Stichting Pensioenfonds Recreatie

INCIDENTENBELEID 2024

6 november 2024

Vertrouwelijkheidsclassificatie: openbaar

Inhoudsopgave

Artikel 1 Definities

Voor deze regeling, waarin het incidentbeleid van het pensioenfonds is vervat, zijn de begripsomschrijvingen zoals opgenomen in de statuten en de gedragscode van het pensioenfonds van toepassing. Dit beleid geldt tevens voor de houders en vervullers van sleutelfuncties, voor zover deze niet door het bestuur zijn aangewezen als verbonden persoon.

Incident:

a. Een gebeurtenis die een gevaar vormt voor de integere en/of beheerste bedrijfsuitoefening van het pensioenfonds, en/of
b. Een gebeurtenis waarbij directe of indirecte financiële schade of aantasting van de goede naam van het pensioenfonds kan ontstaan door ontoereikende of falende interne processen, verbonden personen of systemen of door externe gebeurtenissen.

Er wordt onderscheid gemaakt tussen 'integriteitsincidenten', 'operationele incidenten' en 'operationeel voorval'.

Integriteitsincident:
Een gedraging of gebeurtenis die een gevaar vormt voor de integere en/of beheerste bedrijfsuitoefening van het pensioenfonds met inbegrip van de bij het pensioenfonds betrokken (rechts)personen. Onder een integriteitsincident wordt in ieder geval begrepen:

- een (dreigende) schending van op het fonds toepasselijke wet- en regelgeving;
- (een dreiging van) onjuist informeren van de toezichthouder;
- een (dreigende) schending van de gedragscode van het pensioenfonds;
- (een dreiging van) het achterhouden, vernietigen of manipuleren van informatie met betrekking tot incidenten;
- een gebeurtenis die kan leiden tot reputatieschade voor het pensioenfonds;
- strafbare handelingen door een verbonden persoon die gevolgen kunnen hebben voor de geschiktheid van de betreffende persoon voor een functie bij het pensioenfonds, waaronder fraude, misleiding, bedrog, verduistering of diefstal.

Operationeel incident:
Een gebeurtenis waarbij directe of indirecte financiële schade kan ontstaan door ontoereikende of falende interne processen, verbonden personen of systemen of door externe gebeurtenissen. Hieronder worden tevens begrepen ICT- en cyberincidenten ,anders dan een datalek.

Operationeel voorval:
Een voorval dat plaats heeft gevonden in de dagelijkse uitvoering van de werkzaamheden van het pensioenfonds en waarbij er geen inbreuk is gemaakt op de integere en/of beheerste bedrijfsvoering.

Datalek:
Een inbreuk in verband met persoonsgegevens als bedoeld in de Algemene Verordening Gegevensbescherming (AVG).

DORA:
Digital Operational Resilience Act.

Ernstig ICT-incident:

Een ICT-gerelateerd incident met grote nadelige gevolgen voor de netwerk- en informatiesystemen die kritieke of belangrijke functies van het Fonds ondersteunen, als bedoeld in de DORA. Dit is verder uitgewerkt in de Procedure Ernstige ICT-incidenten.

Melder:
a. de verbonden persoon die melding doet van een incident;
b. de persoon, werkzaam bij een uitbestedingspartij van het pensioenfonds, maar niet als verbonden persoon is aan te merken en die melding doet van een incident.

Artikel 2 Melden, beoordelen en vastleggen van een datalek

Een incident dat zich mogelijk kwalificeert als een datalek wordt afgehandeld conform een separaat beleidsdocument procedure datalekken dat het pensioenfonds hiervoor heeft opgesteld.

Artikel 3 Melden, beoordelen en vastleggen van integriteitsincidenten

3.1 Iedere melder die een (dreigend) integriteitsincident constateert is gehouden dit te melden aan de compliance officer. Voor verbonden personen die de functie van sleutelfunctiehouder vervullen geldt deze meldingsplicht niet wanneer het integriteitsincident 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 de compliance officer over melding aan de toezichthouder. Een dergelijke melding wordt niet afgehandeld conform de hieronder beschreven procedure. In geval van een wettelijk verplichte melding aan de toezichthouder door een sleutelfunctiehouder is artikel 10 van deze regeling van overeenkomstige toepassing. Een melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan. Een melding mag gericht worden aan het bestuursbureau. Het bestuursbureau zorgt dat de melding wordt voorgelegd aan de compliance officer.

3.2 Een oud-verbonden persoon kan een melding van een (dreigend) integriteitsincident alleen melden indien het (dreigend) integriteitsincident betrekking heeft op de periode dat de oud-verbonden persoon een verbonden persoon was. De melding van het (dreigend) integriteitsincident valt onder het incidentenbeleid indien de melding binnen twee maanden na het einde van het zijn van een verbonden persoon is ontvangen.

3.3 De compliance officer beoordeelt de melding en bepaalt of er sprake is van een integriteitsincident. Dit oordeel wordt vastgelegd en terstond op schriftelijke wijze aan het bestuur gemeld.

3.4 Indien het bestuur van mening is dat er geen sprake is van een integriteitsincident meldt zij dit aan de compliance officer en verzoekt hem het dossier te sluiten.

3.5 Indien er, naar het oordeel van het bestuur, sprake is van een ernstig integriteitsincident dan wordt dit onverwijld aan de Nederlandsche Bank (Meldpunt Misstanden) gemeld. De compliance officer legt verantwoording af aan het bestuur.

3.6 Meldingen van integriteitsincidenten en de beoordeling van de compliance officer van het integriteitsincident worden geregistreerd in het incidentenregister. 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.

3.7 De compliance officer brengt de melder van de beoordeling op de hoogte. Dit kan zowel schriftelijk, elektronisch als mondeling worden gedaan.

Artikel 4 Melden, beoordelen en vastleggen van operationele incidenten en operationele voorvallen

4.1 Iedere melder die een (dreigend) operationeel incident of operationeel voorval constateert is gehouden dit te melden aan het bestuursbureau. Voor verbonden personen die de functie van sleutelfunctiehouder vervullen geldt deze meldingsplicht niet wanneer het incident of voorval 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 de compliance officer over melding aan de toezichthouder. Een dergelijke melding wordt niet afgehandeld conform de hieronder beschreven procedure. In geval van een wettelijk verplichte melding aan de toezichthouder door een sleutelfunctiehouder is artikel 10 van deze regeling van overeenkomstige toepassing. Een melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan.

4.2 Iedere melder die een (mogelijk) ernstig ICT-incident constateert is gehouden dit onverwijld te melden aan het bestuursbureau. Of sprake is van een ernstig ICT-incident wordt beoordeeld aan de hand van de criteria opgenomen in de geldende procedure ernstige ICT-incidenten van het fonds. Een ernstig ICT-incident wordt beschouwd als incident en wordt afgehandeld als zodanig geregistreerd.

4.2 De melding geeft in ieder geval een beschrijving van:

- het incident of voorval;
- de achterliggende oorzaak;
- de mogelijke impact op de bedrijfsvoering en reputatie van het fonds en de mogelijke risico's;
- de verwachte hersteltijd;
- de getroffen beheersmaatregelen en/of workarounds en
- de wijze van implementatie van de getroffen maatregelen.

Bij het informeren worden er direct afspraken gemaakt over de voortgangsbewaking om de oplossing en de beheersing van het incident of voorval te kunnen monitoren en daar waar nodig bij te sturen.

4.3 Het bestuursbureau beoordeelt de melding o.b.v. het incidentenbeleid en legt dit ter advisering voor aan de vervuller sleutelfunctie Risicobeheer. Het bestuursbureau zorgt dat de melding, inclusief het advies van de vervuller sleutelfunctie Risicobeheer, wordt voorgelegd aan het dagelijks bestuur. In het advies wordt ook ingegaan of een melding aan DNB of AFM noodzakelijk is. Het dagelijks bestuur beoordeelt of er sprake is van een operationeel incident dan wel of er sprake is van een operationeel voorval. Desgewenst vraagt het dagelijks bestuur een oordeel van de Risicocommissie. In geval van een

operationeel incident vindt zo nodig een tussentijds telefonisch overleg met het dagelijks bestuur plaats of is sprake van agendering voor de eerstvolgende vergadering van het dagelijks bestuur. Is er sprake van een operationeel voorval dan komt het voorval op de agenda van de eerstvolgend vergadering van het dagelijks bestuur.
Het bestuur wordt geïnformeerd via de schriftelijke mededelingen.

4.4 Indien het dagelijks bestuur van mening is dat het incident tevens moet worden beschouwd als integriteitsincident, wordt dit incident afgehandeld conform artikel 3 van deze regeling.

4.5 Een operationeel voorval wordt niet gemeld aan DNB of AFM.

4.6 Meldingen van operationele incidenten/voorvallen en de beoordeling van het dagelijks bestuur worden geregistreerd in het incidentenregister.

4.7 Het dagelijks bestuur brengt de melder van de beoordeling op de hoogte. Dit kan zowel schriftelijk, elektronisch als mondeling worden gedaan.

Artikel 5 Behandeling van incidenten / operationele voorvallen

5.1 Indien het dagelijks bestuur dit wenst kan er een onderzoek worden ingesteld door externen.

5.2 Tijdens het onderzoek naar een incident of een operationeel voorval worden, als een onderzoek naar een of meerdere verbonden personen deel uitmaakt van de werkzaamheden, de regels in acht genomen die gelden voor het doen van een persoonsgericht onderzoek als beschreven in artikel 10.

5.3 Het bestuursbureau bewaakt de voortgang van het meldproces, het onderzoek, alsmede de opvolging van acties.

Artikel 6 Afronding incidenten

Na de behandeling van elk incident worden, ter afronding, door het pensioenfonds maatregelen genomen.
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 7 Rapportage

7.1 De voortgang van de afhandeling van incidenten wordt in de vergadering van het dagelijks bestuur geagendeerd. Het bestuur is eindverantwoordelijk voor het toezien op de opvolging van de genomen acties. Namens het bestuur kan de Compliance Officer of het bestuursbureau toezien op de daadwerkelijke opvolging.

7.2 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 8 Rol dagelijks bestuur

8.1 Indien de aard van het incident snel handelen vereist, is het dagelijks bestuur bevoegd om namens het bestuur een voorlopig besluit te nemen.

8.2 Het dagelijks bestuur is gehouden om de overige leden van het bestuur zo snel mogelijk op de hoogte te brengen van de door hen verrichte acties en genomen (voorlopige) besluiten en deze, indien nodig, alsnog ter definitieve besluitvorming aan het bestuur aan te bieden.

Artikel 9 Melden toezichthouder en overige communicatie

9.1 Door of namens het bestuur wordt onverwijld de relevante toezichthouder en de Raad van Toezicht over een incident geïnformeerd als:
a. aangifte is of wordt gedaan bij justitiële autoriteiten;
b. het voortbestaan van het pensioenfonds wordt bedreigd of zou kunnen worden bedreigd;
c. er sprake is van een ernstige tekortkoming in de opzet en werking van de maatregelen ter bevordering of handhaving van een integere en beheerste bedrijfsvoering door het pensioenfonds;
d. 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.

9.2 Door of namens het bestuur wordt een incident dat tevens kwalificeert als een aan de Autoriteit Persoonsgegevens te melden datalek aan deze Autoriteit Persoonsgegevens gemeld, conform een separate procedure die het pensioenfonds hiervoor heeft opgesteld.

9.3 Het melden van ernstige ICT-incidenten aan DNB verloopt volgens de procedure ernstige ICT-incidenten.

9.4 De toezichthouder en de Raad van Toezicht zullen 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.

9.5 Het bestuur beslist over de communicatie, zowel intern als extern, met betrekking tot incidenten. Het bestuur besluit, eventueel na advies van de Compliance Officer, of en wanneer andere organen van het pensioenfonds, stakeholders en overige belanghebbenden op de hoogte worden gebracht van een incident. Incidenten die gemeld worden aan de toezichthouder worden ook opgenomen in het jaarverslag van het pensioenfonds.

Artikel 10 Persoonsgericht onderzoek

10.1 Als er een redelijk vermoeden bestaat dat een verbonden persoon verantwoordelijk is voor/ zich schuldig heeft gemaakt aan een incident, of als daar naar het oordeel van het bestuur aanleiding toe bestaat, kan een persoonsgericht onderzoek worden ingesteld. De persoon

naar wie het persoonsgericht onderzoek zich richt wordt onverwijld op de hoogte gebracht van het persoonsgericht onderzoek.

10.2 Een persoonsgericht onderzoek wordt ingesteld binnen een redelijke termijn, nadat er voldoende aanwijzingen bekend geworden zijn dat de betreffende verbonden persoon zich schuldig heeft gemaakt aan het incident.

10.3 De verbonden persoon naar wie het persoonsgericht onderzoek verricht wordt, wordt in de gelegenheid gesteld zijn zienswijze kenbaar te maken. Zijn zienswijze wordt schriftelijk vastgelegd.

10.4 Door of namens het bestuur worden een of meerdere personen of organisaties aangewezen die het persoonsgericht onderzoek verrichten.

10.5 Indien het onderzoek en/of het belang van het pensioenfonds dit vereist, kan, in overleg met het bestuur, door de onderzoeker(s) opdracht gegeven worden om bepaalde gegevens of zaken veilig te stellen. Daartoe wordt een belangenafweging gemaakt. Voor het inzien van persoonlijke informatie is toestemming van het bestuur vereist.

10.6 Een persoonsgericht onderzoek vindt op een integere en zorgvuldige wijze plaats. Toegezien wordt op de in acht te nemen zorgvuldigheid, waarbij de belangen van het pensioenfonds, het belang van de persoon dan wel de personen naar wie het onderzoek zich richt en de belangen van overige betrokkenen redelijkerwijs in acht worden genomen. Het persoonsgericht onderzoek wordt binnen een redelijke termijn uitgevoerd.

10.7 Na de uitvoering van een persoonsgericht onderzoek, wordt een schriftelijk advies uitgebracht aan het Bestuur. Het op schrift gestelde advies wordt door de Compliance Officer bewaard.

10.8 Alle relevante documenten, daaronder begrepen de zienswijze van de verschillende betrokkenen, rapportages en het op schrift gestelde advies worden opgenomen in een dossier.

Artikel 11 Meldingen en geheimhouding

11.1 Meldingen van een incident 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.

11.2 Meldingen van een incident worden vertrouwelijk behandeld. De identificatiegegevens van de melder worden niet opgenomen in de communicatie naar derden. Ook indien de melder geen belang hecht aan anonimiteit zal zijn identiteit alleen dan worden vrijgegeven in communicatie, wanneer daartoe een wettelijke verplichting bestaat.

11.3 Incidentendossiers worden in een beveiligde omgeving bewaard. Indien er sprake is van de betrokkenheid van een verbonden persoon worden zijn identificatiegegevens op een zodanige wijze bewaard dat alleen de Compliance Officer, Bestuursondersteuning en de voorzitters toegang hebben tot deze gegevens.

11.4 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.

11.5 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 12 Omgang met meldingen

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

12.2 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.

12.3 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.

12.4 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.

12.5 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 13 Slotbepalingen

13.1 Deze regeling is door het bestuur vastgesteld op en treedt in werking per 16 oktober 2014. Deze regeling kan door het bestuur worden gewijzigd.

13.2 Deze regeling is gewijzigd op 8 september 2015, 14 maart 2017, 12 september 2019, 9 april 2020 en op 6 november 2024.

Ondertekening

Het bestuur van het pensioenfonds heeft dit incidentenbeleid op 9 april 2020 vastgesteld met inwerkingtreding per 1 januari 2020.

Stichting Pensioenfonds Recreatie

A.W. Snijders I.W. Hollander

Voorzitter

Lid dagelijks bestuur