken indien nodig.

Het Pensioenfonds moet op grond van de wet- en regelgeving zorgen voor een deugdelijke vaststelling van de identiteit om te zorgen dat de juiste persoon toegang krijgt tot de Persoonsgegevens. Bij schriftelijke verzoeken kan dit door een kopie identiteitsbewijs op te vragen. In het kader van dataminimalisatie geldt dat het Pensioenfonds niet alle informatie nodig heeft die op het kopie identiteitsbewijs staat. Het Pensioenfonds vraagt daarom in dat geval de Betrokkene de pasfoto, het Burgerservicenummer en de MRZ-code onleesbaar te maken. Pensioenfondsen kunnen ook andere manieren van identificatie gebruiken zoals inloggen met DigiD of op een andere manier zorg te dragen voor dataminimalisatie.

Het is over het algemeen verstandig om het doel van het verzoek te achterhalen. Op die manier kan in samenspraak met Betrokkene de gevraagde informatie verstrekt worden.

Onder een redelijke termijn wordt verstaan: drie maanden.

8.2

Informatieplicht over Verwerking Persoonsgegevens

Doel van de informatieplicht is dat de Betrokkenen weet welke Persoonsgegevens worden verwerkt door het Pensioenfonds. Als de Betrokkene niet op de hoogte is van de Verwerking, kan deze hij zijn rechten niet goed uitvoeren. Pensioenfondsen geven o.a. uitvoering aan deze informatieplicht met

de privacyverklaring op de website van het Pensioenfonds. Doorgaans zullen Pensioenfondsen de Persoonsgegevens verkrijgen via derden, te weten de werkgever en andere instanties als BRP en UWV. In dat geval moet het Pensioenfonds binnen 1 maand na verkrijging van de Persoonsgegevens voldoen aan de informatieplicht, tenzij aan een van de uitzonderingen hiervoor wordt voldaan. In lijn met de specifieke wetgeving die geldt voor het informeren van Deelnemer over hun deelname aan de pensioenregeling kan het Pensioenfonds er voor kiezen de informatie gelaagd aan te bieden.

8.3

Inzage

Het overzicht bevat een omschrijving van het doel van de Verwerking, de categorieën van Persoonsgegevens, de Ontvangers of categorieën van Ontvangers en de herkomst van de Persoonsgegevens.

8.4

Correctie

Het Pensioenfonds geeft geen uitvoering aan het recht op correctie als de gegevens zijn verkregen uit de Basisregistratie Personen (Brp). Correctie kan ook betrekking hebben op onjuiste gegevens die het Pensioenfonds krijgt van de werkgever, bijvoorbeeld via de loonafgifteketen.

8.5.2

Gegevenswissing

Onder sub iv 'overeenkomst' wordt verstaan de Uitvoeringsovereenkomst.

8.5.3

Gegevenswissing ("recht op vergetelheid")

Voor Pensioenfondsen zal het recht op gegevenswissing niet snel ingeroepen kunnen worden. Dit heeft te maken met het feit dat de gegevensverwerking van het Pensioenfonds onder andere noodzakelijk is om te voldoen aan een wettelijke verplichting.

De gegevens van de Betrokkenen moeten over het algemeen in de administratie blijven staan om aan te kunnen tonen dat het Pensioenfonds beschikt over een beheerste en integere bedrijfsvoering. Dit betekent bijvoorbeeld dat het Pensioenfonds moet kunnen aantonen dat gegevens zijn opgeslagen in de administratie en dat bepaalde brieven of bepaalde correspondentie zijn verstuurd.

Onderdeel daarvan is dat er bij een onvoorziene omstandigheid het bedrijf van Pensioenfonds "gewoon" verder kan worden uitgevoerd. Hiervoor worden regelmatig back ups gemaakt. Back ups zijn niet ontworpen of bedoeld om individuele bestanden of Persoonsgegevens eruit weg te halen. Het Pensioenfonds moet wel maatregelen nemen zodat na terug zetten van de back up duidelijk is dat de betreffende deelnemer geormerkt is.

Een verzoek tot gegevenswissing zal bij Pensioenfondsen waarschijnlijk alleen slagen als het Pensioenfonds de gegevens al ten onrechte in de administratie had opgenomen of de geldende bewaartermijn is overschreden.

8.7 Overdraagbaarheid van Persoonsgegevens

Bij Pensioenfondsen zal naar verwachting vooralsnog geen sprake zijn van data portabiliteit. In het kader van waardeoverdracht is er reeds sprake van een goed lopend bestaand proces.

8.8 Bezwaar

Het Pensioenfonds staakt de Verwerking van de Persoonsgegevens bij bezwaar tenzij hij dwingende gerechtvaardigde gronden voor de Verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de Betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.

Wanneer de Betrokkene bezwaar maakt tegen Verwerking ten behoeve van direct marketing, worden de Persoonsgegevens niet meer voor deze doeleinden verwerkt. Daartoe documenteert het Pensioenfonds het bezwaar van de Betrokkene in een intern register.

8.9.1 Geautomatiseerde besluitvorming, waaronder profilering

Op basis van de gegevens die het Pensioenfonds heeft, wordt bepaald tot welke doelgroep iemand behoort. Deze doelgroepen bepalen op welke wijze met iemand wordt gecommuniceerd en waarover. Uit de richtsnoeren inzake geautomatiseerde besluitvorming en profilering (EU 2016/679) valt af te leiden dat het hier gaat het verzamelen van informatie over een persoon (of een groep personen) en het evalueren van hun kenmerken of gedragspatronen om deze persoon of personen in een bepaalde categorie of groep te plaatsen. Het gaat hierbij om verwerken van persoonlijke gegevens om interesses of waarschijnlijke gedrag te analyseren of hierover voorspellingen te doen.

Op basis van de Pensioenwet en de Wet verplichte beroepspensioenregeling moet het Pensioenfonds bevorderen dat de communicatie aansluit bij de informatiebehoefte en kenmerken van de (gewezen) deelnemer, gewezen partner en pensioengerechtigde. Daarnaast moet het Pensioenfonds hun voorzieningen, premies en risicohouding zo nauwkeurig mogelijk vaststellen.

Voorbeelden waarbij profilering wordt toegepast door pensioenfondsen zijn:

Personaliseren van pensioencommunicatie: Hier past een Pensioenfonds segmentering toe, een vorm van profilering om communicatie beter op de persoonlijke situatie af te stemmen. Met deze toepassing wordt beoogd te voldoen aan de eisen uit artikel 48 lid 1, lid 2 en lid 3 van de Pensioenwet. Het profileren uitsluitend gericht op dit doel is daarmee wettelijk toegestaan. Het toepassen van segmentatie uitsluitend voor dit doel is verenigbaar met het uitvoeren van de pensioenovereenkomst.

Beleggen met behulp van life-cycles in DC regelingen, gebaseerd op risico-profielen als onderdeel van de pensioenregeling: Het beleggen volgens het "life cycle"-model is veelal gebaseerd op het risicoprofiel van de deelnemer. De deelnemer vult zelf een risicoprofiel in, met de mogelijkheid deze aan te passen en op basis van dit profiel wordt een passende "life cycle" bepaald. Indien er sprake is van een premiereregeling met beleggingsvrijheid (art. 52 Pw), heeft de deelnemer zelf de mogelijkheid om de beleggingen over te nemen. Beide vormen van geautomatiseerde besluitvorming zijn toegestaan, er is daarmee sprake van menselijke tussenkomst.

9 Overige onderwerpen

9.1.1 Privacy by default

Het waarborgen van de privacy is met name van belang bij online deelnemersportalen en bulk communicatie-activiteiten en is afgestemd op de Pensioenwet en de Wet verplichte beroepspensioenregeling. Daar waar Persoonsgegevens worden verwerkt op basis van een wettelijke verplichting of voor de uitvoering van pensioenovereenkomsten, geldt dat uitsluitend de strikt noodzakelijke gegevens worden verwerkt. Hierdoor wordt geen toestemming van de deelnemer gevraagd, maar volstaat het informeren via de privacyverklaring van het Pensioenfonds. Voor overige verwerkingen geldt het opt-in-principe: pas als een Betrokkene zich ergens voor heeft aangemeld ontvangt deze informatie (opt-in), in plaats van het automatisch ontvangen van informatie totdat het op aanvraag wordt stopgezet (opt-out).

Om aan het principe van privacy by default invulling te geven, kan rekening gehouden worden met de volgende normen: een Betrokkene wordt expliciet gevraagd om Toestemming als deze zich heeft aangemeld voor het ontvangen van informatie, tenzij deze informatie verplicht aan Betrokkene moet worden verstrekt op basis van de wettelijke verplichtingen c.q. het uitvoeren van de pensioenovereenkomst. Een Betrokkene kan op een eenvoudige manier deze Toestemming direct stop zetten.

Persoonsgegevens worden standaard nooit zichtbaar tenzij de Betrokkene daar Toestemming voor geeft.

Bij het gebruik van een app is er geen standaard inzage in het adresboek van de Betrokkene.

Er vindt geen automatische koppeling met en inloggen op andere websites plaats.

Er is geen vooraf aangevinkte optie in online contactformulieren zoals "ik wil op de hoogte gehouden worden".

9.1.2

Privacy by design

Om aan het principe van privacy by design invulling te geven, kan rekening gehouden worden met de volgende technieken die hierbij kunnen worden toegepast zijn:

Algemeen

Online deelnemersportalen en werkgeversportalen beschikken tenminste over een vorm van two factor authenticatie. Dat betekent dat om toegang te krijgen tot de betreffende portalen er naast gebruikersnaam en wachtwoord er nog tweede unieke sleutel nodig is. Voor een specifieke invulling wordt verwezen naar 9.5.2.

Bij bulk communicatie vindt voor verzending van een elektronische of fysieke verzending een extra controle plaats op de Persoonsgegevens (NAW, e-mailadres). Hiervoor wordt gebruik gemaakt van de bronnen die ter beschikking staan van het Pensioenfonds.

Als gegevens niet relevant zijn in het betreffende pensioenproces worden deze gegevens niet opgevraagd aan de Betrokkene.

Pseudonimiseren

Bij pseudonimisering wordt een gegevensbestand in tweeën gedeeld, waarbij bijvoorbeeld met het klantnummer van de deelnemer de koppeling tussen de Bestanden kan worden gemaakt. Het eerste deelbestand bevat gegevens waarmee een deelnemer direct kan worden geïdentificeerd, zoals NAW-gegevens, telefoonnummer, e-mailadres of Burgerservicenummer. Het tweede deelbestand bevat gegevens die alleen indirect iets over de deelnemer zeggen, zoals voorkeuren of antwoorden op een enquête.

Toepassen op: testomgeving, bijvoorbeeld bij interne waardeoverdrachten en aanpassingen in systemen en applicaties. Volgens de AVG is er bij pseudonimisering nog steeds sprake van Persoonsgegevens.

Anonimiseren

Er is sprake van anonimisering als geen koppeling meer gemaakt kan worden met direct of indirect identificerende gegevens, bijvoorbeeld door voor het tweede deelbestand van bovengenoemd voorbeeld het klantnummer van de deelnemer te verwijderen.

Toepassen op: het gebruik van Bestanden voor louter statistische doeleinden. In dat geval is de AVG niet meer van toepassing.

9.2.1

Veel voorkomende samenwerking tussen Pensioenfondsen en dienstverleners.

In de verwerkersovereenkomst moeten tenminste worden vastgelegd:

- onderwerp en duur van de verwerking;
- aard en doel van de verwerking;
- soort van Persoonsgegevens en de categorieën van Betrokkenen;
- rechten en verplichtingen van de Verwerkingsverantwoordelijke, waarin is bepaald dat Verwerker:
- Persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructie van de Verwerkingsverantwoordelijke;

- Persoonsgegevens vertrouwelijk verwerkt;
- de Verwerkingsverantwoordelijke om schriftelijke toestemming vraagt bij uitbesteding;
- de Verwerkingsverantwoordelijke ondersteunt bij diens informatieplicht naar Betrokkene;
- de Verwerkingsverantwoordelijke ondersteunt bij diens beveiligingsplicht
- na afloop van de uitbesteding de Persoonsgegevens teruggeeft aan de Verwerkingsverantwoordelijke en/of verwijderd;
- Verwerkingsverantwoordelijke alle informatie verstrekt die hij nodig heeft om zijn verplichtingen na te komen en voor audits; en
- Verwerkingsverantwoordelijke zo snel mogelijk informeert over een datalek.

9.4

Beleid bewaartermijnen

Pensioenfondsen stellen beleid op ten aanzien van het bewaren en archiveren van Persoonsgegevens. Steeds dienen Pensioenfondsen zich af te vragen of er redenen zijn op grond waarvan de Persoonsgegevens vastgelegd moeten blijven en wie toegang moeten krijgen tot de opgeslagen Persoonsgegevens. Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de verwerking van de doeleinden waarvoor de gegevens zijn verzameld of vervolgens verwerkt. Voorbeelden van bewaar doelstellingen zijn het voldoen aan wettelijke bewaarverplichtingen, het kunnen leveren van bewijs in geval van geschillen en het kunnen beschikken over gegevens voor het verrichten van onderzoek. Een Pensioenfonds stelt beleid op met betrekking tot de bewaartermijnen van de Persoonsgegevens, de verwijdering van de Persoonsgegevens en het eventueel overbrengen van deze Persoonsgegevens naar een archiefbestemming. In het laatste geval zullen de Persoonsgegevens slechts worden gebruikt voor het archiefbeheer, het behandelen van geschillen en het doen van wetenschappelijk, statistisch of historisch onderzoek.

Voor het vaststellen van toereikende bewaartermijnen moet rekening gehouden worden met zowel de belangen van de aanspraak- of pensioengerechtigde als met de belangen van het Pensioenfonds. Omdat pensioenaanspraken geen wettelijke verjaringstermijnen kennen, vraagt het vaststellen van de juiste termijnen om een lange termijn-benadering. Bijvoorbeeld in geval van pensionering, afkoop, echtscheiding en "vergeten pensioenen" is het van belang dat Pensioenfondsen c.q. uitvoerders kunnen reproduceren op welke wijze de pensioenopbouw heeft plaatsgevonden, waarop de berekeningen zijn gebaseerd, over welke deel van het salaris (incl. onkostenvergoedingen) pensioen is opgebouwd. Tussen het moment waarop zich een event (bijv. afkoop) voordoet en het moment dat er een geschil ontstaat, kan een periode van tientallen jaren liggen. Binnen deze termijn kunnen er vragen, aanspraken of geschillen ontstaan over de opgebouwde pensioenrechten.

13 Het servicedocument bewaartermijnen is beschikbaar voor leden van de Pensioenfederatie.

De Pensioenfederatie heeft voor de sector een servicedocument bewaartermijnen afgegeven, die als leidraad dient.¹³ Daarin staan overwegingen om te komen tot beleid voor bewaartermijnen. Overwegingen voor het vaststellen van bewaartermijnen kunnen zijn:

- Na het eindigen van de deelnemersrelatie door overlijden of waardeoverdracht 7 jaar na overlijden van de deelnemer, mits vastgesteld is dat er geen sprake is van een andere mogelijke aanspraak- of pensioengerechtigden, zoals een nabestaande.
- Een nader door de pensioenuitvoerder te bepalen termijn is verstreken na het overlijden van alle aanspraak- en pensioengerechtigden of na het realistisch te bepalen vermoedelijke overlijden (bij niet-opgevraagde pensioenen) van alle mogelijke aanspraak- en pensioengerechtigden terzake een bepaald pensioenrecht. Aanknopingspunt bij de dan te kiezen termijn kan zijn een periode van 5 jaar na het overlijden van de laatst mogelijke aanspraak- of pensioenrechtigde, dit in verband met een mogelijke vordering van de nabestaanden van de aanspraak- of pensioengerechtigden.

In artikel 59 Pensioenwet en in artikel 70 van de Wet verplichte beroeps-pensioenregeling is het volgende bepaald: 'een rechtsvordering tegen een pensioenuitvoerder tot het doen van een uitkering verjaart niet bij leven van de pensioengerechtigde.'

Een Pensioenfonds moet in ieder geval rekening houden met (rechts)vorderingen op pensioen(uitkeringen) die na vele jaren nog worden ingesteld door aanspraakgerechtigden.

Aanspraakgerechtigden hebben de mogelijkheid vorderingen in te stellen.

Het komt bijvoorbeeld voor dat na het overlijden van (gewezen) deelnemers de nabestaanden (partner, wezen) alsnog het niet-uitgekeerde pensioenrecht van de gewezen deelnemer vorderen alsmede het eigenstandige pensioenrecht dat geldt bij hun (eigen) leven, het nabestaandenpensioen. Voor nabestaandenpensioen kunnen zij een beroep doen op pensioenreglementen.

Indien de laatst mogelijke aanspraakgerechtigde overlijdt, is het nog denkbaar dat vervolgens nabestaanden van deze aanspraakgerechtigde niet-uitbetaalde pensioenuitkeringen van de overleden pensioengerechtigden over het verleden claimen. Deze vordering zal dan gebaseerd worden op het erfrecht. In hoeverre niet-uitbetaald pensioen na overlijden van de aanspraakgerechtigden als juridisch opeisbare vordering in de boedel valt is juridisch vooralsnog niet uitgekristalliseerd. Pensioenuitvoerders kunnen er in de praktijk wel mee geconfronteerd worden en dus met de relevantie van gegevens inzake die vordering. Het erfrecht kent voor deze vordering geen specifieke termijn. Als termijn voor die vordering moet derhalve dan de periode van vijf jaar als bedoeld in de artikelen 3:307 en 3:308 Burgerlijk Wetboek als leidend worden aangehouden.

Indien er sprake is van overbrenging ten behoeve van archiefbeheer en ter waarborging van geschillenbeslechting, zullen aanvullende maatregelen in acht worden genomen. Hierbij valt te denken aan een interne procedure voor het

opvragen van archiefstukken, waarbij de FG (of functionaris met een vergelijkbare rol) een centrale rol vervult bij het vaststellen welke partij toegang mag krijgen tot welke gearchiveerde Persoonsgegevens. Hierbij controleert de FG het uitgevoerde proces.

Indien er sprake is van een aanlevering van Persoonsgegevens via UPA dan is het mogelijk dat gegevens van niet Betrokkenen worden aangeleverd aan Pensioenfondsen. De UPA-aanlevering gebeurt in opdracht van werkgevers. Pensioenfondsen zijn verwerkingsverantwoordelijk wanneer zij de aanlevering ontvangen. Het is Good Practice als Pensioenfondsen werkgevers en administrateurs wijzen op de verplichting om uitsluitend noodzakelijke gegevens aan te leveren. Pensioenfondsen zullen de aanlevering in verband met de juistheid van (Persoons)gegevens willen bewaren. Een verwerking van de Persoonsgegevens van niet Betrokkenen door Pensioenfondsen is niet toegestaan, tenzij daarvoor toestemming is verkregen van de Betrokkene, daartoe een wettelijke verplichting bestaat, er sprake is van een gerechtvaardigd belang of indien er sprake is van verenigbaar gebruik.

9.5.1

Beveiliging Verwerking Algemeen

De organisatie die Persoonsgegevens verwerkt treft maatregelen, die rekening houdt met: (i) de stand van de techniek; (ii) de kosten van de tenuitvoerlegging; (iii) de risico's die de Verwerking met zich meebrengt; (iv) en de aard van de Persoonsgegevens, passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen tegen onder meer (opzettelijke) vernietiging, verlies, vervalsing, ongewenste verspreiding of toegang, dan wel tegen enige andere vorm van onrechtmatige Verwerking van Persoonsgegevens. Indien de Verwerking van Persoonsgegevens is uitbesteed, worden deze uitgangspunten contractueel vastgelegd met de partij waaraan de Verwerking is uitbesteed. Passende maatregelen zijn bijvoorbeeld de pseudonimisering en versleuteling van persoonsgegevens en, indien er sprake is van een incident in de continuïteit van de bedrijfsvoering, het tijdig herstellen van de beschikbaarheid en de toegang tot de Persoonsgegevens.

Er is een verschil tussen een datalek en een beveiligingsincident. Als er alleen sprake is van een zwakke plek in de beveiliging, waarbij (nog) geen inbreuk is gemaakt in verband met Persoonsgegevens (dus nog geen verlies of onrechtmatige Verwerking), dan spreken we van een beveiligingsincident en niet van een datalek. Zo'n beveiligingsincident (dus geen datalek) hoeft niet gemeld te worden bij de AP. Afhankelijk van de ernst van het beveiligingsincident kan een wettelijke verplichting bestaan om melding te doen bij een andere toezichthouder. Deze melding wordt dan gedaan op basis van een andere wettelijke verplichting, dan op basis van de AVG.

9.5.2 Beveiliging van Persoonsgegevens

Om toegang te krijgen tot de eigen Persoonsgegevens in portalen zoals de "mijn-omgevingen" dient gebruik worden gemaakt van tenminste twee factor authenticatie voor de deelnemer of de werkgever conform de wet- en regelgeving zoals de EIDAS en de WDO.

Bij het verwerken van de eigen Persoonsgegevens beschikt de Verwerker over een adequate administratieve organisatie en interne controle, waarbij de verschillende rollen van Verwerking zijn vastgelegd en de toegang tot deze Persoonsgegevens gebaseerd zijn op de goede rollen.

Persoonsgegevens worden vertrouwelijk behandeld en deze gegevens worden elektronisch encrypted of versleuteld of op een andere beveiligde methode opgeslagen en de fysieke variant wordt bewaard in een afgesloten ruimte.

9.5.3 Cameratoezicht

Wat betreft de beelden vanuit cameratoezicht wordt rekening gehouden met volgende uitgangspunten.

Indien er sprake is van toegangsbeveiliging worden opgeslagen beelden normaliter automatisch in een tijdsbestek van 5 werkdagen gewist. Deze beelden worden alleen aan derden afgestaan in geval van verzoeken van het bevoegd gezag. Belangrijk is dat camerabeelden zich beperken tot de formele terreinen waarvoor dit is toegestaan en niet op bijvoorbeeld openbare terreinen. Voor de Betrokkene die op beeld kan worden vastgelegd, is dat duidelijk bij binnenkomst. De betreffende beelden worden op een encrypted medium opgeslagen. De camerabeelden vallen onder het recht op inzage.

9.5.4 Telefoongesprekken

De Betrokkene wordt erop gewezen indien telefoongesprekken worden vastgelegd.

Telefoongesprekken, ook voor trainingsdoeleinden, worden encrypted of versleuteld opgeslagen.

Er dient een apart protocol te zijn opgesteld in lijn met het bewaarbeleid, waarin de wijze van opslag, de gehanteerde bewaartermijn en de wijze van wissen zijn vastgelegd.

De telefoongesprekken vallen onder het recht op inzage.

9.5.5 Vastlegging elektronische communicatie

Ook voor de overige vormen van elektronische communicatie, zoals bijvoorbeeld e-mails en chats, zijn uitgangspunten inzake vastlegging, opslag (bewaren) en transport vastgesteld.

Indien de vastlegging niet direct wordt gewist is er sprake van opslag (bewaren).

De vormen van elektronische communicatie dient encrypted of versleuteld te worden vastgelegd en opgeslagen.

Ook de wijze van intern en extern transport van elektronische communicatie dient encrypted of versleuteld plaats te vinden.

Er dient een apart protocol te zijn opgesteld, waarin de wijze van opslag, de gehanteerde bewaartermijn en de wijze van wissen zijn vastgelegd.

9.6.1

Datalekken

Een datalek is een inbreuk op de beveiliging die leidt tot:

- de vernietiging of het verlies van persoonsgegevens ('inbreuk op de beschikbaarheid'), of
- de wijziging van persoonsgegevens ('inbreuk op de integriteit'), of
- de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens ('inbreuk op de vertrouwelijkheid').

Het begrip datalek wordt in de AVG niet gebruikt. De AVG spreekt van een inbreuk in verband met persoonsgegevens. In de praktijk wordt, ook door de AP, deze inbreuk een datalek genoemd.

Van een datalek is eerst sprake bij een daadwerkelijk beveiligingsincident. Bij een dreiging van een datalek of een tekortkoming in de beveiliging is sprake van een beveiligingslek.

Het is voor de kwalificatie als datalek niet relevant of er al dan niet kwaad opzet in het spel is. Een datalek kan ook per ongeluk ontstaan. Dat betekent dat voor de vraag of sprake is van een datalek niet bepalend is wie de schuld draagt of aansprakelijk is voor het datalek. De schuld- en daarmee ook de aansprakelijkheidsvraag speelt pas als er een boete van de AP volgt of anderszins een schadeclaim van degene van wie persoonsgegevens zijn gelekt of een derde die (im)materiële schade opgelopen heeft als gevolg van het datalek.

Voorbeelden van datalekken zijn:

- het verlies van een gegevensdrager (bijv. USB-stick of laptop) met niet-versleutelde persoonsgegevens;
- een cyberaanval of andere vorm van hacking, malware, ransomware en/of phishing waarbij persoonsgegevens zijn buitgemaakt;
- een besmetting met ransomware waarbij persoonsgegevens ontoegankelijk zijn gemaakt;
- het inzien van deelnemersbestanden door onbevoegden;
- e-mail met persoonsgegevens verstuurd aan verkeerde Ontvanger(s)/e-mailadressen;
- e-mail verstuurd met persoonsgegevens in de cc. in plaats van bcc
- persoonsgegevens door storing (tijdelijk) niet beschikbaar
- persoonsgegevens toegevoegd aan het verkeerde dossier

9.6.2

Melden datalekken

Een datalek kan voor Betrokkene, dat wil zeggen degene van wie persoonsgegevens zijn gelekt, grote gevolgen hebben, waaronder verlies van controle over zijn persoonsgegevens, de beperking van zijn rechten, discriminatie, identiteitsdiefstal of financiële verliezen. Het is dan ook belangrijk dat een datalek tijdig en op passende wijze wordt aangepakt, zodat de inbreuk op de rechten en vrijheden van de betrokkene zo veel als mogelijk wordt beperkt en naar de toekomst toe wordt voorkomen.

Om die reden moet in beginsel ieder datalek worden gemeld aan de AP. Alleen als het onwaarschijnlijk is dat het datalek een risico inhoudt voor Betrokkene (zeg maar, geen grote gevolgen heeft voor de rechten en vrijheden van Betrokkene), hoeft het datalek niet gemeld te worden aan de AP. Denk hierbij aan de situatie dat degene die onrechtmatig de persoonsgegevens heeft ontvangen, bevestigt dat hij deze niet ingezien heeft of vernietigd heeft. Of in de situatie dat het datalek binnen de organisatie heeft plaatsgevonden en de medewerker gehouden is aan een geheimhoudingsplicht. Belangrijk is om per geval te onderbouwde inschatting te maken van de mogelijke gevolgen de Betrokkene(n).

Het is belangrijk dat als afgezien wordt van melden aan de AP de reden van het niet melden wordt gedocumenteerd in het datalekregister van het Pensioenfonds.

Als het datalek waarschijnlijk een hoog risico inhoudt voor Betrokkene, moet het datalek ook aan deze gemeld worden.

Van een hoog risico is in ieder geval sprake als:

- er persoonsgegevens van gevoelige aard of bijzondere persoonsgegevens gelekt zijn; of
- betrokkene door het verlies of de onrechtmatige verwerking van zijn persoonsgegevens in zijn belangen geschaad wordt. De schade kan van materiële of van immateriële aard zijn. Voorbeelden van schade zijn onrechtmatige publicatie, aantasting in eer en goede naam, identiteitsfraude of discriminatie.

9.6.3

Bulkmelding datalekken

Een Pensioenfonds verzendt grote aantallen poststukken met daarin gevoelige persoonsgegevens. Een klein deel van de poststukken kan bij een verkeerde Ontvanger terecht komen, of wordt geopend geretourneerd, of komt nooit aan. Deze categorie datalekken vallen ook onder de meldplicht datalekken en moeten worden gemeld aan de AP en als er sprake is van een hoog risico voor Betrokkene ook aan de betrokkene. Met poststukken mogen verzonden e-mails gelijk gesteld worden. Deze gelijkstelling geldt ook voor digitaal in eventuele Mijn-omgevingen opgeslagen poststukken of e-mails.

Datalekken die in bulk gemeld kunnen worden zijn poststukken (brieven of e-mails) met (gevoelige) persoonsgegevens die bij grootschalige postverzending bij de verkeerde Ontvanger terecht komen en/of die geopend worden geretourneerd, of die nooit aankomen. Bij grootschalige postverzendingen voor Pensioenfondsen kan gedacht worden aan verzendacties op UPO, jaaropgave en informatie over het afkopen van pensioen.

Voor het in bulk melden van datalekken gelden de volgende voorwaarden:

- Het in bulk melden van datalekken gebeurt door een specifieke functionaris, zoals een FG of een privacy officer, binnen de organisatie.
- De functionaris die is belast met het doen van de bulkmeldingen beschikt over een overzicht van alle incidenten die in bulk zijn gemeld.

- Bij alle incidenten die in een bulkmelding worden gemeld gaat het om poststukken die inhoudelijk vergelijkbaar zijn, zodat gegevens zoals de aard van de persoonsgegevens en de mogelijke gevolgen voor de Betrokkenen in de melding correct kunnen worden weergegeven.
- De incidenten waarom het gaat worden uiterlijk op de overeenkomstige dag van de eerstvolgende kalendermaand na de dag van ontdekking gemeld aan de AP.

Verder wordt verwezen naar het document "Datalekken bij grootschalige postverzending" van de AP met datum 23 mei 2017.

9.6.4

Melding datalek aan de AP

Een datalek dat aan de AP gemeld moet worden, moet zonder onredelijke vertraging en, indien mogelijk, uiterlijk binnen 72 uur nadat het datalek is ontdekt door of namens de verwerkingsverantwoordelijke, worden gemeld. Onder ontdekt mag verstaan worden dat het datalek is vastgesteld.

De 72 uur-termijn is een doorlopende termijn die ingaat vanaf het moment van ontdekken c.q. vaststellen van het datalek door of namens de verwerkingsverantwoordelijke. Dit betekent dat het weekend en feestdagen binnen deze termijn vallen.

Mocht binnen die 72 uur nog niet alle informatie over het vastgestelde datalek bekend zijn dan wordt binnen die termijn alvast een melding bij de AP gedaan op grond van de op dat moment beschikbare informatie. Indien de informatie nadien compleet is, wordt een aanvullende melding aan de AP gedaan. Als het desondanks niet lukt om binnen de 72 uur te melden dient in de melding aan de AP het later melden te worden toegelicht.

De melding aan de AP gebeurt via een daartoe op de website van de AP voorzien digitaal meldingsformulier (zie <https://datalekken.autoriteitpersoonsgegevens.nl>)

9.6.5

Melding datalek aan Betrokkene

Een datalek dat aan Betrokkene gemeld moet worden, moet onverwijld aan de Betrokkenen worden gemeld.

Wat als 'onverwijld' moet worden aangemerkt zal afhangen van de omstandigheden van het geval. Daarbij moet rekening worden gehouden met het feit dat de Betrokkene tijdig in staat moet zijn gesteld maatregelen te nemen om de nadelige gevolgen van het datalek zo veel mogelijk te beperken of te voorkomen.

De melding aan Betrokkene is vormvrij en in beginsel persoonlijk. Dit kan schriftelijk, per e-mail dan wel telefonisch of in combinatie gebeuren.

9.7.1 Uitvoeren DPIA's

Het uitvoeren van een Gegevensbeschermingseffectbeoordeling (nader te noemen: DPIA) is vanuit artikel 35 AVG voorgeschreven, als de Verwerking een waarschijnlijk een hoog risico vormt voor de rechten en vrijheden van natuurlijke personen. Bij het uitvoeren van de DPIA moet worden beoordeeld wat het effect is van de Verwerking van Persoonsgegevens en waarbij de eventuele risico's worden gekwantificeerd. Deze beoordeling maakt onderdeel uit van de DPIA en moet uitgevoerd worden voordat er (systematisch) nieuwe Verwerkingen mogen plaatsvinden. De beoordeling moet voldoen aan de volgende vereisten:

- De beoogde Verwerkingen en de verwerkingsdoelen moeten systematisch worden beschreven.
- De doeleinden van de Verwerking moeten getoetst worden op de noodzaak en de evenredigheid van de Verwerking.
- De gesignaleerde risico's moeten worden beoordeeld op de mate waarin zij een inbreuk vormen op de rechten en vrijheden van Betrokkenen.
- De risico's moeten voorzien worden van beoogde maatregelen om de risico's te beperken tot het niveau waarmee kan worden aangetoond dat wordt voldaan aan de eisen uit de AVG.

Minimale vereisten bij het uitvoeren van DPIA's binnen de pensioensector.

Een DPIA is gebonden aan minimale vereisten, zoals vastgelegd in artikel 35 lid 7. Om hieraan in de praktijk een goede invulling aan te geven is het van belang om tenminste inzicht te hebben in:

- 1 Verschillende Persoonsgegevens die worden verwerkt.
- 2 Soorten Betrokkene van wie Persoonsgegevens worden verwerkt.
- 3 De classificatie naar type gegevens (regulier/ gevoelig/ bijzonder).
- 4 Rechtsgrond en doelbinding voor de Verwerking.
- 5 Systemen en processen waarbinnen de gegevens worden verwerkt.
- 6 Beveiliging van de gegevens, eventueel in samenhang met de classificatie van type gegevens.

Met behulp van het verkregen inzicht zal de Verwerkingsverantwoordelijke/ Verwerker moeten bepalen waar de belangrijkste risico's zitten op het gebied van Verwerking van Persoonsgegevens. Tevens moet worden vastgesteld of de risico's voldoende worden beheerst, met behulp van een eigen privacy-/ informatiebeveiligingsbeleid. Bij risico's die boven de risk appetite van de organisatie/ opdrachtgever uitkomen zullen aanvullende beheersmaatregelen getroffen moeten worden. Eventuele restrisico's moeten expliciet worden geaccepteerd. Tenslotte zal de volledige DPIA reproduceerbaar en reconstrueerbaar moeten zijn, onder meer door de vastlegging van de processtappen en de bijbehorende resultaten. In de uitgave 'Guidance verwerking persoonsgegevens pensioenfondsen' van de Pensioenfederatie wordt in paragraaf 9 ingegaan op het DPIA.

Als uit het DPIA blijkt dat er sprake is van een hoog risico, kan de DPIA ter consultatie worden voorgelegd aan de AP (artikel 36 AVG).

Er is een aantal organisaties dat werkzaamheden namens de Pensioenfondsen uitvoeren, maar er zijn ook organisaties die werken in de periferie van de pensioenfondsen. Hieronder volgt een overzicht van organisaties die nauw betrokken zijn bij de uitvoeren van pensioenregelingen en in hoeverre een DPIA moet worden uitgevoerd op basis van deze Gedragslijn:

Organisatie	Uitvoeren DPIA	Toelichting
Pensioenuitvoeringsorganisatie	Ja	Evenals een Pensioenfonds worden op grote schaal Persoonsgegevens verwerkt, waaronder ook gevoelige Persoonsgegevens.
Beroepsvereniging	Niet verplicht	In beginsel verwerkt een beroepsvereniging op een beperkte schaal Persoonsgegevens. Er zullen in beginsel geen bijzondere of gevoelige Persoonsgegevens worden verwerkt. Advies aan beroepsverenigingen is om vast te stellen dat er geen bijzondere of gevoelige Persoonsgegevens worden verwerkt.
Uitbestedingspartner voor o.a. pensioencommunicatie portaalbeheer	Ja	Als een Pensioenfonds haar (event)communicatie/portaalbeheer heeft uitbesteed, bestaat er een grote kans dat er op grote schaal Persoonsgegevens worden verwerkt. Ook is de kans groot dat er gevoelige Persoonsgegevens worden verwerkt. Mogelijk is er ook incidenteel sprake van het toepassen van nieuwe technologieën.
Incassobureau	Ja	Verwerkt gevoelige gegevens van Betrokkene, zoals informatie over de financiële positie, eventuele financiële problemen en mogelijk andere gegevens van zeer persoonlijke aard.
Juridisch adviesbureau	Niet verplicht	Een juridisch adviesbureau kan incidenteel te maken krijgen met het verwerken van Persoonsgegevens, soms ook van gevoelige aard. Gelet op de schaal waarmee deze gegevens naar verwachting verwerkt zullen worden, is een DPIA niet verplicht. Advies is wel om vast te stellen in welke gevallen en welke Persoonsgegevens incidenteel verwerkt kunnen worden.

9.8.1

Aanwijzing van een Functionaris (Functionaris)

Het Pensioenfonds of de Pensioenuitvoeringsorganisatie zijn (eind)verantwoordelijk voor een zorgvuldige en juiste naleving van de privacy wet- en regelgeving, in het bijzonder de AVG.

Een FG kan voor het Pensioenfonds of de Pensioenuitvoeringsorganisatie een centrale rol vervullen en de sleutelfiguur zijn om naleving van de bepalingen van de AVG mogelijk te maken.

In de uitgave 'Guidance verwerking persoonsgegevens pensioenfondsen' van de Pensioenfederatie zijn onder paragraaf 11 overwegingen en scenario's opgenomen op grond waarvan het Pensioenfonds of de Pensioenuitvoeringsorganisatie kunnen bepalen of zij al dan niet een FG zullen aanwijzen.

FG's zijn niet persoonlijk verantwoordelijk wanneer de AVG niet nageleefd wordt. Het zijn het Pensioenfonds of de Pensioenuitvoeringsorganisatie zelf die verantwoordelijk zijn en die erop toe dienen te zien en moeten kunnen aantonen dat de verwerking van persoonsgegevens aan de voorwaarden voldoet.

De functie van FG kan ook vervuld worden op basis van een servicecontract met een natuurlijk persoon of organisatie buiten de organisatie van het Pensioenfonds of de Pensioenuitvoeringsorganisatie. In het laatste geval is het essentieel dat elk lid van de organisatie die de taken van een FG vervult aan alle relevante vereisten van de AVG voldoet.

De FG heeft een geheimhoudings- of vertrouwelijkheidsplicht bij de uitoefening van zijn taken.

9.8.1.1

Vanuit elke vestiging makkelijk te contacteren

Het is essentieel dat de FG persoonlijk beschikbaar is.

9.8.1.2

Deskundigheid en vaardigheden van de FG

Het vereiste kennisniveau dient te passen bij de gevoeligheid, complexiteit en de hoeveelheid gegevens die een organisatie verwerkt. De FG dient voldoende inzicht te hebben in de uitgevoerde gegevensverwerkingen en de informatie-systemen en de behoeften van de verantwoordelijke op het gebied van veiligheid van gegevens en gegevensbescherming.

Het vermogen de taken te vervullen die bij de positie van FG horen moet worden opgevat als persoonlijke kwaliteiten (integriteit) en kennis van de FG, maar heeft ook te maken met de positie van de FG binnen de organisatie. De belangrijkste taak van de FG is te zorgen dat de AVG nageleefd wordt. Hij speelt een belangrijke rol in het creëren van een gegevensbeschermingscultuur binnen de organisatie. En hij helpt ook met de implementatie van de verplichtingen uit de AVG.

9.8.1.3

Publicatie en communicatie van de contactgegevens van de FG

Waar het om gaat, is dat de Betrokkenen en toezichthouder gemakkelijk, direct en vertrouwelijk contact met de FG op kunnen nemen. De contactgegevens van de FG dienen informatie te bevatten die betrokkenen en toezichthouder in staat stellen de FG gemakkelijk te bereiken (postadres, een speciaal telefoonnummer, een speciaal e-mailadres of contactformulier).

9.8.2.1

Betrokkenheid van de FG bij alle aangelegenheden die de bescherming van persoonsgegevens betreffen

Om de Functionaris zo vroeg mogelijk bij alle privacy gerelateerde aangelegenheden te betrekken dienen het Pensioenfonds of de Pensioenuitvoeringsorganisatie er bijvoorbeeld op toe te zien dat:

- de FG wordt uitgenodigd voor managementvergaderingen waar beslissingen met gevolgen voor gegevensbescherming worden genomen;
- indien de FG om advies gevraagd wordt deze alle relevante informatie wordt verstrekt die hem in staat stellen passend advies te geven;
- aan de mening van de FG altijd passende waarde wordt gehecht;
- de FG onmiddellijk geraadpleegd wordt indien zich een datalek of ander privacy incident heeft voorgedaan.

9.8.2.2

Benodigde middelen

Het ter beschikking stellen van de benodigde middelen betekent:

- actieve ondersteuning van de functie van de FG door het management;
- voldoende tijd voor de FG om zijn taken te vervullen.
- voldoende steun qua financiële middelen, infrastructuur (terrein, faciliteiten, apparatuur) en, waar nodig, personeel;
- communicatie over de aanwijzing van de FG naar alle medewerkers;
- toegang tot andere diensten, zoals personeelszaken, de juridische afdeling, de ICT-afdeling, de beveiliging enz., zodat de FG van die andere afdelingen de essentiële steun, input en informatie ontvangt;
- FG's dienen middels doorlopende training de kans te krijgen bij te blijven op het gebied van gegevensbescherming; en
- op basis van grootte en structuur van de organisatie eventueel aanstellen van een FG-team.

9.8.2.3

Onafhankelijk handelen

Om er voor te zorgen dat de Functionaris onafhankelijk kan functioneren, dienen Pensioenfondsen:

- erop toe te zien dat de Functionaris geen instructies ontvangt met betrekking tot de uitvoering van taken;
- de Functionaris in staat te stellen zijn taken onafhankelijk te vervullen;
- bij het nemen van beslissingen die niet aan de AVG voldoen en die niet met het advies van de Functionaris overeenkomen, de Functionaris in de gelegenheid te stellen zijn afwijkende mening duidelijk te maken aan diegenen die de beslissingen nemen.

9.8.3.2

De rol van de FG in een DPIA

Pensioenfondsen dienen advies vragen aan de Functionaris inzake een DPIA over:

- o of er al of niet een DPIA uitgevoerd moet worden;
- o welke methodiek voor de DPIA gebruikt moet worden;
- o of de DPIA intern uitgevoerd of uitbesteed moet worden;
- welke waarborgen (zoals technische en organisatorische maatregelen) ingebouwd moeten worden om eventuele risico's voor de rechten en belangen van de Betrokkenen te beperken; en
- of de DPIA correct uitgevoerd is en de conclusies daaruit (de vraag of de Verwerking door moet gaan en welke waarborgen er ingebouwd moeten worden) aan de AVG voldoen.

Indien het Pensioenfonds of de Pensioenuitvoeringsorganisatie het niet met het advies van de FG eens zijn, dient in de documentatie van de DPIA specifiek schriftelijk aangegeven te worden waarom het advies niet overgenomen is.

9.8.3.4

De rol van de FG in het voeren van een administratie

In de praktijk zal het vaak de FG zijn die dit (verwerkings)register bijhoudt, op basis van input uit de organisatie. Ook omdat dit een middel is dat de FG in staat stelt zijn taak te vervullen om op naleving toe te zien en het Pensioenfonds of de Pensioenuitvoeringsorganisatie te informeren en te adviseren. Het register geeft een overzicht van alle Verwerkingen van Persoonsgegevens die een organisatie uitvoert en is daarmee een passend verantwoordingsmiddel naar de AP.

9.9.1.1

Doorgifte op basis van een adequaatheidsbesluit

De Europese Commissie heeft een twaalftal adequaatheidsbeslissingen aangenomen, waaronder ten aanzien van Nieuw-Zeeland, Zwitserland en Canada (behalve Quebec).

De AP geeft aan dat Privacy Shield voor doorgifte naar de Verenigde Staten ongeldig verklaard is. De AP verwijst naar de European Data Protection Board (EDPB) voor guidance naar aanleiding van Schrems II.

¹⁴ http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

De lijst met landen en organisaties die bij besluit een passend beschermingsniveau zijn toegekend, wordt door de EC bekend gemaakt in het Publicatieblad van de EU en op haar [website](#).¹⁴

9.9.1.3

Doorgifte in afwijkende situaties

Pensioenfondsen verwerken in beginsel geen Persoonsgegevens buiten de EER. Indien doorgifte buiten de EER echter toch noodzakelijk is, dan is het advies om te kiezen voor de opties beschreven in 9.9.1.1. en 9.9.1.2. Indien het Pensioenfonds hier geen mogelijkheid toe ziet dan hebben de opties 1 en 7 van 9.9.1.3 de voorkeur.

Dit kan onder andere voorkomen in geval van cloud toepassingen of indien het Pensioenfonds internationaal opereert of in geval van verstrekking van gegevens in strafrechtelijke zaken.

11 Naleving van de Gedragslijn

11.1 Maatregelen

Jaarlijks stelt het Pensioenfonds vast of de Gedragslijn in voldoende mate is nageleefd. Er zijn verschillende manieren om dit vast te stellen, bijvoorbeeld door:

- Interne rapportages of rapportages van derden (waaronder van de Pensioenuitvoeringsorganisatie), zoals kwartaalrapportages en privacyrapportages;
- Een externe partij of een onafhankelijke interne functionaris, die door het Pensioenfonds is aangewezen, opdracht te geven te beoordelen of de Gedragslijn in voldoende mate is nageleefd. De opdrachtverstrekking wordt mede geformuleerd op basis van de Gedragslijn;
- Interne controle methodes: Een Pensioenfonds kan eigen interne controle methodes en/of audit standaarden inzetten om de naleving van de Gedragslijn te toetsen. Daarbij kan worden gekeken naar het totaal aan controle methodes en in hoeverre deze sluiten bij de reikwijdte van de Gedragslijn en gaat eventueel vergezeld van een onafhankelijke opinie door bijvoorbeeld de interne of externe accountant.

Informatie die gebruikt kan worden voor de jaarlijkse verantwoording betreft onder andere:

- Standaard 3402- en Standaard 3000-rapportages;
- ISO certificatie, informatie beveiliging en soortgelijke verklaringen;
- Compliance statement als onderdeel van het in control statement;
- Control Framework met key risks en key controls op het gebied van privacy en informatiebeveiliging.

11.2 Verantwoording

Het Pensioenfonds verantwoordt zich jaarlijks of de Gedragslijn in voldoende mate is nageleefd. De vorm waarin verantwoording wordt afgelegd is vormvrij en wordt bepaald door het Pensioenfonds.

Bijlage Verwerkingsverantwoordelijke of Verwerker?

Bent u verwerkingsverantwoordelijke of verwerker?

