

Pensioenfonds Avebe

**Klokkenluiders- en incidentenregeling
Stichting Pensioenfonds Avebe**

2024

Pensioenfonds Avebe

Artikel 1.	Definities.....	4
Artikel 2.	Melden incidenten en misstanden	5
Artikel 3.	Afhandelen incidenten en misstanden.....	7
Artikel 4.	Rechtsbescherming.....	9
Artikel 5.	Rapportage	10
Artikel 6	Onvoorziene omstandigheden	10
Artikel 7	Inwerkingtreding.....	10
Bijlage 1	Procedure datalekken	12

Pensioenfonds Avebe

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

Pensioenfonds Avebe

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:

- a. Een schending of gevaar voor schending van het Unierecht¹, of
- b. Een handeling of nalatigheid waarbij het maatschappelijk belang in het geding is bij:
 - a. een schending of een gevaar voor schending van een wettelijk voorschrift of van interne regels die een concrete verplichting inhouden en die op grond van een wettelijk voorschrift door een werkgever zijn vastgesteld, dan wel
 - b. een gevaar voor de volksgezondheid, voor de veiligheid van personen, voor de aantasting van het milieu of voor het goed functioneren van de openbare dienst of een onderneming als gevolg van een onbehoorlijke wijze van handelen of nalaten².

Het maatschappelijk belang is in ieder geval in het geding indien de handeling of nalatigheid niet enkel persoonlijke belangen raakt en er sprake is van oftewel een patroon of structureel karakter dan wel de handeling of nalatigheid ernstig of omvangrijk is.

Onder de volgende definities wordt verstaan:

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
Belanghebbenden	Alle bij het pensioenfonds betrokken belanghebbenden, waaronder mede begrepen de verbonden persoon, als bedoeld in de gedragscode.
Benadeling	omvat in ieder geval elke vorm van, dreiging of poging tot ontslag of schorsing, een boete als bedoeld in artikel 650 van Boek 7 van het Burgerlijk Wetboek, demotie, het onthouden van bevordering, een negatieve beoordeling, een schriftelijke berisping, overplaatsing naar een andere vestiging, discriminatie, intimidatie, pesterijen of uitsluiting, smaad of laster, voortijdige beëindiging van een overeenkomst voor het leveren van goederen of diensten.

¹ Onder Unierecht valt Europese regelgeving op het gebied van onder meer overheidsopdrachten, financiële diensten, producten en markten, voorkoming van witwassen van geld en terrorismefinanciering, productveiligheid en productconformiteit, veiligheid van het vervoer, bescherming van het milieu, stralingsbescherming en nucleaire veiligheid, veiligheid van levensmiddelen en diervoeders, diergezondheid en dierenwelzijn, volksgezondheid, consumentenbescherming, bescherming van de persoonlijke levenssfeer

² Het gaat hier om een direct aan het pensioenfonds toe te rekenen gedraging die tot de misstand leidt, dus niet bijvoorbeeld het pensioenfonds in haar rol van institutioneel belegger of aandeelhouder.

Pensioenfonds Avebe

Betrokken derde	a) een derde die verbonden is met een melder en die kan worden benadeeld door de werkgever van de melder, of b) een persoon of organisatie waarmee de melder anderszins in een werkgerelateerde context verbonden is, c) een rechtspersoon die eigendom is van de melder, waarvoor de melder werkt of waarmee de melder anderszins werkgerelateerd betrokken is.
Betrokkene	Degene op wie een persoonsgegevens betrekking heeft.
Compliance Officer	De externe functionaris die als compliance officer is benoemd.
Dagelijks bestuur	Het dagelijks bestuur van het pensioenfonds, bestaande uit de voorzitter en de vice-voorzitter van het bestuur.
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.
Melder	De belanghebbende die melding doet van een incident of een (vermoeden van een) 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.
Pensioenfonds	Stichting Pensioenfonds Avebe
Persoonsgegevens	Alle informatie over een geïdentificeerde of te identificeerbare natuurlijke persoon.
Verwerker	Een natuurlijk persoon of rechtspersoon die ten behoeve van het pensioenfonds persoonsgegevens verwerkt.
Visitatiecommissie	De visitatiecommissie (het intern toezicht) van het pensioenfonds

Beheersing

Artikel 2. Procedure melden incidenten en misstanden

Incidenten

- 2.1. De melding van een incident 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 en de datum waarop deze is gemeld.

Pensioenfonds Avebe

- 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 geanoniseerd '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.

Misstanden

- 2.4. De melding van een misstand wordt gedaan bij de compliance officer.
- 2.5. Het heeft de voorkeur dat de melder zijn melding intern doet. De melder is echter niet verplicht om een melding van een vermoeden van een misstand eerst intern te melden. De melder kan daarvan ook direct een externe melding doen bij een bevoegde autoriteit. Verder kan de melder ook kiezen voor een externe melding als:
- a. De melder het niet eens is met het standpunt van het pensioenfonds of van oordeel is dat de melding ten onrechte terzijde is gelegd of onvoldoende onderzocht is, of;
 - b. De melder niet binnen 3 maanden na de verzending van de ontvangstbevestiging van zijn melding een standpunt heeft ontvangen over de interne melding.
- 2.6. De melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan. De melder heeft de mogelijkheid om de melding te doen via een gesprek op locatie. Dat gesprek dient op redelijke termijn na ontvangst van het verzoek plaats te vinden.
- 2.7. Bij een mondelinge melding, al dan niet op locatie, registreert het pensioenfonds de melding door een opname of een schriftelijk verslag van het gesprek te maken. De melder wordt in de gelegenheid gesteld het verslag te controleren, aan te vullen en voor akkoord te tekenen.
- 2.8. De ontvanger van de melding draagt er zorg voor dat de melder binnen zeven dagen een ontvangstbevestiging ontvangt en stelt het dagelijks bestuur, door middel van een afschrift van de vastlegging van de melding, op de hoogte van de melding. De naam van de melder wordt alleen bekendgemaakt met toestemming van de melder of wanneer daartoe een wettelijke verplichting bestaat. Ingeval enig wettelijk voorschrift tot mededeling van de identiteit van een melder verplicht, dan wordt de melder daarvan in kennis gesteld.
- 2.9. De compliance officer beoordeelt of de melding kwalificeert als het vermoeden van een misstand zoals bedoeld in deze regeling en in de Wet bescherming klokkenluiders. Wanneer de melding kwalificeert als een misstand informeert de compliance officer het dagelijks bestuur over de melding en adviseert hen over het op te starten onderzoek. Bij twijfel overlegt de compliance officer met de sleutelfunctiehouder risicobeheer.
- 2.10. Het dagelijks bestuur besluit over de vervolgstappen en de wijze van onderzoek¹. Ook worden de overige bestuursleden en de visitatiecommissie op de hoogte gebracht van de melding. Het besluit tot verder onderzoek en de gronden waarop het gebaseerd is wordt binnen twee weken na de melding genomen en schriftelijk aan de melder meegedeeld.

¹ Indien de misstand tevens kwalificeert als een integriteitsincident in de zin van de incidentenregeling dan zal het pensioenfonds op grond van die regeling ook een melding aan de toezichthouder moeten doen. De uitgangspunten rondom vertrouwelijkheid gelden in dat geval onverkort.

Pensioenfonds Avebe

- 2.11. Wanneer de melding niet kwalificeert als een misstand, beoordeelt de compliance officer wie de melding namens het pensioenfonds verder afhandelt. De compliance officer informeert de melder binnen twee weken na de melding gemotiveerd over de beoordeling en over de verdere afhandeling.
- 2.12. Een melder kan een adviseur in vertrouwen raadplegen over een vermoeden van een misstand. Ook kan een melder een vertrouwenspersoon of de afdeling advies van het Huis voor Klokkenuitdrukkers verzoeken om informatie, advies en ondersteuning in verband met het vermoeden van een misstand. De afdeling advies van het Huis voor Klokkenuitdrukkers is telefonisch te bereiken via 088-1331 030.
- 2.13. Wanneer de melder niet zelf wil melden, kan een vertrouwelijke melding worden gedaan via de vertrouwenspersoon van het pensioenfonds. De contactgegevens van de vertrouwenspersoon zijn te vinden op de website van het pensioenfonds.
- 2.14. Wanneer de melder zijn melding geheel anoniem wil doen, dan kan de melder een tijdelijk e-mailadres aanmaken, waarmee met de compliance officer gecommuniceerd kan worden.
- 2.15. Een melder heeft de mogelijkheid om een melding van een misstand openbaar te maken. Openbaarmaking is alleen toegestaan:
 - c. als de melder redelijke gronden heeft om aan te nemen dat de gemelde informatie over het vermoeden van een misstand op het moment van openbaarmaking juist is; én
 - d. als de melder voorafgaand aan de openbaarmaking melding heeft gedaan bij de compliance officer; of
 - e. als de melder voorafgaand aan de openbaarmaking melding heeft gedaan bij het dagelijks bestuur; én
 - f. als de melder redelijke gronden heeft om aan te nemen dat het onderzoek naar het vermoeden van een misstand onvoldoende voortgang heeft.

Een melding op grond van deze regeling en de beoordeling van de melding worden geregistreerd in een register. Gedurende het verdere proces worden in het dossier de relevante documenten opgenomen, zoals de communicatie tussen de verschillende betrokkenen, de rapportages en de resultaten van eventueel onderzoek. De gegevens worden vernietigd op het moment dat deze niet meer noodzakelijk zijn dan wel indien enig wettelijk voorschrift dit voorschrijft.

- 2.16. De compliance officer zorgt ervoor dat informatie over de melding alleen toegankelijk is voor diegenen die bij de melding betrokken zijn.

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.

Pensioenfonds Avebe

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 dagelijks bestuur draagt het onderzoek op aan onderzoekers die onafhankelijk en onpartijdig zijn. Het onderzoek kan intern worden uitgevoerd of door een extern bureau.
- 3.5 . De onderzoekers stellen de melder in de gelegenheid te worden gehoord. Hiervan wordt verslag gemaakt. Indien akkoord bevonden, tekent de melder het verslag voor goedkeuring en ontvangt een kopie. De onderzoekers kunnen ook anderen horen. Ook hiervan wordt verslag gemaakt. Diegene die gehoord is, tekent het verslag indien akkoord bevonden voor goedkeuring en ontvangt hiervan een kopie.
- 3.6 De onderzoekers kunnen binnen het pensioenfonds alle documenten en gegevens opvragen en inzien die zij voor het onderzoek redelijkerwijs noodzakelijk vinden, met inachtnaam van het privacybeleid van het pensioenfonds.
- 3.7 De melder mag de onderzoekers alle documenten en gegevens verstrekken waarvan hij het redelijkerwijs nodig vindt dat de onderzoekers daar kennis van nemen.
- 3.8 De onderzoekers stellen een concept onderzoeksrapport op. De melder krijgt de gelegenheid om daar opmerkingen bij te maken, tenzij hiertegen ernstige bezwaren bestaan. De onderzoekers stellen vervolgens het onderzoeksrapport vast en stellen dit rapport ter beschikking aan het dagelijks bestuur.
- 3.9 De werkzaamheden genoemd in artikel 3.4 tot en met 3.8 vinden plaats binnen drie maanden na ontvangst van de melding. De compliance officer houdt de melder op de hoogte van de voortgang in het dossier, bijvoorbeeld door het sturen van een periodiek voortgangsbericht.
- 3.10 Het dagelijks bestuur deelt het onderzoeksrapport zo spoedig mogelijk met de rest van het bestuur. Het bestuur besluit binnen een redelijke termijn na ontvangst van het onderzoeksrapport of en zo ja welke maatregelen genomen worden en welke personen/fondsgremia en/of externe instanties geïnformeerd worden over het onderzoeksrapport en/of de genomen maatregelen.
- 3.11 Indien de melder het niet eens is met de uitkomst in het onderzoeksrapport of de manier waarop de melding wordt opgepakt en onderzocht, dan kan de melder zich met zijn zorg wenden tot de visitatiecommissie. Deze commissie neemt passende maatregelen en informeert de melder hierover.

Algemeen

- 3.12 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.

Pensioenfonds Avebe

- 3.13 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 (arbeidsrechtelijke) positie bij het pensioenfonds benadeeld wordt, voor zover te goeder trouw gehandeld is. Het pensioenfonds gaat er van uit dat een melding te goeder trouw is gedaan, tot het moment dat hij overtuigd is geraakt van het tegendeel. 4.4. Als de melder van een misstand van mening is dat sprake is van benadeling kan de melder:
- a. De compliance officer verzoeken om onderzoek te (laten) doen naar de wijze waarop met de melder is omgegaan; en/of;
 - b. Hierover advies inwinnen bij de afdeling advies van het Huis voor Klokkeluiders; en/of;
 - c. Een bejegeningsonderzoek aanvragen bij de afdeling onderzoek van het Huis voor Klokkeluiders.
- 4.5. Represailles als gevolg van melden worden beschouwd als een ernstige schending van deze regeling, in welk geval door het bestuur passende actie zal worden ondernomen om de (arbeidsrechtelijke) positie van de melder te beschermen
- 4.6. 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.
- 4.7. 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.
- 4.8. 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.
- 4.9. De bepalingen in dit artikel gelden ook voor degene die de melder bijstaat en voor betrokken derden.

Pensioenfonds Avebe

Evaluatie

Artikel 5. Publicatie en rapportage

- 5.1. Het pensioenfonds zorgt ervoor dat deze regeling intern wordt gepubliceerd en op de website wordt geplaatst.
- 5.2. De compliance officer stelt jaarlijks een rapportage op voor het bestuur. Deze staat los van de reguliere compliance rapportage, en bevat niet incidenten die gerelateerd zijn aan de AVG, welke de bestuursondersteuner namelijk opstelt. 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 per 28 maart 2024.
- 7.2. Het bestuur kan deze regeling te allen tijde wijzigen. Jaarlijks wordt bezien of deze regeling geactualiseerd dient te worden.

Pensioenfonds Avebe

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:

Pensioenfonds Avebe

- 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.