



Stichting Bedrijfstakpensioenfonds voor de Zuivel en aanverwante industrie

Incidentenregeling

Deze Incidentenregeling is een uitgave van
Stichting Bedrijfstakpensioenfonds voor de Zuivel en aanverwante Industrie

Datum
24 maart 2026

Versie
2026.1

Inhoudsopgave

Inleiding	3
Artikel 1 Definities	4
Artikel 2 Melden, beoordelen en vastleggen van incidenten	6
Artikel 3 Behandeling van incidenten	7
Artikel 4 Afronding incidenten.....	8
Artikel 5 Rapportage	8
Artikel 6 Spoedeisend belang.....	9
Artikel 7 Melden toezichthouder en overige communicatie	9
Artikel 8 Omgang met meldingen	10
Artikel 9 Klokkenluidersregeling	10
Artikel 10 Overig	10

Inleiding

Incidenten kunnen een gevaar vormen voor de integere en beheerste bedrijfsvoering van ons pensioenfonds. Deze Incidentenregeling geeft aan welke stappen gevolgd worden als het vermoeden bestaat dat er sprake is van een incident binnen het fonds. 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 BPZ uitvoering aan de vereisten van de Pensioenwet en andere relevante wetgeving inzake de omgang met en vastlegging van incidenten.

Artikel 1 Definities

Datalek	Een inbreuk op de beveiliging van persoonsgegevens.
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 toezichtorganen met jurisdictie ten aanzien van BPZ.
Incident	<p>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.</p> <p>Onder incidenten worden in ieder geval verstaan:</p> <ul style="list-style-type: none">• een (dreigende) bewuste schending van wet- en regelgeving;• een (dreiging van) bewust onjuist informeren van publieke organen;• een (dreigende) bewuste en/of ernstige schending van 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 (mogelijk) aanwijzing van een toezichthouder, een last onder dwangsom of het voornemen om een bestuurlijke boete op te leggen;• overige strafbare feiten;• een gebeurtenis die de beveiliging van de netwerk- en informatiesystemen in gevaar brengen en een nadeling effect hebben op de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens. <p>Er wordt een onderscheid gemaakt tussen integriteitsincidenten, ICT-gerelateerde incidenten, operationele incidenten en overige incidenten</p>

Integriteitsincident	Een gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van de desbetreffende organisatie.
ICT-gerelateerd incident	<p>1) regulier ICT-incident: een gebeurtenis of een reeks gekoppelde gebeurtenissen die niet door het pensioenfonds zijn gepland en die de beveiliging van de netwerk- en informatiesystemen in gevaar brengen en een nadelig effect hebben op de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens of op de door het pensioenfonds verleende diensten.</p> <p>2) ernstig ICT-gerelateerd incident: een ICT-gerelateerd incident met grote nadelige gevolgen voor de netwerk- en informatiesystemen die kritieke of belangrijke functies van het pensioenfonds ondersteunen.</p>
Operationeel incident	Een incident is een gebeurtenis die plaats heeft gevonden in de dagelijkse uitvoering van de werkzaamheden door het pensioenfonds en waarbij er een inbreuk is geweest op de beheerste bedrijfsvoering.
Overige incidenten	Alle incidenten, die niet beschouwd kunnen worden als integriteitsincident, ICT-gerelateerd incident of operationele incidenten. Onder overige incidenten worden in ieder geval verstaan:
Incidentenregister	De registratie van alle binnengekomen gebeurtenissen alsmede de wijze van opvolging, ingestelde onderzoeken, onderzoeksresultaten, de genomen preventieve en repressieve maatregelen en eventuele meldingen aan de betrokken toezichthouder(s).
Compliance Officer	De functionaris die als compliance officer is benoemd door het pensioenfonds.
Verbonden Personen	<p>Verbonden personen zijn (categorieën) van personen die door het pensioenfonds op grond van de gedragscode zijn aangewezen als verbonden persoon, waaronder in ieder geval:</p> <ul style="list-style-type: none"> • leden van het bestuur van het pensioenfonds; • leden van het belanghebbendenorgaan van het pensioenfonds; • leden van de raad van toezicht van het pensioenfonds; • de houders van de sleutelfunctie; • leden van eventuele commissies die het pensioenfonds heeft ingesteld. • een medewerker van het pensioenfonds onafhankelijk van de duur of de juridische basis waarop deze werkzaam is.

Pensioenfonds	Stichting Bedrijfstakpensioenfonds voor de Zuivel en aanverwante industrie (BPZ).
Vertrouwenspersoon	De compliance officer van het pensioenfonds.
Voorzitter	De voorzitter van het bestuur van het pensioenfonds.

Artikel 2 Melden, beoordelen en vastleggen van incidenten

1. Ieder verbonden persoon die een (vermoeden van een) incident constateert, is gehouden dit te melden aan de compliance officer. Een melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan. Meldingen kunnen ook anoniem gedaan worden. Indien en voor zover het (vermoedelijke) incident óók te kwalificeren is als een datalek in de zin van de procedure datalekken, dient de melding ook te worden gedaan aan de functionaris gegevensbescherming volgens de procedure datalekken van het pensioenfonds.
2. Voor sleutelfunctiehouders geldt de meldingsplicht aan de vertrouwenspersoon niet wanneer het incident kwalificeert als een substantieel risico of een significante inbreuk als bedoeld in artikel 143a lid 3 van de Pensioenwet en de sleutelfunctiehouder op grond van dit artikel gehouden is tot melding aan de toezichthouder. De sleutelfunctiehouder informeert in dat geval de vertrouwenspersoon over de melding aan de toezichthouder. Deze regeling is niet van toepassing op de in de vorige volzin genoemde melding aan de toezichthouder, met uitzondering van het bepaalde in artikel 8 lid 1 tot en met 3.
3. 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. Indien de melding betrekking heeft op de voorzitter, dan treedt de rest van het bestuur in het kader van deze regeling in zijn plaats. Het pensioenfonds draagt er zorg voor dat de uitbestedingsrelatie bekend is met deze regeling en weet bij wie een incident gemeld moet worden.
4. Het staat een verbonden persoon vrij een (vermoeden van een) incident ook aan de vertrouwenspersoon te melden. Deze is – indien deze functie niet door dezelfde persoon wordt vervuld – gehouden de compliance officer op de hoogte te brengen.
5. De compliance officer beoordeelt de melding en bepaalt of er sprake is van een incident en zo ja, of er dan sprake is van een operationeel Incident, ICT-gerelateerd incident, integriteitsincident of een overig incident. Dit oordeel wordt vastgelegd. Bij de beoordeling of het een ICT-gerelateerd incident betreft, dient vervolgens ook onderscheid gemaakt te worden tussen een regulier en een ernstig ICT-gerelateerd incident. Hierbij moet gebruik gemaakt worden van de criteria beschreven in DORA-wetgeving. Alleen ernstige ICT-gerelateerde incidenten hoeven gemeld te worden.

6. Meldingen van incidenten en de beoordeling van de compliance officer van het incident worden geregistreerd in het incidentenregister, tenzij de gevoeligheid van de informatie een dergelijke registratie in de weg staat. Gedurende het verdere proces worden in het dossier 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 (externe uitgevoerd) onderzoek. In geval van significante cyberdreigingen worden deze ook bijgehouden in het incidentenregister.
7. Incidentendossiers 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.
8. De compliance officer informeert de melder over zijn beoordeling zoals bedoeld in artikel 2.5. Dit kan zowel schriftelijk, elektronisch als mondeling worden gedaan.
9. 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.
10. 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 3 Behandeling van incidenten

1. Indien de compliance officer van mening is dat er sprake is van een operationeel incident of een ICT-gerelateerd incident brengt hij de leidinggevende van de afdeling waar zich het incident heeft voorgedaan op de hoogte. Indien de compliance officer van mening is dat er sprake is of kan zijn van een integriteitsincident of een overig incident brengt hij de voorzitter op de hoogte. Door de voorzitter 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 incident.
2. De afdeling waar zich het operationele of ICT-gerelateerde incident heeft voorgedaan zorgt voor de afhandeling van het incident. De leidinggevende coördineert de afhandeling van het incident met, afhankelijk van de aard van het incident, ondersteuning van de compliance officer.

3. De compliance officer behandelt de integriteitsincidenten en overige incidenten, tenzij het bestuur, na advies van de compliance officer, besluit dat, gelet op de aard of achtergronden van het incident, afwikkeling door een andere functionaris of een speciaal daarvoor te benoemen onderzoekscommissie de voorkeur geniet. Een onderzoekscommissie kan bestaan uit medewerkers van het pensioenfonds en/of externe deskundigen.
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 4 Afronding incidenten

Na de behandeling van elk incident wordt, ter afronding, door het pensioenfonds 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 5 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.
3. Het incidentenregister wordt met inachtneming van het bepaalde in deze regeling aan de sleutelfunctiehouders “interne audit” en “risicobeheer” als bedoeld in artikel 143a van de Pensioenwet op diens verzoek ter kennis gebracht.

Artikel 6 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 7 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 toezichthouder in verband met haar toezichtstaak redelijkerwijs, of op basis van een wettelijke verplichting, behoort te worden geïnformeerd.
2. De 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. Ernstige ICT-gerelateerde incidenten worden altijd gemeld bij de toezichthouder. Daarbij zal een eerste kennisgeving binnen 4 uur na classificatie als ernstig ICT-gerelateerd incident en niet later dan 24 uur na identificatie van het ICT-gerelateerd incident, worden gedeeld met de toezichthouder. Een tussentijds verslag over het ernstige ICT-gerelateerde incident wordt naar de toezichthouder gestuurd binnen 72 uur na de eerste kennisgeving. Een eindverslag wordt met de toezichthouder gedeeld, uiterlijk één maand na het laatste tussentijdse verslag.
4. Het bestuur beslist over de communicatie, zowel intern als extern, met betrekking tot incidenten.

Artikel 8 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 zij 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 9 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 kwalificeert als een misstand, dan kan de verbonden persoon de procedure zoals beschreven in de klokkenluidersregeling volgen.

Artikel 10 Overig

Deze regeling is vastgesteld door het bestuur en in werking getreden op 1 januari 2015 en laatstelijk gewijzigd met ingang van 1 januari 2026.