Klokkenluiders- en incidentenregeling

Klokkenluiders- en incidentenregeling
Stichting Pensioenfonds Avebe

2022

Inleiding

De klokkenluiders- en incidentenregeling bevat een procedure voor interne en externe meldingen van (potentiële) misstanden en/of incidenten en de afhandeling daarvan. Ook een datalek, zoals bedoeld in de Algemene Verordening Gegevensbescherming (AVG) wordt aangemerkt als een incident. In bijlage 1 is de procedure inzake datalekken opgenomen. De regeling bevat waarborgen voor de bescherming van degene (de melder) van alle bij Stichting Pensioenfonds Avebe (hierna te noemen: het pensioenfonds) betrokken belanghebbenden, waaronder mede begrepen de verbonden persoon als bedoeld in de gedragscode, die te goeder trouw melding maakt van (potentiële) misstanden.

Regelgeving

Met deze regeling geeft het pensioenfonds uitvoering aan de vereisten van

a. De Wet op het financieel toezicht (Wft);

b. De Pensioenwet;

c. Het Besluit Financieel Toetsingskader Pensioenfondsen (Besluit FTK); en

d. De Code Pensioenfondsen.

e. De Algemene Verordening Gegevensbescherming

De Pensioenwet schrijft voor dat een pensioenfonds zijn organisatie zodanig inricht dat deze een beheerste en integere bedrijfsvoering waarborgt.

Misstanden en incidenten kunnen een gevaar vormen voor de beheersing en de integriteit van de bedrijfsvoering. Het is van groot belang dat misstanden en incidenten kunnen worden gemeld en dat deze zorgvuldig worden vastgelegd en afgehandeld. In het Besluit FTK en de bijbehorende toelichting is dit nader uitgewerkt. Het Besluit FTK stelt dat pensioenfondsen een systematische analyse moeten maken van integriteitrisico's en dat aan de hand van de analyse een integriteitsbeleid moeten worden vastgesteld en uitvoering aan dit beleid dient te worden gegeven. Deze klokkenluiders- en incidentenregeling is onderdeel van het integriteitsbeleid van het pensioenfonds.

Samenhang interne regelingen

Er bestaat binnen het pensioenfonds ook een gedragscode. Ook in deze gedragscode zijn gedragsnormen, waarden en regels opgenomen. Deze conflicteren niet met deze regeling en zijn eveneens van toepassing. Indien het belang van het pensioenfonds, van derden of de bescherming van de eigen positie van de belanghebbende dit vraagt (bijvoorbeeld omdat hij vreest dat een melding nadelige gevolgen kan hebben voor zijn positie of indien aan een eerdere melding geen gevolg is gegeven), doet de belanghebbende bij de compliance officer melding van een misstand of incident conform deze regeling. Het oordeel van de belanghebbende dat een melding dient plaats te vinden conform deze regeling is daarbij doorslaggevend.

Beleid

Artikel 1. Definities

Onder (vermoeden van een) ***incident*** wordt verstaan:

a. een gebeurtenis die een (ernstig) gevaar vormt voor de integere bedrijfsuitoefening van het pensioenfonds, en/of
b. een gebeurtenis waarbij directe of indirecte financiële schade of aantasting van het imago of reputatie van het pensioenfonds en haar organen kan ontstaan door ontoereikende of falende interne processen en systemen, door externe gebeurtenissen, of door laakbaar of niet-integer gedrag van belanghebbenden, en/of
c. fraude, misleiding, bedrog, verduistering of diefstal door een of meer personen in zijn/hun hoedanigheid van verbonden persoon, en/of
d. onregelmatigheden van algemene, operationele en financiële aard, en/of
e. datalekken.

Onder ***incident*** wordt in ieder geval verstaan:

a. een (dreigend) strafbaar feit;
b. een (dreigende) schending van wet- en regelgeving;
c. een (dreiging van) bewust onjuist informeren van publieke organen;
d. een schending van binnen het pensioenfonds geldende gedragsregels;
e. (een dreiging van) het bewust achterhouden, vernietigen of manipuleren van informatie over deze feiten.

Onder ***misstand*** wordt verstaan een toestand die dringend verbetering behoeft.

Onder de volgende definities wordt verstaan:

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
Verwerker	Een natuurlijk persoon of rechtspersoon die ten behoeve van het pensioenfonds persoonsgegevens verwerkt
Datalek	Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, of opgeslagen of anderszins verwerkte gegevens
Persoonsgegevens	Alle informatie over een geïdentificeerde of te identificeerbare natuurlijke persoon
Betrokkene	Degene op wie een persoonsgegeven betrekking heeft
Compliance Officer	De externe functionaris die als compliance officer is benoemd.
Belanghebbenden	Alle bij het pensioenfonds betrokken belanghebbenden, waaronder mede begrepen de verbonden persoon, als bedoeld in de gedragscode.
Melder	De belanghebbende die melding doet van een incident of misstand binnen het pensioenfonds;
Onderzoekscommissie	Een interne of externe onderzoekscommissie ter uitvoering van een onderzoek en de behandeling van een incident. De voorzitter van het bestuur is verantwoordelijk voor het samenstellen van deze commissie. Een interne onderzoekscommissie bestaat uit ten minste drie onafhankelijke personen. De onderzoekscommissie onderzoekt of sprake is van een incident als gedefinieerd en brengt advies uit inzake de afhandeling van het incident aan zowel de voorzitter van het bestuur als de compliance officer.

Beheersing

Artikel 2. Melden incidenten en misstanden

2.1. De melding van een incident en/of misstand wordt gedaan bij de compliance officer. Voor de melding van een datalek geldt een afwijkende procedure zoals beschreven in bijlage 1. De melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan. Meldingen kunnen anoniem gedaan worden. Indien aanvullende informatie benodigd is in het belang van het onderzoek, kan de melder worden verzocht zijn medewerking hieraan te verlenen. De melder is hiertoe niet verplicht.

2.2. De compliance officer stuurt een bevestiging aan de melder dat hij de melding ontvangen heeft en stelt de voorzitter van het bestuur door middel van een afschrift van de vastlegging van de melding op de hoogte van (de melding van) het incident of de misstand en de datum waarop deze is gemeld.

2.3. Meldingen worden vertrouwelijk behandeld. De (identificatie)gegevens van de melder worden alleen bekendgemaakt wanneer daartoe een wettelijke verplichting bestaat. Hiertoe wordt gewerkt met een geanonimiseerd ‘zaaknummer’. Ook indien de melder geen belang hecht aan anonimiteit zal zijn identiteit alleen dan worden vrijgegeven in communicatie, wanneer daartoe een wettelijke verplichting bestaat.

Artikel 3. Afhandelen incidenten en misstanden

Incidenten

3.1 De compliance officer onderzoekt of de melding betrekking heeft op een incident en of deze voldoende ernstig is om een verdergaand onderzoek in te stellen. Incidenten die als voldoende ernstig worden gekwalificeerd, worden afgehandeld door een onderzoekscommissie.

3.2 Het besluit over de wijze van afhandeling van incidenten door de compliance officer en de gronden waarop het gebaseerd is, worden direct, doch uiterlijk binnen twee weken na de melding schriftelijk aan de melder medegedeeld. Een afschrift van de toewijzing dan wel de afwijzing wordt gestuurd aan de voorzitter van het bestuur. Indien de melding betrekking heeft op de voorzitter van het bestuur, wordt het besluit gestuurd aan het verantwoordingsorgaan.

3.3 De compliance officer dient het incident, na afgerond onderzoek en gegrondverklaring, bij De Nederlandsche Bank (hierna: DNB) te melden evenals de maatregelen die het pensioenfonds heeft genomen.

Misstanden

3.4 Het orgaan waar zich de misstand heeft voorgedaan is in eerste instantie zelf verantwoordelijk voor een adequate afhandeling hiervan. De voorzitter van het orgaan coördineert de afhandeling van de misstand met eventuele ondersteuning van de compliance officer.

3.5 Het besluit over de wijze van afhandeling van misstanden door het betreffende orgaan en de gronden waarop het gebaseerd is, worden door de compliance officer uiterlijk binnen vier weken na de melding schriftelijk aan de melder meegedeeld. Een afschrift van de toewijzing dan wel de afwijzing wordt gestuurd aan de voorzitter van het bestuur. Indien de melding betrekking heeft op de voorzitter van het bestuur, wordt het besluit gestuurd aan het verantwoordingsorgaan.

Algemeen

3.6 Voor de afhandeling van het incident of de misstand worden maatregelen genomen die zijn gericht op het beheersen van het optredende risico, het bevestigen van geldende normen en het voorkomen van negatieve effecten – zowel intern als extern – om herhaling in de toekomst voorkomen.

3.7 De compliance officer registreert meldingen op datum van ontvangst. Per melding wordt een dossier bijgehouden. Gedurende het verdere proces worden in het dossier relevante documenten opgenomen, zoals de communicatie tussen de verschillende partijen, de rapportages en de resultaten van eventueel onderzoek. Het dossier wordt in een beveiligde omgeving bewaard. Identificatiegegevens van de melder worden op zodanige wijze bewaard dat alleen de compliance officer en (eventueel) de voorzitter van het bestuur en/of het betreffende orgaan toegang hebben tot deze gegevens. De compliance officer bewaakt de voortgang van het meldproces en de opvolging van acties.

Artikel 4. Rechtsbescherming

4.1. Een ieder die uit hoofde van deze regeling informatie verkrijgt over (de melding van) een incident of een misstand, betracht daarover uiterste geheimhouding tegenover derden, tenzij op basis van deze regeling of bij of krachtens de wet de bevoegdheid of de verplichting bestaat om die informatie aan een derde te verschaffen.

4.2. Het pensioenfonds draagt er zorg voor dat de melder op geen enkele wijze in zijn positie bij het pensioenfonds benadeeld wordt, voor zover te goeder trouw gehandeld is.

4.3. Het pensioenfonds draagt er zorg voor dat de compliance officer en de onderzoekscommissie op geen enkele wijze in hun positie bij het pensioenfonds benadeeld worden vanwege het uitoefenen van hun taken op grond van deze regeling.

4.4. De melder die willens en wetens heeft deelgenomen aan of veroorzaker is van een incident of een misstand zal bij melding hiervan geen recht kunnen ontlenen aan de beschermingsregel zoals die geldt voor een te goeder trouw handelende melder.

4.5. In geval van intrekking van de misstand door de melder vergewissen de compliance officer en de onderzoekscommissie zich ervan dat de intrekking niet onder invloed van dreigementen of door omkoping heeft plaatsgevonden.

Evaluatie

Artikel 5. Rapportage

De compliance officer stelt jaarlijks een rapportage op voor het bestuur. Deze staat los van de reguliere compliance rapportage. In de rapportage wordt ook inzicht gegeven in het aantal incidenten en misstanden dat zich het betreffende jaar heeft voorgedaan en de aard daarvan. Tevens betreft de rapportage de voortgang van de afhandeling van eerder gemelde incidenten en misstanden en eventueel opgelegde sancties. De voorzitter van het bestuur is verantwoordelijk voor het toezien op de opvolging van de genomen acties door agendering van de voortgang van de afhandeling van het incident in de vergadering van het bestuur.

Algemeen

Artikel 6 Onvoorziene omstandigheden

Voor kwesties waarin deze regeling niet voorziet, beslissen de voorzitter en de vice voorzitter van het bestuur in overleg met de compliance officer gezamenlijk.

Artikel 7 Inwerkingtreding

7.1. Deze regeling treedt in werking met ingang van 1 juli 2015 en is laatstelijk gewijzigd dd. 12 april 2022.

7.2. Het bestuur kan deze regeling te allen tijde wijzigen. Jaarlijks wordt bezien of deze regeling geactualiseerd dient te worden.

Bijlage 1 (Procedure Datalekken)

Met ingang van 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Onderdeel van deze verordening is de meldplicht van een inbreuk in verband met persoonsgegevens aan de Autoriteit Persoonsgegevens (AP) en in bepaalde gevallen aan de betrokkene(n).

In het navolgende wordt onder datalek verstaan, hetgeen is gedefinieerd in artikel 1: Uitgangspunten en definities, uit het Privacybeleid van het pensioenfonds.

Deze procedure beschrijft hoe te handelen binnen het pensioenfonds indien er sprake is van:
- een datalek of wanneer een datalek vermoed wordt;
- een datalek bij een verbonden persoon als bedoeld in de gedragscode van het pensioenfonds;
- een datalek bij een verwerker van persoonsgegevens van het pensioenfonds.

Per gemeld datalek behoudt het pensioenfonds zich de vrijheid voor om te beoordelen of de procedure, zoals hierna beschreven, gevolgd kan worden, dan wel afwijking van deze procedure gerechtvaardigd is.

Artikel 1 – Identificeren datalek

Met verbonden personen dan wel verwerker is afgesproken om tijdig, zonder onnodige vertraging, doch uiterlijk binnen 48 uur nadat de verbonden persoon dan wel verwerker een (mogelijk) datalek heeft geconstateerd, het bestuur van het pensioenfonds hiervan in kennis te stellen.

Daarnaast informeert de verbonden persoon of verwerker het pensioenfonds, zo mogelijk niet later dan 48 uur nadat het (mogelijk) datalek is geconstateerd, accuraat over:
a. de aard en omvang van de inbreuk op de beveiliging van persoonsgegevens;
b. de naam en contactgegevens van degene bij wie meer informatie over de inbreuk kan worden verkregen;
c. de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens en (kring van) de betrokkenen;
d. de maatregelen die de verbonden persoon dan wel de verwerker heeft getroffen of voorstelt te treffen om de (negatieve) gevolgen van de inbreuk te beperken en te verhelpen;
e. aanvullende gegevens die het pensioenfonds desgevraagd nodig heeft om een eventuele melding bij AP te kunnen verrichten.

Artikel 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 dat moet worden gemeld bij de AP. Indien het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor rechten en vrijheden van betrokkene(n), zal geen melding worden gemaakt bij de AP.
De beoordeling of er sprake is van een incident, dat gemeld moet worden aan de AP, komt tot stand met behulp van de schema's te vinden in de beleidsregels van de AP.

Tevens wordt beoordeeld of er per direct maatregelen genomen moeten worden om de schade te beperken, waaronder het doen van een (voorlopige) melding aan betrokkene(n).

Het pensioenfonds documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen.

Artikel 3 – Melding aan de AP

Het dagelijks bestuur verzorgt de tijdige (onverwijld, zonder onnodige vertraging, en niet later dan 72 uur na de ontdekking van het datalek) elektronische melding bij 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.

Bij de melding aan de AP wordt ten minste het volgende omschreven:

a. De aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
b. De naam en de contactgegevens van de personen bij wie informatie kan worden verkregen;
c. De waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
d. De maatregelen die het pensioenfonds heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen ervan.

Daarnaast wordt eventueel rekening gehouden met hetgeen bepaald is in het document 'Datalekken bij grootschalige postverzending' van de AP van 23 februari 2017.

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

Wanneer de inbreuk op de persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van de betrokkene(n), deelt het pensioenfonds de betrokkene dit onverwijld mee.
Het dagelijks bestuur stelt vast of het datalek ook moet worden gemeld aan degenen om wiens gegevens het gaat. Het dagelijks bestuur maakt hierbij gebruik van de schema's in de beleidsregels van de AP.

Artikel 5 – Oorzaken en verbetermaatregelen

De verbonden persoon of verwerker is verplicht om bij constatering van een datalek, in goed overleg met het pensioenfonds, voor eigen rekening en risico alle noodzakelijke maatregelen te nemen om het datalek te dichten en de schade die hieruit voortvloeit of kan voortvloeien, te beperken. De verbonden persoon of verwerker zal het pensioenfonds 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 verwerker te vragen bepaalde aanvullende organisatorische en/of beveiligingsmaatregelen te treffen. Het dagelijks bestuur bewaakt de voortgang van deze eventuele aanvullende beveiligingsmaatregelen.