

## **Incidentenregeling**

### **Stichting Bedrijfstakpensioenfonds voor de Meubelindustrie en de Meubileringsbedrijven**

#### ***Inleiding***

De incidentenregeling van Stichting Bedrijfstakpensioenfonds voor de Meubelindustrie en de Meubileringsbedrijven (hierna: "het Fonds") bevat een procedure voor interne en externe meldingen van Incidenten en de afhandeling daarvan. Het bestuur bevordert dat de dienstverleners van het Fonds een overeenkomstige regeling hebben die aansluit bij de Incidentenregeling van het Fonds.

Voor deze regeling zijn de begripsomschrijvingen zoals opgenomen in de statuten, de gedragscode en de procedure datalekken van het Fonds van toepassing. Deze regeling geldt tevens voor de houders en vervullers van de sleutelfuncties, voor zover deze niet door het bestuur zijn aangewezen als verbonden persoon.

#### **Samenhang interne regelingen**

Er bestaat binnen het Fonds ook een gedragscode. Ook in deze gedragscode zijn gedragsnormen opgenomen. Deze conflicteren niet met deze regeling en zijn eveneens van toepassing.

Het Fonds beschikt tevens over een klokkenluidersregeling met een procedure voor het melden van (potentiële) incidenten en de afhandeling daarvan, waarbij de melder zich niet vrij voelt om te melden volgens deze incidentenregeling.

#### **Inwerkingtreding**

Deze regeling is door het bestuur vastgesteld en treedt in werking op 13 januari 2021 en is laatstelijk gewijzigd op 22 december 2021.

## Artikel 1. Definities

### Bestuur:

Het uitvoerend en niet-uitvoerend bestuur van het Fonds.

### Bestuursbureau:

Het (externe) bestuursbureau van het Fonds, bpfmeubel-bestuursbureau@montaepartners.nl.

### Compliance Officer:

De externe functionaris die als Compliance Officer is benoemd. Dit is mevrouw B. (Bianca) van Tilburg. E-mailadres: compliancebpfmeubel@hvglaw.nl en/of telefoonnummer: +31 (0) 6 2908 38 12.

### Datalek:

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

### Functionaris Gegevensbescherming:

De externe functionaris die als Functionaris Gegevensbescherming is benoemd. Dit is de heer S. van de Giessen. E-mailadres: BPFMeubel-Privacy@montaepartners.nl en/of telefoonnummer: +31 (0) 6 1124 28 70.

### Incident:

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

Er wordt onderscheid gemaakt tussen 'integriteitsincidenten' en 'operationele incidenten'.

### Integriteitsincident:

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

- 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 (mogelijke) schending van binnen het Fonds geldende gedragsregels;
- e. (een dreiging van) het bewust achterhouden, vernietigen of manipuleren van informatie over deze feiten;
- f. gedragingen die kunnen leiden tot reputatieschade voor het Fonds;
- g. een (mogelijke) aanwijzing van een toezichthouder, een last onder dwangsom of het voornemen om een bestuurlijke boete op te leggen.

### Melder:

- a. de verbonden persoon die melding doet van een Incident binnen het Fonds;
- b. de persoon die anderszins betrokken is bij het Fonds, maar niet als verbonden persoon is aan te merken en die melding doet van een Incident binnen het Fonds.

### 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 onderzoekscommissie bestaat uit drie onafhankelijke personen.

Operationeel incident:

Een gebeurtenis waarbij directe of indirecte (financiële of reputatie) schade kan ontstaan door ontoereikende of falende interne processen, verbonden personen of systemen of door externe gebeurtenissen,.

Operationele gebeurtenis:

Een gebeurtenis die heeft plaatsgevonden in de dagelijkse uitvoering van de werkzaamheden van het Fonds en waarbij er geen inbreuk is gemaakt op de integere en/of beheerste bedrijfsvoering.

Verbonden Personen zijn:

- a. leden van het Bestuur,
- b. leden van het Verantwoordingsorgaan en de onafhankelijke auditcommissie,
- c. externe beleggingsadviseur,
- d. medewerkers van het Bestuursbureau
- e. het bestuur kan andere (groepen van) mensen 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.

## **Artikel 2. Melden Incidenten**

### ***Algemeen***

- 2.1 Een Operationele gebeurtenis is geen Incident als bedoeld in deze regeling en wordt niet volgens deze regeling afgehandeld.
- 2.2 Meldingen van Incidenten worden vertrouwelijk behandeld. De identificatiegegevens van de Melder worden niet opgenomen in de communicatie naar derden. Hiertoe wordt gewerkt met een geanonimiseerd '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.

### ***Melding en registratie van de melding***

- 2.3 Iedere Verbonden Persoon en sleutelfunctiehouder die een (dreigend) Incident constateert is gehouden dit onverwijld te melden aan het Bestuursbureau conform dit artikel. Ook andere personen betrokken bij het Fonds kunnen een melding doen van een (dreigend) Incident conform deze Incidentenregeling.
- 2.4 Eenieder die een (dreigend) Incident constateert en zich niet vrij voelt dit te melden op grond van de Incidentenregeling, kan dit melden aan de Compliance Officer op grond van de Klokkeluidersregeling. De Incidentenregeling is van toepassing tenzij anders bepaald in de Klokkeluidersregeling.
- 2.5 Voor sleutelfunctiehouders geldt deze meldingsplicht niet wanneer het Incident kwalificeert als een substantieel risico of significante inbreuk als bedoeld in artikel 143a, lid 3 van de Pensioenwet en de sleutelhouder op grond van dit artikel is gehouden tot melding aan DNB. De

sleutelfunctiehouder informeert de Compliance Officer voorafgaand over de melding aan DNB. Een dergelijke melding wordt niet volgens deze regeling afgehandeld. In geval van een wettelijke verplichte melding door een sleutelfunctiehouder aan DNB is artikel 6 van deze regeling van overeenkomstige toepassing.

- 2.6 Iedere Verbonden Persoon en sleutelfunctiehouder die een (mogelijk) Datalek constateert is gehouden dit onverwijld te melden aan de Functionaris Gegevensbescherming en de uitvoerend bestuurder risicobeheer. Een Datalek wordt beschouwd als Incident en wordt als zodanig geregistreerd. Een (mogelijk) Datalek wordt volgens de geldende procedure datalekken van het Fonds afgehandeld..
- 2.7 Het Bestuursbureau registreert meldingen van Incidenten 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 Bestuursbureau bewaakt de voortgang van het meldproces en de opvolging van acties en rapporteert hierover aan het uitvoerend bestuur.
- 2.8 Alle identificatiegegevens van de Melder worden volgens de eisen en richtlijnen van de Algemene Verordening Gegevensbescherming en de Autoriteit Persoonsgegevens en in lijn met het privacyreglement van het Fonds verwerkt.
- 2.9 De melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan. Een mondelinge melding wordt schriftelijk vastgelegd door het Bestuursbureau. 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.

### ***Behandeling van de melding***

- 2.10 Het Bestuursbureau stuurt binnen vijf werkdagen een ontvangstbevestiging aan de Melder en stelt tevens het uitvoerend bestuur van het Fonds 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.
- 2.11 Als de Melder vreest voor tegenmaatregelen of als een eerdere melding van hetzelfde Incident deze niet heeft weggenomen, bestaat de mogelijkheid om direct melding te doen aan de voorzitter van het Bestuur. De voorzitter van het Bestuur stuurt deze melding onverwijld door naar de Compliance Officer. Als het de voorzitter zelf betreft dan dient de Melder in een soortgelijk geval onverwijld melding te doen aan de Compliance Officer.
- 2.12 Als de voorzitter van het Bestuur binnen 5 werkdagen na de melding als bedoeld in artikel 2.11 geen actie onderneemt, kan melding worden gedaan bij de Compliance Officer.

### **Artikel 3. Afhandelen Incidenten**

Voor de afhandeling van het Incident worden door het uitvoerend bestuur 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 te voorkomen, waaronder melding aan DNB indien en voor zover dit nodig is op grond van de Pensioenwet. Om de negatieve gevolgen van het Incident zo spoedig mogelijk te beperken,

kunnen door het uitvoerend bestuur, separaat aan de afhandeling van het Incident, tussentijdse maatregelen getroffen worden.

- 3.1 Het Bestuursbureau beoordeelt de melding en stelt uiterlijk binnen acht werkdagen na de ontvangen melding met het uitvoerend bestuur van het Fonds vast:
  - a. Of het een Integriteitsincident dan wel een Operationeel incident betreft;
  - b. Of het Incident wel of niet tevens een Datalek betreft. Indien het tevens een Datalek betreft is artikel 2.6 van toepassing;
  - c. De (mogelijke) risico-impact van het Incident. De risico-impact wordt op basis van een vaste procedure (bijlage bij deze regeling), ingedeeld naar laag, medium en hoog. Is de risico-impact hoog, dan wordt hier melding van gedaan aan de Compliance Officer.
- 3.3 De beoordeling bedoeld onder artikel 3.2 wordt ter oordeelsvorming aan de sleutelfunctiehouder risicobeheer voorgelegd. Indien de sleutelfunctiehouder risicobeheer tot een ander oordeel komt, wordt zijn oordeel gevolgd. Van zijn oordeel kan alleen bij een gemotiveerd bestuursbesluit worden afgeweken.
- 3.4 Operationele incidenten met een risicoclassificatie 'laag' of 'medium' worden door het uitvoerend bestuur afgehandeld. Integriteitsincidenten en operationele incidenten met een risicoclassificatie 'hoog' worden onverwijld na de beoordeling en oordeelsvorming als bedoeld in de artikelen 3.1, 3.2 en 3.3 ter afhandeling aan de Compliance Officer en de voorzitter van het fonds voorgelegd. Indien in dit geval de incidentmelding betrekking heeft op de voorzitter, treedt de loco-voorzitter in diens plaats op.
- 3.5 Indien de melding van een Operationeel Incident met risicoclassificatie 'laag' of 'medium' een van de leden van het uitvoerend bestuur betreft, wordt het Incident afgehandeld door het andere lid van het uitvoerend bestuur. Wanneer deze melding het volledige uitvoerend bestuur betreft, wordt het Incident afgehandeld door de Compliance Officer en de voorzitter van het fonds.
- 3.6 De wijze waarop het Incident is afgehandeld en de gronden waarop dit is gebaseerd, worden uiterlijk binnen twee weken na de afhandeling schriftelijk aan de Melder meegedeeld. Indien het uitvoerend bestuur de melding heeft afgehandeld, ontvangt de Compliance Officer een afschrift ter informatie. Ook degene op wie de melding betrekking had wordt geïnformeerd.
- 3.7 De Compliance Officer kan, bij Incidenten die conform artikel 3.4 of 3.5 ter afhandeling aan de Compliance Officer zijn voorgelegd, op basis van een zelfstandige oordeelsvorming de voorzitter adviseren een Onderzoekscommissie in te stellen. Van zijn advies kan alleen bij een gemotiveerd bestuursbesluit worden afgeweken. De Onderzoekscommissie wordt door het Bestuur ingesteld en bestaat uit drie personen. De Onderzoekscommissie brengt en houdt de Compliance Officer op de hoogte van alle ontwikkelingen in het onderzoek.
- 3.8 Het Bestuur dient het Incident, als bedoeld in artikel 3.1, na afgerond onderzoek, bij DNB te melden evenals de maatregelen die het Fonds heeft genomen.

#### **Artikel 4. Persoonsgericht onderzoek**

- 4.1 Als er een redelijk vermoeden bestaat dat een Verbonden Persoon verantwoordelijk is voor of zich schuldig heeft gemaakt aan een Integriteitsincident, of als daar naar het oordeel van het Bestuur aanleiding toe bestaat, kan het Bestuur een persoonsgericht onderzoek instellen. De Verbonden Persoon op wie het persoonsgericht onderzoek zich richt wordt onverwijld op de hoogte gebracht van het persoonsgericht onderzoek.

- 4.2 Een persoonsgericht onderzoek wordt ingesteld binnen een redelijke termijn, nadat er voldoende aanwijzingen bekend zijn geworden dat de betreffende verbonden persoon zich schuldig heeft gemaakt aan het Integriteitsincident.
- 4.3 De Verbonden Persoon naar wie het persoonsgericht onderzoek wordt verricht, wordt in de gelegenheid gesteld zijn zienswijze kenbaar te maken. Zijn zienswijze wordt schriftelijk vastgelegd.
- 4.4 Door of namens het Bestuur worden een of meerdere personen of organisaties aangewezen die het persoonsgericht onderzoek verrichten.
- 4.5 Indien het onderzoek en/of het belang van het Fonds dit vereist, kan, in overleg met het Bestuur, door de onderzoeker(s) opdracht worden gegeven om bepaalde gegevens of zaken veilig te stellen. Daartoe wordt een belangenafweging gemaakt. Voor het inzien van persoonlijke informatie is toestemming van het Bestuur c.q. de overige bestuursleden vereist.
- 4.6 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 Fonds, het belang van de Verbonden Persoon (dan wel de Verbonden 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.
- 4.7 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.
- 4.8 Alle relevante documenten, daaronder begrepen de zienswijze van de verschillende betrokkenen, rapportages en het op schrift gestelde advies worden opgenomen in een dossier dat door de Compliance Officer wordt bewaard.

#### **Artikel 5. Melden aan de toezichthouder(s) en overige communicatie**

- 5.1 DNB wordt, door of namens het Bestuur, bij een te melden Incident in ieder geval geïnformeerd binnen een termijn van vijf werkdagen nadat:
  - a. aangifte is of wordt gedaan bij justitiële autoriteiten;
  - b. het voortbestaan van het Fonds 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 bedrijfsvoering door het Fonds;
  - d. mede gelet op verwachte publiciteit, rekening behoort te worden gehouden met (een ernstige mate van) reputatieschade voor het Fonds; of
  - e. 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.
- 5.2 Van een aan DNB te melden Incident wordt tevens gelijktijdig melding gedaan aan de AFM en/of de AP indien het Incident betrekking heeft op onderdelen van de bedrijfsvoering van het Fonds waarop zij toezicht houden.
- 5.3 Het Bestuur beslist over de communicatie, zowel intern als extern, met betrekking tot Incidenten. Door het bestuur wordt, na advies van de Compliance Officer, besloten of en wanneer andere

organen van het Fonds, stakeholders en overige belanghebbenden op de hoogte worden gebracht van een Incident.

#### **Artikel 6. Rechtsbescherming**

- 6.1. Een ieder die uit hoofde van deze regeling informatie verkrijgt over (de melding van) een Incident, 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.
- 6.2. Het Fonds draagt er zorg voor dat de Melder en eventueel door de Melder betrokken perso(o)n(en) op geen enkele wijze in zijn positie bij het Fonds benadeeld wordt, voor zover te goeder trouw gehandeld is.
- 6.3. Het Fonds draagt er zorg voor dat de Compliance Officer en de onderzoekscommissie op geen enkele wijze in hun positie bij het Fonds benadeeld worden vanwege het uitoefenen van hun taken op grond van deze regeling.
- 6.4. De Melder die willens en wetens heeft deelgenomen aan of veroorzaker is van een Incident zal bij melding hiervan geen recht kunnen ontlenen aan de beschermingsregel zoals die geldt voor een te goeder trouw handelende Melder.

#### **Evaluatie**

#### **Artikel 7. Rapportage**

- 7.1 Het Bestuursbureau rapporteert periodiek aan het uitvoerend bestuur en de sleutelfunctiehouder risicobeheer over de voortgang en afhandeling van Incidenten. Opgetreden incidenten worden periodiek gerapporteerd aan het Bestuur. De voortgang van de afhandeling van Incidenten met een risicoclassificatie 'hoog' 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 het uitvoerend bestuur toezien op de daadwerkelijke opvolging.
- 7.2 In de rapportage(s), zoals die jaarlijks door de Compliance Officer aan het bestuur worden aangeboden, wordt inzicht gegeven in het aantal Incidenten dat zich in de betreffende periode heeft voorgedaan en de aard daarvan. Tevens bevat de rapportage informatie over de voortgang van de afhandeling van Incidenten die op basis van artikel 3.4 of 3.5 aan de Compliance Officer ter behandeling zijn voorgelegd, en de naar aanleiding van deze Incidenten genomen maatregelen.
- 7.3 De voorzitter van het Bestuur is bij Incidenten met een risicoclassificatie 'hoog' 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. Bij Incidenten met een risicoclassificatie 'laag' of 'medium' is het uitvoerend bestuur verantwoordelijk voor het toezien op de opvolging van de genomen acties.

## ***Algemeen***

### **Artikel 8 Onvoorziene omstandigheden**

Voor kwesties waarin deze incidentenregeling niet voorziet, beslissen de voorzitter en het uitvoerend bestuur gezamenlijk.

### **Artikel 9 Wijzigingen in deze regeling**

Het bestuur kan deze regeling te allen tijde wijzigen. Tenminste driejaarlijks wordt bezien of de incidentenregeling geactualiseerd dient te worden.



## Bijlage Indeling incidenten

### Bijlage bij de incidentenregeling (inzake artikel 3.2)

#### Niet-financiële risico's

Risicoclassificatie	Beschrijving
Laag	<ul style="list-style-type: none"><li>Niveau dienstverlening van het fonds wordt beïnvloed &gt; beperkte daling tevredenheid stakeholders;</li><li>Risico op interne negatieve / kritische berichtgeving (incl. uitvoerders);</li><li>Opmerkingen van toezichthouders die uitlegbaar / deels weerlegbaar zijn;</li><li>Is te herstellen.</li></ul>
Medium	<ul style="list-style-type: none"><li>Niveau dienstverlening van het fonds wordt beïnvloed &gt; behoorlijke daling tevredenheid stakeholders;</li><li>Risico op negatieve publiciteit richting pensioensector;</li><li>Negatieve reacties vanuit toezichthouders die onvoldoende kunnen worden uitgelegd;</li><li>Is moeilijk te herstellen.</li></ul>
Hoog	<ul style="list-style-type: none"><li>Niveau dienstverlening van het fonds wordt beïnvloed &gt; grote daling tevredenheid stakeholders;</li><li>Risico op negatieve publiciteit richting pensioensector;</li><li>Structureel negatieve reacties vanuit toezichthouders die onvoldoende kunnen worden uitgelegd;</li><li>Erg moeilijk te herstellen.</li></ul>

#### Financiële risico's

Risicoclassificatie	Beschrijving
Laag	< 0,25 bp met een minimum van € 10.000 < € 150.000(*)
Medium	Tussen de 0,25 bp en 2 bp Tussen de € 150.000 en € 1.200.000
Hoog	Meer dan 2 bp Meer dan € 1.200.000

(\*) Op basis van een belegd vermogen van € 6 mld.