Incidenten- en klokkenluidersregeling

SBZ Pensioen[1]

Vastgesteld in de bestuursvergadering van 14 december 2020

Versie 2021

Inhoud Incidenten- en klokkenluidersregeling SBZ Pensioen

[1] SBZ Pensioen is een handelsnaam van Stichting Bedrijfstakpensioenfonds Zorgverzekeraars kvk 41178751

Incidenten- en klokkenluidersregeling SBZ Pensioen

Aanleiding en doel

SBZ Pensioen (verder te noemen: het fonds) ziet de goede reputatie en integriteit van haar organisatie als een belangrijk vereiste om succesvol te opereren als pensioenfonds. Incidenten kunnen een gevaar vormen voor de integere en beheerste bedrijfsvoering van het fonds. Het doel van de Incidenten- en klokkenluidersregeling is om te regelen op welke wijze incidenten worden geconstateerd, gemeld, vastgelegd en aanleiding zijn voor het nemen van corrigerende maatregelen. Daarnaast geeft de Incidenten- en klokkenluidersregeling elke verbonden persoon van het fonds de gelegenheid om een misstand, al dan niet anoniem te melden, zodat al het nodige gedaan kan worden in het geval van mogelijke overtredingen van interne of externe regelgeving of andere misstanden.

1. Definities

1.1 Verbonden persoon:
- de leden van het Bestuur;
- sleutelfunctiehouders;
- de leden van het Verantwoordingsorgaan;
- externe leden van commissies;
- het Bestuur kan andere (groepen van) personen als verbonden persoon aanwijzen; Medewerkers van uitbestedingspartners zijn geen verbonden personen, tenzij deze op basis van het voorgaande punt van dit artikel wel als zodanig door het Bestuur zijn aangewezen.

1.2 Melder: Ieder (rechts)persoon die werkzaamheden verricht voor, dan wel betrokken is bij het fonds (dit met inbegrip van de verbonden personen).

1.3 Meldpunt operationele incidenten: het Bestuur heeft de bestuursondersteuning aangewezen als meldpunt.

1.4 Meldpunt integriteitsincidenten en misstanden: de voorzitter van de Audit-, Risk- en Compliancecommissie. Indien de melding betrekking heeft op de voorzitter van de Audit-, Risk- en Compliancecommissie, dan fungeert de voorzitter van het Bestuur als meldpunt.

1.5 Vertrouwenspersoon: degene die is aangewezen om als zodanig voor de organisatie van SBZ Pensioen te fungeren (mevrouw A. Pierik, bereikbaar via pierik@compliance-instituut.nl, 088 99 88 100 of 06 83 59 98 47)

1.6 Incident: gedraging of gebeurtenis die een ernstig gevaar vormt of kan vormen voor de beheerste en integere uitoefening van het bedrijf van het fonds, en/of een gebeurtenis waarbij directe of indirecte financiële schade ontstaat door toereikende of falende interne processen, verbonden personen of systemen of door externe gebeurtenissen, dan wel een datalek zoals gedefinieerd in de Algemene Verordening Gegevensbescherming.

Er wordt onderscheid gemaakt tussen operationele incidenten en integriteitsincidenten.

1.7 Operationeel incident: een incident dat plaats heeft gevonden in de dagelijkse uitvoering van de werkzaamheden door het fonds en waarbij er een inbreuk is geweest op de beheerste bedrijfsvoering.

1.8 Integriteitsincident: alle incidenten die niet als operationeel incident kwalificeren. Dit is in ieder geval als de gedraging of gebeurtenis:

a. een strafbaar feit oplevert,

b. een schending inhoudt van interne of externe regelgeving of beleidsregels, waaronder de gedragscode,

c. autoriteiten of personen die belast zijn met de uitvoering van of het toezicht de naleving van wettelijke regelingen, of wettelijke opsporingsambtenaren beoogt te misleiden,

d. beoogt dat informatie over de hiervoor genoemde feiten wordt achtergehouden,

e. op enigerlei wijze direct of indirect de goede naam van het fonds kan schaden, of

f. een ernstig gevaar vormt voor de integere bedrijfsvoering van het fonds, hieronder vallen ook de zogenoemde datalekken zoals beschreven in artikel 33 en 34 AVG. Ten aanzien van datalekken en het operationele en urgente karakter van een datalek is bijlage -1- aan deze regeling toegevoegd.

1.9 Misstand: een integriteitsincident, waarbij het maatschappelijk belang in het geding is bij de schending van een wettelijk voorschrift, een gevaar voor de volksgezondheid, een gevaar voor de veiligheid van personen, een gevaar voor de aantasting van het milieu of een gevaar voor het goed functioneren van het fonds als gevolg van een onbehoorlijke wijze van handelen of nalaten.

2. Algemeen

2.1 Het bestuur van het fonds zal ervoor zorgdragen dat de Incidenten- en klokkenluidersregeling bekend is bij alle hierboven genoemde personen.

2.2 De Audit-, Risk- en Compliancecommissie is belast met het toezicht op de naleving van deze regeling.Het Uitvoerend Bestuur behandelt het incident en rapporteert over de voortgang aan de voorzitter van de Audit-, Risk- en Compliancecommissie. Een incident wordt vertrouwelijk en met grote zorgvuldigheid behandeld.

2.3 De Vertrouwenspersoon kan benaderd worden met vermoedens en/of twijfels en treedt in eerste instantie raadgevend op. De Vertrouwenspersoon houdt gesprekken vertrouwelijk en onderneemt geen actie, tenzij hij hier in rechte toe is verplicht of dit door de Melder wordt gevraagd. De Vertrouwenspersoon rapporteert jaarlijks aan het Bestuur omtrent het aantal gesprekken en de gemaakte uren. Over de inhoud wordt geen informatie aan derden gedeeld, ook niet aan het Bestuur en aan de compliance officer.

2.4 Het Meldpunt ontvangt de meldingen en beoordeelt of het een incident betreft in de zin van deze regeling.

2.5 Indien het Meldpunt zich onbevoegd acht vanwege de aard van de melding dan verwijst hij de Melder door naar het bevoegde Meldpunt.

2.6 Indien het Meldpunt melding krijgt van een integriteitsincident of misstand dan verwijst hij de Melder op de beschikbaarheid en de rol van de Vertrouwenspersoon.

3. Incidenten

3.1 Iedere verbonden persoon die een (dreigend) incident constateert is gehouden dit te melden aan het Meldpunt. Een incident kan zowel schriftelijk, elektronisch als mondeling worden gemeld. De Melder krijgt hiervan een bevestiging. Meldingen kunnen ook anoniem worden gedaan.

3.2 De verbonden persoon kan het vermoeden van een integriteitsincident of misstand melden via de Vertrouwenspersoon. De Vertrouwenspersoon stuurt de Melding, overleg met de verbonden persoon, door naar het Meldpunt waarbij de naam van de verbonden persoon alleen bij de Vertrouwenspersoon bekend is.

3.2 Het Meldpunt zal een voorlopig onderzoek uitvoeren, zodra hij een melding van een Melder heeft ontvangen. Daar waar van toepassing zal de Meldpunt en Melder gezamenlijk de melding verder afwikkelen, dit geldt met name bij toezichtrelevante meldingen (DNB, AFM, ACM en AP).

3.3 Het Meldpunt zal een binnengekomen melding met het Bestuur bespreken.

3.4 Het Meldpunt zal het Bestuur adviseren de melding terzijde te leggen als uit zijn onderzoek geen grond blijkt voor de melding. Als het voorlopig onderzoek serieuze indicaties geeft van mogelijke schending van interne of externe regelgeving of andere onregelmatigheden, dan zal het Bestuur de klacht nader laten onderzoeken.

3.5 De Melder ontvangt algemene informatie over de voortgang van het onderzoek (en de uitkomst).

4. Onderzoek

4.1 Indien van toepassing kan het Meldpunt een onderzoek instellen. Het doel van het onderzoek is:

a. waarheidsvinding met betrekking tot het Incident en de daarmee samenhangende bewijsvoering voor disciplinaire, civielrechtelijke en strafrechtelijke vervolgstappen;
b. het beperken van de (potentiële) schade naar een beheersbaar niveau; en
c. het herstel van de bedrijfsvoering, voor zover het Incident daarop enige invloed had.

4.2 Het onderzoek naar het Incident wordt uitgevoerd in opdracht van het Meldpunt, of het Bestuur in haar plaats, door interne en/of externe deskundigen. Als de melding betrekking heeft op een Incident bij een partij aan wie werkzaamheden zijn uitbesteed, wordt het onderzoek verricht in overleg met of door deze partij. Indien van toepassing wordt een onderzoeksprotocol opgesteld.

4.3 Het onderzoek wordt uitgevoerd onder de volgende voorwaarden:
a. De beginselen van de AVG worden in acht genomen;
b. Gegevens worden rechtmatig en proportioneel verzameld, van onrechtmatig verkregen gegevens wordt geen gebruik gemaakt;
c. Degene naar wie onderzoek wordt gedaan, wordt direct geïnformeerd tenzij dit in het belang van het onderzoek niet gewenst is;
d. De gegevens worden zodanig vastgelegd dat hoor en wederhoor kan plaatsvinden, tenzij in redelijkheid kan worden aangenomen dat dit schadelijk kan zijn voor het onderzoek;
e. De Onderzoekers stellen de Melder in de gelegenheid te worden gehoord eventueel door tussenkomst van de Vertrouwenspersoon. De Onderzoekers dragen zorg voor een schriftelijke vastlegging hiervan;
f. De Onderzoekers kunnen ook anderen horen. De Onderzoekers dragen zorg voor een schriftelijke vastlegging hiervan.

4.4 De onderzoekers rapporteren de onderzoeksresultaten aan het Meldpunt en haar opdrachtgever. De rapportage bevat een kort relaas van feiten en omstandigheden en indien vastgesteld is dat sprake is van een Incident de bewijsvoering daarvoor in hoofdlijnen en een advies met betrekking tot de te nemen maatregel(en).

4.5 Alle betrokkenen waarborgen een vertrouwelijke behandeling van de melding en het onderzoek. Informatie mag niet gedeeld worden tenzij dit op grond van de wet of dit beleid noodzakelijk is.

4.6 Het traject tussen melding en afronding onderzoek duurt maximaal 6 weken. Indien deze termijn wordt overschreden worden betrokken partijen geïnformeerd en wordt de motivatie voor overschrijding van deze termijn vastgelegd.

5. Standpunt Bestuur en maatregelen

5.1 Het Bestuur neemt op basis van het onderzoeksrapport een standpunt in. Indien het standpunt afwijkt van de conclusies en aanbevelingen van de Onderzoekers, dan onderbouwt zij haar standpunt.

5.2 Op basis van de onderzoeksresultaten beoordeelt het Bestuur en besluit ten aanzien van de volgende punten:
- Arbeidsrechtelijke of disciplinaire maatregelen jegens betrokken verbonden personen
- Civielrechtelijke maatregelen, zoals regres
- Interne en externe communicatie
- Aanpassing procedures
- Overige maatregelen voor het herstel van de bedrijfsvoering

- Melding aan de toezichthouder(s).

Indien het Incident betrekking heeft op één van de Bestuursleden, dan wordt door de overige bestuursleden besloten over de te nemen maatregel(en) zoals hiervoor aangegeven.

5.3 Indien een Integriteitsincident veroorzaakt is door een Verbonden persoon, wordt bij het bepalen van de maatregel(en) en sancties in overweging genomen dat het veroorzaken van incidenten als een ernstige schending wordt beschouwd van de vertrouwensrelatie tussen het fonds enerzijds en de verbonden (rechts)persoon anderzijds.

5.4 Het veroorzaken van een incident of anderszins daarbij betrokken zijn, kan leiden tot ontheffing uit de functie die de verbonden persoon bij het fonds vervult. In geval sprake is van opzettelijk en ernstige strafbare overtredingen, zoals misdrijven als genoemd in het Wetboek van Strafrecht en de Wet Economische Delicten, wordt in beginsel aangifte gedaan bij justitie of politie.

5.5 De voorzitter van de Audit-, Risk- en Compliancecommissie ziet toe op de implementatie en naleving van nieuwe procedures en maatregelen, die naar aanleiding van het incident getroffen zijn. De Audit-, Risk- en Compliancecommissie ziet toe op de implementatie en naleving van het geheel, wordt door de voorzitter op de hoogte gehouden van de verschillende incidenten en ondersteunt met advies.

6. Externe melding

6.1 Na het doen van een interne Melding van een vermoeden van een misstand, kan de Melder ook direct een externe Melding doen indien:

a. de Melding niet-ontvankelijk is verklaard en de Melder zich niet in de motivatie hiervan kan vinden;
b. de Melder zich benadeelt voelt naar aanleiding van de melding;
c. de voorgeschreven termijnen worden overschreden zonder bericht waarom deze in redelijkheid worden overschreden;
d. een eerdere melding de Misstand niet heeft weggenomen;
e. indien het eerst doen van een interne Melding in redelijkheid niet van hem kan worden gevraagd.

6.2 De Melder kan de externe Melding doen bij een instantie die daarvoor naar het redelijk oordeel van de Melder het meest in aanmerking komt en naar het oordeel van de Melder mogelijk actie tegen de Misstand kan ondernemen. Dit betreft bijvoorbeeld politie, justitie, toezichthouder of het Huis voor Klokkenluiders.

7. Bescherming van de Melder tegen benadeling

7.1 Het fonds zal de Melder niet benadelen in verband met het te goeder trouw en naar behoren melden van een vermoeden van een integriteitsincident bij het fonds of een externe instantie.

7.2 Van benadeling als bedoeld in 7.1 is ook sprake als een redelijke grond aanwezig is om de Melder aan te spreken op zijn functioneren of een benadelende maatregel als bedoeld in lid 2 jegens hem te nemen, maar de maatregel die het fonds neemt niet in redelijke verhouding staat tot die grond.

7.3 Indien het fonds jegens de Melder binnen afzienbare tijd na het doen van een melding overgaat tot het nemen van een benadelende maatregel als bedoeld in 7.2 motiveert het waarom het deze maatregel nodig acht en dat deze maatregel geen verband houdt met het te goeder trouw en naar behoren melden van een vermoeden van een integriteitsincident.

7.4 Het fonds draagt er zorg voor dat leidinggevenden en collega's van de Melder zich onthouden van iedere vorm van benadeling in verband met het te goeder trouw en naar behoren melden van een

vermoeden van een integriteitsincident, die het professioneel of persoonlijk functioneren van de Melder belemmert.

7.5 Het fonds spreekt verbonden persoons die zich schuldig maken aan benadeling van de Melder daarop aan en kan hen een waarschuwing of een disciplinaire maatregel opleggen.

7.6 In geval de Melder de melding intrekt, vergewissen de onderzoekers zich ervan dat de intrekking niet onder invloed van dreigementen of door omkoping heeft plaatsgevonden**.**

8. Bescherming van andere betrokkenen tegen benadeling

Het fonds zal de Vertrouwenspersoon en de onderzoekers niet benadelen vanwege het uitoefenen van de in deze regeling beschreven taken. Bovendien zal het fonds geen verbonden persoon benadelen die wordt gehoord of die documenten verstrekt in het kader van een onderzoek.

9. Registratie

Het Meldpunt houdt door middel van een incidentenregister een registratie bij van alle binnengekomen meldingen, de wijze van opvolging, ingestelde onderzoeken, onderzoeksresultaten, de genomen preventieve en repressieve maatregelen en de meldingen aan de relevante toezichthouder(s).

10. Melden aan toezichthouders

Ernstige incidenten worden onverwijld en tijdig door de voorzitter aan de relevante toezichthouder(s) gemeld onder opgaaf van de feiten en omstandigheden van het incident, alsmede de informatie over de functie, de hoedanigheid en de positie van de betrokken (rechts)perso(o)n(en) die verantwoordelijk is/zijn voor het ontstane incident.

De voorzitter informeert de relevante toezichthouder(s) tevens over de maatregelen die naar aanleiding van het incident zijn genomen of nog zullen worden genomen**.**

Ondertekening

Utrecht, 14 december 2020

Namens het Bestuur van SBZ Pensioen

Ties Tiessen
Onafhankelijk voorzitter

Jobert Koomans
Uitvoerend Bestuurslid Pensioenen en Risicobeheer

Bijlage -1- (Procedure Datalekken)

Met ingang van 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) in werking getreden. Sindsdien geldt een meldplicht voor datalekken. Deze meldplicht houdt in dat het fonds Datalekken onverwijld moeten melden aan:

- de Autoriteit Persoonsgegevens (AP),
- in bepaalde gevallen aan De Nederlandsche Bank[2], en
- in bepaalde gevallen aan de betrokkene(n).

In het geval dat het incident niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens, is er geen sprake van een Datalek maar van een beveiligingsincident. Melding aan de AP is dan niet nodig, het beveiligingsincident dient echter wel opgenomen te worden in het incidentenregister net als alle datalekken.

Deze procedure beschrijft hoe te handelen binnen het fonds indien er sprake is van:

- een datalek of wanneer een datalek vermoed wordt,
- een datalek bij een verbonden persoon,
- een datalek bij een derde, bijvoorbeeld een verwerker van persoonsgegevens van het fonds.

De procedure is mede gebaseerd op de beleidsregels van de AP inzake de meldplicht datalekken in de AVG.

Per gemeld datalek wil het fonds zich de vrijheid voorbehouden om te beoordelen of de procedure gevolgd kan worden, dan wel afwijking van deze procedure gerechtvaardigd is.

1. Identificeren datalek

Met verbonden personen en derde (PUO) is afgesproken om zonder onnodige vertraging, doch uiterlijk binnen 48 uur nadat de verbonden persoon of derde (PUO) een (mogelijk) datalek heeft geconstateerd het Meldpunt bij het fonds hiervan in kennis te stellen. Het Meldpunt stelt de Functionaris voor de Gegevensbescherming (FG) direct op de hoogte van de melding.

Daarnaast informeert de verbonden persoon of derde (PUO) het fonds zo mogelijk niet later dan 48 uur nadat het (mogelijk) datalek is geconstateerd accuraat over:

a. de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van Persoonsgegevens en (kring van) de betrokkenen;
b. de maatregelen die de derde (PUO) heeft getroffen of voorstelt te treffen om de (negatieve) gevolgen van de inbreuk te beperken en te verhelpen.
c. desgevraagd aanvullende gegevens die het fonds nodig heeft om een eventuele melding bij de toezichthouder te kunnen verrichten.

2. Beoordeling datalek ja/nee

Op basis van de verkregen informatie en bij vermoeden van een datalek wordt door het dagelijks bestuur zo spoedig mogelijk de beoordeling gemaakt of er daadwerkelijk sprake is van een Datalek, hierbij wordt tevens advies van de FG ingewonnen. De beoordeling of er sprake is van een incident, dat gemeld moet worden aan de AP komt tot stand met behulp van de WP29 guidelines on data breach notification (6 februari 2018).

Tevens wordt beoordeeld of er per direct maatregelen genomen moeten worden om de schade te beperken, waaronder het doen van een (voorlopige) melding aan betrokkenen.
In geval dat het incident niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens is er geen sprake van een datalek maar van een beveiligingsincident. Melding aan de AP is dan niet nodig. Wel overlegt het dagelijks bestuur dan of het zinvol is om het beveiligingsincident te onderzoeken om herhaling te voorkomen.

3. Melden aan de Autoriteit Persoonsgegevens

Het dagelijks bestuur verzorgt de tijdige (onverwijld, zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek) elektronische melding bij de AP volgens het online meldingsformulier van de AP. Het dagelijks bestuur fungeert als contactpersoon inzake de communicatie naar de AP. Dit geldt ook in geval nog niet duidelijk is dat het incident een datalek is. Dan is de mogelijkheid aanwezig om na vaststelling van de aard van het incident de melding aan te vullen dan wel in te trekken.

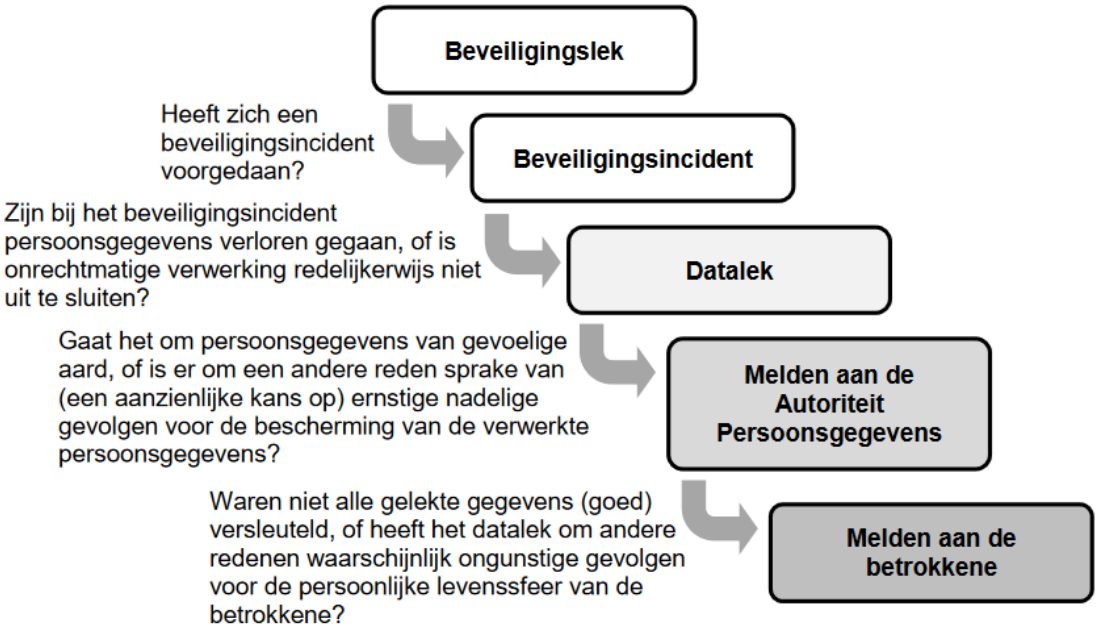
Indien de concrete situatie zich daartoe leent, zal het dagelijks bestuur aan de derde (PUO) vragen de melding aan de Autoriteit Persoonsgegevens te doen en het dagelijks bestuur op de hoogte te houden van de melding[3].

[2] Pensioenfondsen zijn gehouden toezichtincidenten te melden bij DNB. Het gaat om incidenten die het vertrouwen in het pensioenfonds of financiële markten kunnen schaden. Daaronder vallen ook IT-incidenten waarbij bijvoorbeeld persoonlijke informatie van deelnemers uitlekt door een beveiligingslek.

[3] Deze clausule geldt alleen voor uitvoerders

4. Beoordeling of datalek gemeld dient te worden aan betrokkene(n)

Het dagelijks bestuur stelt vast of het datalek ook moeten worden gemeld aan degenen om wiens gegevens het gaat. Het dagelijks bestuur maakt hierbij gebruik van de WP29 guidelines on data breach notification (6 februari 2018) en het advies van de FG. Schematische weergave van deze guideline is onderstaand opgenomen.



5. Oorzaken en verbetermaatregelen

De verbonden persoon of derde (PUO) is verplicht om bij constatering van een datalek, in goed overleg met het fonds, voor eigen rekening en risico alle noodzakelijke maatregelen te nemen om het datalek te dichten en de schade die hieruit voortvloeit of kan vloeien te beperken. De verbonden persoon of derde (PUO) zal het fonds volledig op de hoogte houden en blijven houden van de ontwikkelingen met betrekking tot een datalek en de genomen of te nemen maatregelen om de gevolgen hiervan te beperken en herhaling te voorkomen.

Het dagelijks bestuur zal aan de hand van de ontvangen informatie beoordelen of het noodzakelijk is aan de verbonden persoon of derde (PUO) te vragen bepaalde aanvullende beveiligingsmaatregelen te treffen. Het dagelijks bestuur bewaakt de voortgang ten aanzien van eventuele aanvullende beveiligingsmaatregelen.

6. Registratie

Het Meldpunt houdt een registratie bij van alle beveiligingsincidenten en datalekken binnen het fonds.
De derde (PUO) houdt tevens een registratie bij van ieder datalek bij de derde (PUO) en verstrekt deze periodiek aan het fonds.

Definities behorende bij bijlage -1-

AP
Autoriteit Persoonsgegevens, v/h College Bescherming Persoonsgegevens (CBP).

AVG en UAVG
Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

Betrokkene
Degene op wie een persoonsgegeven betrekking heeft (artikel 1f, Wbp).

BeveiligingsIncident
Een mogelijk beveiligingsincident, waardoor de bescherming van persoonsgegevens op enig moment is doorbroken en waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Het is daarbij niet van belang of de verantwoordelijke passende technische of organisatorische beschermingsmaatregelen heeft getroffen of niet. Ieder datalek is een incident, niet ieder incident is een datalek.

Datalek
Een inbreuk op de beveiliging (zoals bedoeld in artikel 33 en 34, AVG) waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking; dus blootgesteld aan datgene waartegen beveiligingsmaatregelen (artikel 5 onder f, AVG) bescherming moesten bieden.

Persoonsgegeven
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4, AVG).

PUO
Pensioenuitvoeringsorganisatie (verwerker).

Verwerker
Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen (artikel 4 AVG). De PUO is in veel gevallen een verwerker.

Verwerkingsverantwoordelijke
De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4, AVG). Het fonds is de verwerkingsverantwoordelijke.

Verwerking van persoonsgegevens
Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 4, AVG).