Incidentenregeling

van

Stichting Pensioenfonds voor Dierenartsen

Inleiding

Incidenten kunnen een gevaar vormen voor de integere en beheerste bedrijfsvoering van Stichting Pensioenfonds voor Dierenartsen. Deze Incidentenregeling geeft aan welke stappen gevolgd worden als het vermoeden bestaat dat er sprake is van een Incident binnen het Pensioenfonds. Doel van deze regeling is aldus het beschrijven van de procedure omtrent het melden, vastleggen en afhandelen van Incidenten zodat eventuele schade kan worden voorkomen of beperkt en herhaling van het Incident wordt voorkomen.

Met deze regeling geeft Stichting Pensioenfonds voor Dierenartsen uitvoering aan de vereisten van de Wet verplichte Beroepspensioenregeling en de Code Pensioenfondsen inzake de omgang met en vastlegging van Incidenten.

Artikel 1 Definities

Pensioenfonds	Stichting Pensioenfonds voor Dierenartsen
Bestuur	Het bestuur van het pensioenfonds
Toezichthouder	De Nederlandsche Bank (DNB), de Autoriteit Financiële Markten (AFM), de Autoriteit Persoonsgegevens (AP), de Autoriteit Consument en Markt (ACM), de fiscus en overige publieke toezichtsorganen met jurisdictie ten aanzien van (de werkzaamheden van) het pensioenfonds.
Incident	Een gebeurtenis die een ernstig gevaar vormt of kan vormen voor de beheerste en integere bedrijfsuitoefening van het pensioenfonds, en/of een gebeurtenis waarbij directe of indirecte financiële schade ontstaat door ontoereikende of falende interne processen, verbonden personen of systemen of door externe gebeurtenissen, dan wel een datalek zoals gedefinieerd in de Algemene Verordening Gegevensbescherming (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. Bij ICT-gerelateerde incidenten zijn ook de bepalingen van de Digital Operational Resilience Act (DORA) en het IT-beleid van het Pensioenfonds van toepassing. Er wordt een onderscheid gemaakt tussen operationele incidenten en overige incidenten.
Operationeel Incident	Een incident dat plaats heeft gevonden in de dagelijkse uitvoering van de werkzaamheden door of namens het pensioenfonds en waarbij er een inbreuk is geweest op de beheerste bedrijfsvoering.
Overige Incidenten	Alle incidenten, die niet beschouwd kunnen worden als operationele Incidenten. Onder overige incidenten worden in ieder geval verstaan: • een (dreigende) bewuste schending van wet- en regelgeving; • een (dreiging van) bewust onjuist informeren van publieke organen; • een (dreigende) schending van de binnen het pensioenfonds geldende gedragsregels;

- (een dreiging van) het achterhouden, vernietigen of manipuleren van informatie over deze feiten;
- een ernstig gevaar voor de integere bedrijfsuitoefening van het Pensioenfonds;
- gebeurtenissen die kunnen leiden tot een groot afbreukrisico in de media;
- fraude, misleiding, bedrog, verduistering of diefstal door een of meer personen in zijn/hun hoedanigheid van verbonden persoon;
- een (mogelijke) aanwijzing van een toezichthouder, een last onder dwangsom of het voornemen om een bestuurlijke boete op te leggen;
- overige strafbare feiten.

Compliance Officer	De functionaris die als compliance officer is benoemd of indien er geen compliance officer benoemd is, degene die verantwoordelijk is voor het uitvoeren van de compliancewerkzaamheden.
Voorzitter	De voorzitter van het bestuur van het pensioenfonds.
Vicevoorzitter	De vicevoorzitter van het bestuur van het pensioenfonds.
Verbonden Persoon	De verbonden personen zoals aangewezen in de gedragscode van het pensioenfonds.
Melder	De verbonden persoon die een (dreigend) Incident meldt.

Artikel 2 Melden van Incidenten

1. Iedere verbonden persoon die een (dreigend) incident constateert is gehouden dit te melden aan de voorzitter. Een melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan. Meldingen kunnen ook anoniem gedaan worden bij de voorzitter.

2. Als zich bij een partij, waaraan het pensioenfonds werkzaamheden heeft uitbesteed, een incident voordoet, meldt deze uitbestedingsrelatie het incident aan de voorzitter van het pensioenfonds. Het pensioenfonds draagt er zorg voor dat de uitbestedingsrelatie bekend is met deze regeling en weet bij wie een incident gemeld moet worden. De voorzitter van de monitoringscommissie pensioenbeheer wordt op de hoogte gehouden van de meldingen vanuit Achmea Pensioenservices. De voorzitter van de beleggingsadviescommissie wordt op de hoogte gehouden van de meldingen vanuit Achmea Investment Management.

3. Indien de melding betrekking heeft op de voorzitter, dan treedt de vicevoorzitter in het kader van deze regeling in zijn plaats.

Artikel 3 Beoordeling en vastleggen van incidenten

1. De voorzitter, beoordeelt de meldingen van de partijen waaraan het pensioenfonds werkzaamheden heeft uitbesteed en bepaalt of er sprake is van een incident en zo ja, of er dan sprake is van een operationeel dan wel een overig incident. De voorzitter meldt overige incidenten na beoordeling bij de compliance officer die de melding registreert in het incidentenregister.

2. Gedurende het verdere proces worden in het dossier van het overige incident de naar het oordeel van de compliance officer relevante documenten opgenomen, zoals de communicatie tussen de verschillende betrokkenen, de rapportages en de resultaten van eventueel onderzoek.

3. Dossiers van een overig incident worden in een beveiligde omgeving bewaard zodat de vertrouwelijkheid wordt gewaarborgd. Indien er sprake is van de betrokkenheid van een

verbonden persoon worden zijn identificatiegegevens op een zodanige wijze bewaard dat alleen de compliance officer en de voorzitter toegang hebben tot deze gegevens.

4. De voorzitter of vice-voorzitter informeert de melder over zijn beoordeling zoals bedoeld in artikel 3.1. Als wordt besloten om geen onderzoek in te stellen wordt hierin gemotiveerd aangegeven waarom er geen sprake is van een incident. Dit kan zowel schriftelijk, elektronisch als mondeling worden gedaan.

5. De melding en de daarbij beschikbaar gestelde gegevens worden door alle betrokken partijen strikt vertrouwelijk behandeld. De identiteit van de melder wordt niet opgenomen in communicatie naar derden, tenzij daar een wettelijke verplichting toe bestaat.

6. Een ieder die uit hoofde van deze regeling informatie verkrijgt over (de melding van) een incident, betracht daarover uiterste geheimhouding, 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. Indien voor de afronding van het incident openheid van zaken is vereist, kan het bestuur beslissen dat de verplichting tot geheimhouding geheel of gedeeltelijk vervalt.

Artikel 4 Behandeling van incidenten

1. Indien de voorzitter van mening is dat er sprake is van een operationeel incident behandelt de uitbestedingspartij waar zich het operationeel incident heeft voorgedaan het operationeel incident. De voorzitter van de monitoringscommissie of de beleggingsadviescommissie coördineert de afhandeling van het operationele incident met, afhankelijk van de aard van het operationele incident, ondersteuning van de voorzitter en/of de compliance officer.

2. Indien de voorzitter van mening is dat er sprake is of kan zijn van een overig incident brengt hij de vicevoorzitter en de compliance officer op de hoogte. Door de voorzitter en vicevoorzitter wordt, na advies van de compliance officer, besloten of en wanneer andere organen van het pensioenfonds, sleutelfunctiehouders en/of overige belanghebbenden op de hoogte worden gebracht van het overige incident.

3. De compliance officer behandelt de overige incidenten of adviseert het bestuur dat, gelet op de aard of achtergronden van het overige incident, afwikkeling door een andere functionaris of een speciaal daarvoor te benoemen onderzoekscommissie de voorkeur geniet. Het bestuur besluit op basis van dit advies of het overig incident behandeld wordt door een andere functionaris of onderzoekscommissie, Een onderzoekscommissie kan bestaan uit bestuursleden, medewerkers van de uitvoerder die betrokken zijn bij het pensioenfonds en/of externe deskundigen. Het onderzoek wordt niet uitgevoerd door personen die mogelijk betrokken zijn of zijn geweest bij het overig incident.

4. Als een onderzoek wordt verricht door een andere persoon dan de compliance officer of door een onderzoekscommissie is/zijn de onderzoeker(s) gehouden de compliance officer op de hoogte te brengen en te houden van alle ontwikkelingen in het onderzoek vanwege zijn coördinerende en registrerende rol.

5. De compliance officer bewaakt de voortgang van het meldproces, het onderzoek, alsmede de opvolging van acties en rapporteert hierover aan het bestuur.

Artikel 5 Afronding incidenten

Na de behandeling van elk incident wordt het bestuur op de hoogte gesteld van de behandeling van het incident en, ter afronding, door het bestuur besloten of er maatregelen genomen dienen te worden. De genomen maatregelen zullen zijn gebaseerd op de aard van het incident en de daaruit voortvloeiende gevolgen.

De maatregelen kunnen onder meer zijn gericht op het beheersen en beperken van het optredende risico, het bevestigen van geldende normen en het voorkomen van negatieve effecten – zowel intern als extern – van het incident om herhaling in de toekomst te voorkomen. De eindverantwoordelijkheid voor de afronding van het incident en de eventuele getroffen maatregelen ligt bij het bestuur.

Artikel 6 Rapportage

1. De voortgang van de afhandeling van incidenten wordt in de vergadering van het bestuur geagendeerd. Het bestuur is eindverantwoordelijk voor het toezien op de opvolging van de genomen acties. Namens het bestuur kunnen de compliance officer en/of de voorzitter toezien op de daadwerkelijke opvolging.

2. In de rapportage(s), zoals die periodiek aan het bestuur worden aangeboden, wordt inzicht gegeven in het aantal incidenten dat zich de betreffende periode heeft voorgedaan en de aard daarvan. Tevens bevat de rapportage informatie over de voortgang van de afhandeling van incidenten en naar aanleiding van deze incidenten genomen maatregelen.

Artikel 7 Spoedeisend belang

1. Indien de aard van het incident snel handelen vereist is de voorzitter, of diens plaatsvervanger, bevoegd om namens het bestuur een (voorlopig) besluit te nemen over de afhandeling van het incident.

2. De voorzitter is gehouden om de overige leden van het bestuur zo snel mogelijk op de hoogte te brengen van de door hem verrichte acties en genomen (voorlopige) besluiten en deze, indien nodig, alsnog ter definitieve besluitvorming aan het bestuur voor te leggen.

Artikel 8 Melden toezichthouder en overige communicatie

1. Door of namens het bestuur wordt onverwijld de relevante toezichthouder over een incident geïnformeerd als er sprake is van een incident dat een ernstig gevaar vormt voor de beheerste en integere bedrijfsvoering. Hiervan is in ieder geval sprake als:
   - aangifte is of wordt gedaan bij justitiële autoriteiten;
   - het voortbestaan van het pensioenfonds wordt bedreigd of zou kunnen worden bedreigd;
   - er sprake is van een ernstige tekortkoming in de opzet en werking van de maatregelen ter bevordering of handhaving van een integere bedrijfsvoering door het pensioenfonds;
   - mede gelet op verwachte publiciteit, rekening behoort te worden gehouden met (een ernstige mate van) reputatieschade voor het pensioenfonds;
   - of de ernst, de omvang of de overige omstandigheden van het incident in aanmerking genomen, de relevante toezichthouder in verband met haar toezichtstaak redelijkerwijs, of op basis van een wettelijke verplichting, behoort te worden geïnformeerd.

2. De relevante toezichthouder zal op de hoogte worden gebracht van alle feiten, omstandigheden en achtergronden van het incident, alsmede de maatregelen die naar aanleiding van het incident zijn genomen.

3. Het bestuur beslist over de communicatie, zowel intern als extern, met betrekking tot incidenten. Tenzij de melding het bestuur betreft, dan beslist de compliance officer,

Artikel 9 Omgang met meldingen

1. Het pensioenfonds gaat er altijd van uit dat een melding van een incident te goeder trouw is gedaan, tot het moment dat het overtuigd is geraakt van het tegendeel.

2. Het pensioenfonds draagt er zorg voor dat een melder, ongeacht de wijze waarop hij melding heeft gemaakt van een incident, op geen enkele wijze in zijn positie bij het pensioenfonds benadeeld wordt, voor zover te goeder trouw gehandeld is.

3. Het pensioenfonds draagt er zorg voor dat niemand wordt benadeeld in zijn of haar positie bij het pensioenfonds vanwege het uitoefenen van de taken en/of verplichtingen uit deze regeling.

4. In geval van intrekking van een melding zal het pensioenfonds, ongeacht de wijze waarop melding is gemaakt van een incident, zich ervan vergewissen dat de intrekking niet onder invloed van dreigementen of door omkoping heeft plaatsgevonden.

5. Een verbonden persoon die willens en wetens heeft deelgenomen aan of veroorzaker is van een incident, zal bij melding van dit incident geen recht kunnen ontlenen aan de beschermingsregels zoals die gelden voor een te goeder trouw handelende verbonden persoon.

Artikel 10 Klokkenluidersregeling

Het pensioenfonds beschikt tevens over een klokkenluidersregeling. Deze regeling is van toepassing bij (een vermoeden van) een misstand. De definitie van (een vermoeden van) een misstand is opgenomen in de klokkenluidersregeling. Indien een gebeurtenis wordt gekwalificeerd als een misstand, dan kan de verbonden persoon de procedure zoals beschreven in de klokkenluidersregeling volgen en is de incidentenregeling niet van toepassing.

Artikel 11 Inwerkingtreding

Deze regeling is vastgesteld door het bestuur en in werking getreden op 15 april 2025 onder gelijktijdige intrekking van de incidentenregeling van 31 januari 2023.

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. Er geldt sindsdien een meldplicht die inhoudt dat alle verbonden personen en derden (onder andere de pensioenuitvoeringsorganisatie) van het fonds datalekken onverwijld moeten melden aan:

- het fonds;
- in bepaalde gevallen of aan de AP, of DNB, of in bepaalde gevallen aan de betrokkene(n);

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 bewerker 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 behoudt het fonds zich de vrijheid voor om te beoordelen of de procedure gevolgd kan worden, dan wel afwijking van deze procedure gerechtvaardigd is.

1. Identificeren datalek

Met verbonden personen en derden is afgesproken om zonder onnodige vertraging, doch uiterlijk binnen 48 uur nadat de verbonden persoon of derde een (mogelijk) datalek heeft geconstateerd de voorzitter en secretaris (hierna: het dagelijks bestuur) hiervan in kennis te stellen. Het dagelijks bestuur bestaat uit de voorzitter en de secretaris van het pensioenfonds.
Daarnaast informeert de verbonden persoon of derde 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 uitvoerder 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 relevante 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. 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 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 beveiligingslek. Melding aan de AP is dan niet nodig. Wel overlegt het dagelijks bestuur dan of het zinvol is om het beveiligingslek te onderzoeken om herhaling te voorkomen.

3. Melden aan de AP

Het dagelijks bestuur zorgt dat er tijdig (onverwijld, zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek) een elektronische melding bij de AP volgens het online meldingsformulier van de AP wordt gedaan. Het dagelijks bestuur brengt de compliance officer op de hoogte van de melding. 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 (pensioenuitvoeringsorganisatie) vragen de melding aan de AP te doen en het dagelijks bestuur op de hoogte te houden van de melding (deze clausule geldt alleen voor pensioenuitvoeringsorganisaties).

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).

5. Oorzaken en verbetermaatregelen

De verbonden persoon of derde (pensioenuitvoeringsorganisatie) 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 (pensioenuitvoeringsorganisatie) 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 (pensioenuitvoeringsorganisatie) te vragen bepaalde aanvullende beveiligingsmaatregelen te treffen. Het dagelijks bestuur bewaakt de voortgang ten aanzien van eventuele aanvullende beveiligingsmaatregelen.

6. Registratie

De derde (pensioenuitvoeringsorganisatie) houdt tevens een registratie bij van ieder datalek bij de derde.