Regeling Incidenten

SBZ Pensioen[1]

Vastgesteld in de bestuursvergadering van 10 februari 2020

Versie 2020

Inhoud Regeling Incidenten SBZ Pensioen

Aanleiding en doel		1
1.	Definities	1
2.	Algemeen	1
3.	Incidenten	2
4.	Uitkomst onderzoek	2
5.	Maatregelen	2
6.	Registratie	2
7.	Melden aan toezichthouders	2
Ondertekening		3
Bijlage -1- (Procedure Datalekken)		4

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

Regeling incidenten 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. Het doel van de regeling is om te regelen op welke wijze incidenten, worden geconstateerd, gemeld, vastgelegd en aanleiding zijn voor het nemen van corrigerende maatregelen en daarnaast om elke verbonden persoon van het fonds de gelegenheid te geven 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 (rechts)persoon:
- De leden van het bestuur;
- de leden van het verantwoordingsorgaan;
- alle medewerkers van het fonds, onafhankelijk van de duur waarvoor of de juridische basis waarop zij werkzaam zijn; De regeling geldt derhalve ook voor personen werkzaam op oproepbasis en voor adviseurs in de BeleggingsAdviescommissie;
- degenen die voor het fonds werkzaamheden verrichten maar niet bij het fonds in dienst zijn;
- andere (categorieën) personen aangewezen door het bestuur van het fonds;
- uitbestedingpartners en overige dienstverleners .

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 Toezicht en meldpunt: De voorzitter van de Audit-, Risk- en Compliancecommissie is belast met het toezicht op de naleving van deze regeling, de voorzitter kan een (operationeel) Meldpunt aanwijzen. Het bestuur heeft bestuursondersteuning in het kader van deze regeling aangewezen als operationeel Meldpunt.

1.4 Incident: gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van het fonds met inbegrip van de bij het fonds betrokken (rechts)personen dat:

a. een strafbaar feit oplevert,

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

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. Deze bijlage bevat de operationele procedure waarlangs het fonds werkt in geval van een datalek.

2. Algemeen

2.1 Het bestuur van het fonds zal ervoor zorgdragen dat de Regeling Incidenten bekend is bij alle hierboven genoemde (rechts)personen.

2.2 De voorzitter van de Audit-, Risk- en compliancecommissie is belast met het toezicht op de naleving van deze regeling en de behandeling van het incident. Een incident wordt vertrouwelijk en met grote zorgvuldigheid behandeld.

2.3 Het bestuur heeft bestuursondersteuning in het kader van deze regeling aangewezen als Meldpunt.

2.4 Het Meldpunt ontvangt de meldingen en voert een voorlopig onderzoek uit. Daarbij kan het Meldpunt zich door derden (waaronder de melder) laten ondersteunen.

3. Incidenten

3.1 Een incident dient, bij voorkeur schriftelijk, te worden gemeld bij het Meldpunt. De Melder krijgt hiervan een bevestiging.

3.2 Het Meldpunt zal een voorlopig onderzoek uitvoeren, zodra hij een melding van een Melder heeft ontvangen. Daar waarvan 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. Uitkomst onderzoek

Het Meldpunt rapporteert de onderzoeksresultaten aan het bestuur. De rapportage bevat een kort relaas van feiten en omstandigheden, de bewijsvoering in hoofdlijnen, de eventuele (tijdkritische) melding aan toezichthouders, alsmede het advies met betrekking tot de te nemen maatregel(en).

5. Maatregelen

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).

Het uitgangspunt bij het bepalen van het soort maatregel(en) en sancties is dat het veroorzaken van incidenten als een ernstige schending wordt beschouwd van de vertrouwensrelatie tussen het fonds enerzijds en de verbonden (rechts)persoon anderzijds.

Het veroorzaken van een incident of anderszins daarbij betrokken zijn, kan leiden tot arbeidsrechtelijke maatregelen, waaronder ontslag op staande voet. 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.

De voorzitter 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. 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).

De voorzitter informeert de compliance officer over het ingestelde onderzoek, de onderzoeksresultaten en de genomen preventieve en repressieve maatregelen.

7. 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**.**

8. Slot bepaling

Indien de melding de voorzitter betreft zal de plaatsvervangend voorzitter in het kader van deze regeling in zijn plaats treden.

Ondertekening

Utrecht, 10 februari 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, 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[2].

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.

[2] Deze clausule geldt alleen voor uitvoerders

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).