Operationele Incidentenregeling

SBZ Pensioen is een handelsnaam van Stichting Bedrijfstakpensioenfonds Zorgverzekeraars kvk 41178751

Inhoud

Inleiding

Incidenten kunnen een gevaar vormen voor de integere en beheerste bedrijfsvoering van SBZ Pensioen (hierna: het fonds). Deze Operationele Incidentenregeling geeft aan welke stappen gevolgd worden als het vermoeden bestaat dat er sprake is van een Operationeel Incident of een IT-Incident met uitsluitend operationele gevolgen binnen het fonds. Doel van deze regeling is aldus het beschrijven van de procedure omtrent het melden, vastleggen en afhandelen van deze Incidenten zodat eventuele schade kan worden voorkomen of beperkt en herhaling van het Incident wordt voorkomen.

Artikel 1 Definities

Benadeling: omvat in ieder geval elke vorm van, dreiging of poging tot schorsing, een boete als bedoeld in artikel 650 van Boek 7 van het BW, een negatieve beoordeling, een schriftelijke berisping, discriminatie, intimidatie, smaad of laster, voortijdige beëindiging van een overeenkomst voor het leveren van goederen of diensten.

Betrokkene: iedere persoon die werkzaamheden gaat verrichten, verricht of heeft verricht voor, dan wel betrokken is of is geweest bij het fonds (dit met inbegrip van Verbonden personen).

Betrokken derde: een natuurlijk persoon verbonden met de Melder die kan worden benadeeld door de organisatie waar de Melder werkzaamheden voor verricht dan wel een persoon waarmee de Melder verbonden is binnen de context van diens werkzaamheden. Een rechtspersoon die eigendom is van de Melder, waarvoor de Melder werkt of deze binnen de context van diens werkzaamheden verbonden is.

Compliance officer: diegene die is aangewezen om als zodanig voor het fonds te fungeren. Dit is de heer Albert de Jong, bereikbaar via a.dejong@compliance-instituut.nl, 088-99 88 100 of 06-83 17 29 15.

Incident: Een gedraging of gebeurtenis die een ernstig gevaar vormt of kan vormen voor de beheerste en integere bedrijfsuitoefening van het fonds. Deze regeling ziet toe op operationele incidenten en IT-incidenten met uitsluitend operationele gevolgen:

- **IT-incident met uitsluitend operationele gevolgen**: een incident (op zichzelf staande- of als onderdeel van een samenhangende gebeurtenis) die kan leiden tot een beperkte verstoring van de IT-dienstverlening die valt binnen de risicoparameters van de overeengekomen operationele SLA afspraken en waarbij er geen sprake is van integriteitsrisico's. Van een operationeel gerelateerd IT-incident is onder meer sprake wanneer een IT-applicatie of IT-hardware bijvoorbeeld niet meer (volgens specificaties) werkt, waardoor de normale dienst wordt verstoord.
- **Operationeel incident**: een incident dat plaats heeft gevonden in de dagelijkse uitvoering van werkzaamheden door het fonds en waarbij een inbreuk is geweest op de beheerste bedrijfsvoering.

Incidentenregister: een register waarin de Uitvoerende Bestuursleden Incidenten vastleggen. Dat zij incidenten met betrekking tot het pensioen- en vermogensbeheer.

Integriteitsincidenten: incidenten met een of meerdere kenmerken van een (ernstig) integriteitsincident zijn een gedraging of gebeurtenis als die in ieder geval:

a. Een strafbaar feit oplevert,
b. een schending inhoudt van interne of externe regelgeving of beleidsregels, waaronder de gedragscode,
c. autoriteiten of personen die belast zijn met de uitvoering van of het toezicht de naleving van wettelijke regelingen, of wettelijke opsporingsambtenaren beoogt te misleiden,
d. beoogt dat informatie over de hiervoor genoemde feiten wordt achtergehouden of,
e. op enigerlei wijze direct of indirect de goede naam van het fonds kan schaden.
f. leidt tot datalekken zoals beschreven in artikel 33 en 34 AVG (ook als zij een IT-component kennen).
g. leidt tot een Misstand, waarbij het maatschappelijk belang in het geding is bij de schending van een wettelijk voorschrift, een gevaar voor de volksgezondheid, een gevaar voor de veiligheid van personen, een gevaar

voor de aantasting van het milieu of een gevaar voor het goed functioneren van het fonds als gevolg van een onbehoorlijke wijze van handelen of nalaten. Ook ongewenst gedrag kan in bepaalde situaties een misstand zijn en,.

h. **een I**T-incident met een of meerdere kenmerken van een (ernstig) Integriteitsincident is een incident (op zichzelf staande- of als onderdeel van een samenhangende gebeurtenis) dat de veiligheid van een netwerk en informatiesystemen negatief beïnvloedt en/of negatieve gevolgen heeft op de beschikbaarheid, betrouwbaarheid, integriteit of vertrouwelijkheid van (persoons)gegevens en/of de diensten die aangeboden worden vanuit of namens het fonds. Het fonds beschikt over een aparte procedure voor het melden van IT-incidenten.

Melder: iedere persoon die in het kader van de Incidentenregeling een melding doet van een Incident.

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 (de werkzaamheden van) SBZ Pensioen.

Verbonden persoon (overeenkomst artikel 1.1 van de gedragscode van SBZ Pensioen):

a. De leden van het Bestuur van SBZ Pensioen (verder: het fonds);
b. De leden van het Verantwoordingsorgaan van het fonds;
c. Externe leden van commissies;
d. Sleutelfunctiehouders;
e. Het Bestuur kan andere (groepen van) personen als verbonden persoon aanwijzen.

Medewerkers van uitbestedingspartners zijn geen verbonden personen, tenzij deze op basis van lid e van dit artikel wel als zodanig door het Bestuur zijn aangewezen. Het fonds heeft afspraken met uitbestedingspartijen over het verplicht melden van incidenten aan het fonds.

Vertrouwelijk: niet openbaar of publiek maken van verkregen informatie of van omstandigheden waarin een Incident zich heeft voorgedaan dan wel de gevolgen van dat Incident.

Artikel 2 Melden, beoordelen en vastleggen van Incidenten

1. Het Bestuur van het fonds zal ervoor zorgdragen dat deze regeling bekend is bij Verbonden personen en via diens website gepubliceerd wordt.

2. Iedere Melder die een (dreigend) Incident constateert, is gehouden dit tijdig en duidelijk te melden aan de Uitvoerende Bestuursleden, direct of via bestuursondersteuning.

3. De Uitvoerende Bestuursleden ontvangen de meldingen en beoordelen of het een Incident betreft in de zin van deze regeling.

4. **Ernstige Incidenten** met de volgende kenmerken zijn integriteitsincidenten:
    a. Een belangrijke en verstrekkende invloed op de integere of beheerste bedrijfsvoering en/of,
    b. Een groot risico of reputatieschade voor het fonds in de media en/of,
    c. De betrokkenheid van het Openbaar Ministerie en/of,
    d. Kunnen leiden tot een aanwijzing van enige toezichthouder, een last onder dwangsom of het voornemen een bestuurlijke boete op te leggen en/of,
    e. Elk incident dat door de (Niet) Uitvoerende Bestuursleden als ernstig wordt geclassificeerd.

    Als een incident met één of meerdere van bovengenoemde kenmerken wordt gemeld aan de Uitvoerende Bestuursleden dan wordt het incident parallel aan de afhandeling van de operationele aspecten onder deze regeling

óók afgehandeld conform de Integriteitsincidentenregeling van het fonds. Daarbij hoort ook het hiervan op de hoogte stellen van de voorzitter van het Bestuur en de betrokkenheid van de Compliance officer voor zover dat betrekking heeft op de integriteitsaspecten van het incident.

5. Het Bestuur beslist over communicatie, zowel intern als extern, met betrekking tot Incidenten.

6. Meldingen van Incidenten worden namens de Uitvoerende Bestuursleden geregistreerd in een Incidentenregister (door bestuursondersteuning). Gedurende het verdere proces worden in het dossier de naar het oordeel van de Uitvoerende Bestuursleden (ondersteund door bestuursondersteuning) relevante documenten opgenomen, zoals de communicatie tussen de verschillende betrokkenen, de rapportages, de resultaten van eventueel onderzoek, wijze van opvolging, de genomen preventieve en repressieve maatregelen en de meldingen aan de relevante toezichthouder(s).

7. Eenieder die uit hoofde van deze regeling informatie verkrijgt over (de melding van) een Incident behandelt dat als vertrouwelijk, 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 deze verplichting geheel of gedeeltelijk vervalt.

Artikel 3 Behandeling van Incidenten

1. Indien de Uitvoerende Bestuursleden van mening zijn dat er sprake is van een Incident (operationeel en IT-incident met uitsluitend operationele gevolgen) dan brengen zij de voorzitter van de Audit- Risk- en Compliance commissie daarvan achteraf per e-mail op de hoogte. Vanwege hun karakter en aard is bij deze categorie meldingen geen standaard betrokkenheid en taak voor de Compliance Officer weggelegd, tenzij een Incident aantoonbaar het gevolg is van moedwillig niet compliant handelen.

2. Na de behandeling van elk Incident wordt door de Uitvoerende Bestuursleden besloten of er (aanvullende) beheersmaatregelen genomen dienen te worden. De genomen beheersmaatregelen 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 de Uitvoerende Bestuursleden.

Artikel 4 Rapportage

Als de aard van het Incident dit, naar de mening van de Uitvoerende Bestuursleden nodig maakt, zullen zij daarover rapporteren aan het Bestuur.

Artikel 5 Spoedeisend belang

Bij spoedeisend belang zijn de Uitvoerende Bestuursleden na afstemming met de voorzitter van de Audit-, Risk- en Compliance commissie gerechtigd om een voorlopig besluit te nemen over de afhandeling van een Incident. De Uitvoerende Bestuursleden stellen de leden van het Bestuur zo snel mogelijk op de hoogte van de verrichte acties en genomen (voorlopige) besluiten.

Artikel 6 Rechtsbescherming

1. Het Bestuur zal de Melder niet benadelen in verband met het te goeder trouw en naar behoren melden van een vermoeden van een Incident.

2. Van Benadeling als bedoeld in artikel 6.1 is ook sprake als een redelijke grond aanwezig is om de Melder aan te spreken op zijn functioneren of een benadelende maatregel als bedoeld in lid 3 jegens hem te nemen, maar de maatregel die het fonds neemt niet in redelijke verhouding staat tot die grond.

3. Indien het Bestuur jegens de Melder binnen afzienbare tijd na het doen van een melding overgaat tot het nemen van een benadelende maatregel motiveert het waarom het deze maatregel nodig acht en dat deze maatregel geen verband houdt met het te goeder trouw en naar behoren melden van een vermoeden van Incident.

4. Het Bestuur draagt er zorg voor dat leidinggevenden en collega's van de Melder zich onthouden van iedere vorm van Benadeling in verband met het te goeder trouw en naar behoren melden van een vermoeden van een Incident, die het professioneel of persoonlijk functioneren van de Melder belemmert.

5. Het Bestuur spreekt Verbonden personen die zich schuldig maken aan Benadeling van de Melder daarop aan en kan hen een waarschuwing of een disciplinaire maatregel opleggen.

6. In geval de Melder de melding intrekt, vergewist het Bestuur zich ervan dat de intrekking niet onder invloed van dreigementen of door omkoping heeft plaatsgevonden.

Artikel 7 Integriteitsincidentenregeling

Het fonds beschikt tevens over een Integriteitsincidentenregeling. Deze regeling is van toepassing bij Integriteitsincidenten. Indien een gebeurtenis kwalificeert als een Integriteitsincident, dan kan de Melder de procedure zoals beschreven in de Integriteitsincidentenregeling volgen.

Artikel 8 Klokkenluidersregeling

Het fonds beschikt tevens over een Klokkenluidersregeling. Deze regeling is van toepassing op integriteitsmeldingen die voldoen aan de criteria van een Misstand of een inbreuk op Unierecht. Er is sprake van een Klokkenluidersincident als de Melder besluit om een melding te doen buiten het fonds en/of direct de publiciteit zoekt. Onder de Wet bescherming klokkenluiders is het volgen van een intern meldproces niet langer verplicht. Extern melden kan ook het gevolg zijn van onvrede bij de Melder over de manier waarop, dan wel de uitkomst van een intern onderzoek naar aanleiding van een melding door de Melder.

Artikel 9 Regeling datalekken

Het fonds beschikt tevens over een Regeling datalekken. Deze regeling is van toepassing bij (een vermoeden van) een datalek. Indien een gebeurtenis kwalificeert als een datalek, dan kan de Melder de procedure zoals beschreven in de Regeling datalekken volgen.

Artikel 10 Regeling IT-incident

Het fonds beschikt over een Regeling IT incidenten[1]. Deze Regeling IT-incidenten is van toepassing op alle soorten IT-incidenten met dien verstande dat:

- Een IT-incident met uitsluitend operationele consequenties zal worden afgehandeld in lijn met de instructies inzake Operationele risico's en specifieke bepalingen uit het IT-Beleid; en
- Dat IT-incidenten die voldoen aan één of meerdere van de kenmerken zoals genoemd in artikel 1 Definities (Integriteitsincidenten) en/of art. 2 lid 4 (Ernstige Integriteitsincidenten) worden afgehandeld in lijn met de instructies inzake Integriteitsrisico's en specifieke bepalingen uit het IT-Beleid waarbij de Regeling Integriteitsincidenten leidend is voor zover er sprake is van melding aan de toezichthouder; en
- Dat IT-incidenten die voldoen aan één of meerdere kenmerken van een Datalek zoals genoemd in artikel 1 Definities (Datalek) worden afgehandeld in lijn met de procedure Datalekken en specifieke bepalingen uit het IT-Beleid waarbij de procedure Datalekken leidend is voor zover er sprake is van melding aan de toezichthouder.

[1] In aanvulling op de bestaande routering wordt in 2024 een procedure voor de melding van IT-incidenten conform de wettelijke (DORA) en regelingsvereisten (m.n. vanuit DNB) opgesteld. Vooralsnog geldt dan ook melding via de Uitvoerende Bestuursleden direct of/en via de bestuursondersteuning.

Artikel 11 Overig

Deze regeling is vastgesteld door het Bestuur op 7 juni 2024 en treedt in werking op 7 juni 2024.

Deze regeling wordt ten minste een keer in de drie jaar geëvalueerd en geactualiseerd via de Audit-, Risk- en Compliance commissie, tenzij tussentijds sprake is van belangrijke wijzigingen. Dan wordt deze Regeling onverwijld aangepast.

Zeist, 7 juni 2024

Ties Tiessen
Onafhankelijk voorzitter

Edwin Schokker
Uitvoerend bestuurslid