Incidenten- en klokkenluidersregeling

Stichting Pensioenfonds SABIC

Datum: 19 mei 2022

Stichting Pensioenfonds SABIC
Het Overloon I, 6411 TE Heerlen • Postbus 6500, 6401 JH Heerlen • **T** +31 (0)45 578 81 00
E info.PensioenfondsSABIC@dsm.com • **I** www.spf-pensioenen.nl • KvK nr. 14076811

Aanleiding en doel
Incidenten kunnen een gevaar vormen voor de integere en beheerste bedrijfsvoering van Stichting Pensioenfonds SABIC (SPF). Deze Incidenten- en klokkenluidersregeling (deze Regeling) geeft aan welke stappen gevolgd worden als het vermoeden bestaat dat sprake is van een incident binnen het fonds. Doel van deze Regeling is het voorkomen van schade aan de beheerste en integere bedrijfsvoering en goede naam van SPF of de voor het fonds werkzame personen, alsmede het beperken van mogelijke gevolgschade.

Daarnaast wil SPF leren van incidenten om herhaling te voorkomen. SPF streeft er naar een betrouwbare, transparante en lerende organisatie te zijn. Het Bestuur van SPF draagt er zorg voor dat de Regeling bekend is bij alle verbonden personen en relevante medewerkers van uitbestedingspartners of andere belanghebbenden.

Deze Regeling combineert Regelingen voor incidenten, misstanden en klokkenluiders.

Regelgeving
Met deze Regeling geeft SPF mede uitvoering aan de vereisten van de Pensioenwet[1] (Pw), het Besluit financieel toetsingskader[2](Bftk), de Wet bescherming klokkenluiders (Wbk) en de Code Pensioenfondsen.

- ***De Pensioenwet***
  Deze schrijft voor dat een pensioenfonds zijn organisatie zodanig inricht dat deze een beheerste en integere bedrijfsvoering waarborgt.
- ***Besluit financieel toetsingskader***
  Omdat sommige incidenten een gevaar (kunnen) vormen voor de beheersing en de integriteit van de bedrijfsvoering, is het van belang dat deze kunnen worden gemeld, zorgvuldig worden vastgelegd en afgehandeld. In het Bftk en de bijbehorende toelichting is dit nader uitgewerkt.
- ***Wet bescherming klokkenluiders***
  Deze wet schrijft voor dat SPF beschikt over een procedure voor de melding van en omgang met meldingen van (vermoeden van) misstanden en inbreuken op de Europese Richtlijn 2019/1937 (Bescherming van personen die inbreuken op het Unierecht melden).
- ***Code Pensioenfondsen***
  In de Code Pensioenfondsen is bepaald dat een bestuur er zorg voor moet dragen dat alle personen die betrokkene zijn bij of financieel afhankelijk zijn van het fonds, zonder gevaar voor hun positie, de mogelijkheid hebben te rapporteren over incidenten van algemene, operationele en financiële aard. Dit kan zowel gaan om incidenten binnen SPF als bij partijen aan wie taken worden uitbesteed. Daarnaast moet duidelijk worden vastgelegd bij wie en op welke wijze hierover gerapporteerd kan worden. Met deze Regeling wordt voorzien in deze eisen.

[1] Artikel 143, Pw.
[2] Artikel 19a, Bftk.

1 Definities

Adviseur

Dit betreft de persoon die een Betrokkene kan raadplegen over een (potentiële) Melding danwel de toepassing van deze Regeling. SPF heeft de Vertrouwenspersoon aangewezen als vaste Adviseur. De Betrokkene kan ook zelf een Adviseur in de arm nemen maar zal dan ook zelf eventuele kosten betalen.

Afdeling advies Huis voor Klokkenluiders:

Dit betreft een externe organisatie waar Betrokkenen advies in kunnen winnen met betrekking tot Misstanden. De afdeling advies staat in zijn geheel los van de meldafdeling van het Huis voor Klokkenluiders, vragen om advies is dus niet hetzelfde als het doen van een Melding.

Bestuur:

Het bestuur van SPF.

Betrokkene:

Iedere persoon die werkzaamheden verricht of heeft verricht voor, dan wel betrokken is of is geweest bij SPF, dit met inbegrip van de verbonden personen.

Betrokken Derde:

Een derde die is verbonden aan een (potentiële) Melder en die zou kunnen worden benadeeld door SPF. Het betreft bijvoorbeeld het meldpunt, de Vertrouwenspersoon of Adviseur.

Bevoegde Autoriteit:

De instantie die naar het redelijk oordeel van de Melder of SPF het meest in aanmerking komt om de externe Melding van het Integriteitsincident bij te doen, bijvoorbeeld Huis voor Klokkenluiders, DNB, AFM, AP of opsporingsinstantie.

Compliance Officer:

De door het Bestuur aangewezen (externe) functionaris die is belast met het houden van toezicht op de naleving van de complianceregelgeving zoals beschreven in het complianceprogramma.

Dagelijks Bestuur:

Het Dagelijks Bestuur van SPF. In deze Regeling acteert het Dagelijks Bestuur in opdracht van het Bestuur.

Incident:

Onder deze definitie vallen zowel Integriteitsincidenten als Operationele Incidenten.

Integriteitsincident, Misstand en Inbreuk op Unierecht:

Integriteitsincident: gedraging of gebeurtenis die een gevaar vormt voor de **integere** uitoefening van het bedrijf van SPF met inbegrip van de bij SPF betrokken (rechts)personen.
Misstanden en Inbreuken op Unierecht kwalificeren in ieder geval als Integriteitsincident.

(Vermoeden van een) Misstand: het vermoeden van een Betrokkene dat binnen SPF of een zakelijke relatie van het fonds, sprake is van een Misstand voor zover het vermoeden gebaseerd is op redelijke gronden, die voortvloeien uit de kennis die de Betrokkene bij SPF heeft opgedaan. Men spreekt van een Misstand wanneer deze:

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 op de naleving van wettelijke regelingen, of wettelijke opsporingsambtenaren beoogt te misleiden;
d. Een gedraging of gebeurtenis die kan leiden tot een groot afbreukrisico in de media;
e. Een ernstig gevaar vormt voor de integere bedrijfsvoering van SPF, hieronder valt in ieder geval:
    - Onheuse bejegening door verbonden personen of andere personen in uitvoering van werkzaamheden voor het fonds
    - Onoorbaar gedrag van verbonden personen in het algemeen,
f. Elke andere gebeurtenis die redelijkerwijs kan worden beschouwd als Misstand.

Inbreuk op Unierecht: een handeling of nalatigheid die:

a. Onrechtmatig is en betrekking heeft op Uniehandelingen en beleidsterreinen die binnen het in artikel 2 van de Europese Richtlijn 2019/1937 (Bescherming van personen die inbreuken op het Unierecht melden) bedoelde materiële toepassingsgebied vallen, of
b. Het doel of de toepassing ondermijnt van de regels in de Uniehandelingen en beleidsterreinen die binnen het in artikel 2 van de Europese Richtlijn 2019/1937 (Bescherming van personen die inbreuken op het Unierecht melden) bedoelde materiële toepassingsgebied vallen.

Melder

Iedere Betrokkene die werkzaamheden verricht of heeft verricht voor, dan wel betrokken is of is geweest bij SPF en die een Melding in het kader van deze Regeling verricht.

Meldpunt Operationele Incidenten

Het Dagelijks bestuur acteert als Meldpunt voor Operationele Incidenten. Bij vermeende betrokkenheid van het Dagelijks bestuur bij het te melden Incident kan de Melding verricht worden bij het Meldpunt Integriteitsincidenten of bij de voorzitter van de Raad van Toezicht.

Meldpunt Integriteitsincidenten

De Compliance Officer acteert als Meldpunt voor Integriteitsincidenten waaronder Misstanden en Inbreuken op Unierecht. Bij vermeende betrokkenheid van het Meldpunt bij het te melden Incident kan de Melding verricht worden bij het Meldpunt Operationele Incidenten dan wel bij de voorzitter van de Raad van Toezicht.

Melding

De Melding van (het vermoeden van) een Integriteitsincident of Operationeel Incident.

Onderzoekscommissie:

Een interne of externe Onderzoekscommissie ter uitvoering van een onderzoek en de behandeling van een Integriteitsincident.

Operationeel Incident:

Gedraging of gebeurtenis die een gevaar vormt voor de **beheerste** uitoefening van het bedrijf van SPF met inbegrip van de bij SPF betrokken (rechts)personen.
Dit staat los van integriteit, het kunnen menselijke fouten zijn of systeemfouten (bijvoorbeeld een IT-storing). Deze fouten zijn incidenten/gebeurtenissen waarbij directe of indirecte financiële schade kan ontstaan door ontoereikende of falende interne processen, operationele fouten (backoffice), verbonden personen of systemen of door externe gebeurtenissen. Hieronder vallen ook de meldingsplichtige datalekken zoals beschreven in de Algemene verordening gegevensbescherming tenzij deze opzettelijk zijn veroorzaakt. In dat geval kan het ook een Integriteitsincident betreffen. In bijlage 1 is de procedure datalekken opgenomen.

Raad van Toezicht

De interne toezichthouder van SPF.

Verbonden persoon

Personen die op grond van de gedragscode als zodanig zijn aangewezen.

Vertrouwenspersoon

Het Bestuur wijst een Vertrouwenspersoon aan.

Zwaar Incident

Een Incident kwalificeert zich als Zwaar Incident als er sprake is van:

a. Een belangrijke invloed op de integere of beheerste bedrijfsvoering;
b. De betrokkenheid van het Openbaar Ministerie;
c. Een aanwijzing van de Toezichthouder, een last onder dwangsom of het voornemen om een bestuurlijke boete op te leggen;
d. Een incident dat een dusdanige impact heeft op SPF dat afhandeling door de Onderzoekscommissie vereist is;
e. Een incident dat door het Bestuur of door de RvT als Zwaar Incident is bestempeld.

2. Algemeen

2.1 Het Bestuur van SPF draagt er zorg voor dat de Incidenten- en klokkenluidersregeling kenbaar is bij en beschikbaar is voor Betrokkenen en Betrokken Derden.

2.2 De Vertrouwenspersoon kan benaderd worden door Betrokkene met vermoedens van een Integriteitsincident of advies over een (potentiële) Melding. De Vertrouwenspersoon treedt in eerste instantie raadgevend op. De Vertrouwenspersoon houdt gesprekken vertrouwelijk en onderneemt geen actie, tenzij hij hier in rechte toe is verplicht of door de Melder schriftelijk wordt gevraagd. De Vertrouwenspersoon rapporteert jaarlijks over zijn werkzaamheden aan het Bestuur. Over de inhoud van gesprekken wordt geen informatie met derden gedeeld, ook niet aan het Bestuur en de Compliance Officer.

2.3 De Betrokkene kan met betrekking tot Misstanden ook advies inwinnen bij de afdeling advies van het Huis voor Klokkenluiders. In dat geval gelden dezelfde voorwaarden, rechten en plichten als wanneer advies wordt ingewonnen bij de aangewezen Vertrouwenspersoon.

3. Melding en meldpunt

Integriteits- en operationele incidenten

3.1 Een Betrokkene kan een Incident schriftelijk, mondeling of digitaal bij het Meldpunt melden. Bij mondelinge Melding zet het Meldpunt de Melding op papier en legt deze ter goedkeuring (per handtekening of bevestiging per mail) voor aan de Melder. De Melder ontvangt in alle gevallen binnen 7 dagen een ontvangstbevestiging van de Melding.

3.2 Het Meldpunt ontvangt de Meldingen en beoordeelt binnen een redelijke termijn of het een Incident betreft in de zin van deze Regeling. Indien het Meldpunt van oordeel is dat de Melding geen Incident betreft deelt hij dit de Melder binnen 14 dagen na ontvangst van de Melding mee.

3.3 Indien het Meldpunt zich onbevoegd acht vanwege de aard van de Melding dan verwijst hij de Melder door naar het bevoegde meldpunt.

3.4 Indien de Melder vermoedt dat het aangewezen Meldpunt betrokken is bij het Incident dan kan hij de Melding verrichten bij:

- Het andere meldpunt of
- De voorzitter van de Raad van Toezicht.

Integriteitsincidenten

3.5 Indien het Meldpunt een Melding krijgt van een Integriteitsincident dan wijst hij de Melder op de beschikbaarheid en rol van de Vertrouwenspersoon.

3.6 De Betrokkene kan het Incident ook melden via de Vertrouwenspersoon. De Vertrouwenspersoon stuurt de Melding, in overleg met de Betrokkene, door naar het Meldpunt waarbij de naam van de Betrokkene alleen bij de Vertrouwenspersoon bekend is.

3.7 Op schriftelijk verzoek van de Melder kan de Vertrouwenspersoon namens hem optreden. Daarom dient vanaf hier in deze Regeling ‘Melder’ in die gevallen ook gelezen te worden als ‘de Vertrouwenspersoon namens de Melder’.

3.8 Het Meldpunt zal, eventueel na een verkort onderzoek, een zienswijze formuleren, zodra hij een Melding van een Melder heeft ontvangen. Deze zienswijze wordt binnen 14 dagen teruggekoppeld aan de Melder en het Dagelijks Bestuur.

3.9 Het Meldpunt zal het Dagelijks Bestuur adviseren over afhandeling van de Melding dan wel het starten van verder onderzoek. In de terugkoppeling van de zienswijze aan het Dagelijks Bestuur zal het Meldpunt de naam van de Melder geheimhouden tenzij hij voor openbaarmaking schriftelijke toestemming heeft van de Melder.

3.10 Indien het Incident volgens het Meldpunt een Zwaar Incident betreft dat gelieerd is aan of betrokkenheid heeft met een lid van het (Dagelijks) Bestuur dan zal het Meldpunt het Incident met de voorzitter van de Raad van Toezicht bespreken.

3.11 De Compliance Officer treedt op als procesbewaker met betrekking tot de afhandeling van integriteitincidenten.

4. Onderzoek

4.1 Indien van toepassing kan het Dagelijks Bestuur namens het Bestuur een onderzoek instellen. Het Dagelijks Bestuur informeert het Bestuur onverwijld over een Melding en het wel of niet instellen van een onderzoek. Indien van toepassing kan het Bestuur het Dagelijks Bestuur gelasten een onderzoek in te stellen. Het doel van het onderzoek is:

a. Waarheidsvinding met betrekking tot het Incident en de daarmee samenhangende bewijsvoering voor disciplinaire, civielrechtelijke en strafrechtelijke vervolgstappen;
b. Beperken van de (potentiële) schade naar een beheersbaar niveau; en
c. Herstel van de bedrijfsvoering, voor zover het Incident daarop enige invloed had.

4.2 Het onderzoek naar het Incident wordt uitgevoerd in opdracht van het Dagelijks Bestuur (of de bestuursvoorzitter dan wel de voorzitter Raad van Toezicht in haar plaats). Bij een Integriteitsincident kan hiertoe een Onderzoekscommissie worden aangewezen met interne en/of externe deskundigen. Als de Melding betrekking heeft op een Incident bij een partij aan wie werkzaamheden zijn of waren uitbesteed, wordt het onderzoek verricht in overleg met of door deze partij. Indien van toepassing wordt een onderzoeksprotocol opgesteld.

4.3 Het onderzoek wordt uitgevoerd onder de volgende voorwaarden:

- De beginselen van de Algemene verordening gegevensbescherming worden in acht genomen.
- Gegevens worden rechtmatig en proportioneel verzameld; van onrechtmatig verkregen gegevens wordt geen gebruik gemaakt.
- Degene naar wie onderzoek wordt gedaan, wordt direct geïnformeerd tenzij dit in het belang van het onderzoek, naar mening van de Onderzoekscommissie, niet gewenst is.
- De gegevens worden zodanig vastgelegd dat hoor en wederhoor kan plaatsvinden, tenzij in redelijkheid kan worden aangenomen dat dit schadelijk kan zijn voor het onderzoek of wanneer de Melder de identiteit niet wil vrijgeven.
- De onderzoekers stellen de Melder in de gelegenheid te worden gehoord, eventueel door tussenkomst van de Vertrouwenspersoon. De onderzoekers dragen zorg voor een schriftelijke vastlegging hiervan.
- De onderzoekers kunnen ook anderen horen. De onderzoekers dragen zorg voor een schriftelijke vastlegging hiervan.
- De Onderzoekscommissie kan binnen de organisatie van SPF alle documenten opvragen en inzien die zij voor het doen van het onderzoek redelijkerwijs nodig acht, met in achtneming van de regels van vertrouwelijke meldingen.

4.4 De Onderzoekscommissie rapporteert de onderzoeksresultaten aan het Meldpunt en het volledige Bestuur (of de Raad van Toezicht in haar plaats). De rapportage bevat een kort relaas van feiten en omstandigheden en, indien vastgesteld is dat sprake is van een Incident, de bewijsvoering daarvoor in hoofdlijnen en een advies met betrekking tot de te nemen maatregel(en).

4.5 Alle Betrokkenen waarborgen een vertrouwelijke behandeling van de Melding en het onderzoek. Informatie mag niet gedeeld worden tenzij dit op grond van de wet of dit beleid noodzakelijk is.

4.6 Het traject tussen Melding en afronding onderzoek duurt maximaal 12 weken. Indien deze termijn wordt overschreden worden betrokken partijen geïnformeerd en wordt de motivatie voor overschrijding van deze termijn vastgelegd.

4.7 De Melder en het Dagelijks Bestuur ontvangen tenminste maandelijks algemene informatie over de voortgang van het onderzoek.

5. Persoonsgericht onderzoek

5.1 Indien een redelijk vermoeden bestaat dat een Verbonden Persoon verantwoordelijk is voor of zich schuldig heeft gemaakt aan een Incident, kan het Bestuur (of de Raad van Toezicht) een persoonsgericht onderzoek doen instellen dat door de onderzoekers uitgevoerd wordt. De persoon waartegen het persoonsgericht onderzoek plaatsvindt wordt onverwijld op de hoogte gebracht van het persoonsgericht onderzoek.

5.2 Een persoonsgericht onderzoek wordt ingesteld binnen een redelijke termijn, nadat voldoende aanwijzingen bekend geworden zijn dat een Incident mogelijk aan een persoon kan worden toegerekend.

5.3 De persoon, naar wie het persoonsgericht onderzoek verricht wordt, is in de gelegenheid zijn zienswijze kenbaar te maken in de vorm van 'hoor' en 'wederhoor' en kan zich juridisch laten bijstaan. Het Bestuur stelt hiervoor een toereikend budget beschikbaar. De zienswijze wordt schriftelijk vastgelegd en door middel van een handtekening of een bevestiging per e-mail vastgesteld door deze persoon.

5.4 De Compliance Officer kan, indien het onderzoek en/of het belang van SPF dit vereist, opdracht geven om bepaalde gegevens of zaken veilig te stellen. Daartoe wordt een belangenafweging gemaakt en schriftelijk vastgelegd. Voor het inzien van persoonlijke informatie is toestemming van het Bestuur vereist met inachtneming van de rechten van Betrokkenen.

5.5 De onderzoekers handelen onafhankelijk en onpartijdig tijdens de uitvoering van de onderzoekswerkzaamheden.

5.6 De onderzoekers zien tijdens de uitvoering van een persoonsgericht onderzoek toe op de in acht te nemen zorgvuldigheid, waarbij de belangen van SPF, het belang van de persoon dan wel de personen op wie het onderzoek zich richt en de belangen van overige Betrokkenen redelijkerwijs in acht worden genomen.

5.7 Na de uitvoering van een persoonsgericht onderzoek brengen de onderzoekers schriftelijk een dringend advies uit aan het Bestuur (of Raad van Toezicht) en de Compliance Officer. Het op schrift gestelde advies wordt door de Compliance Officer bewaard. De Compliance Officer ziet toe op ordentelijke opvolging en afhandeling van het advies.

5.8 Alle relevante documenten worden opgenomen in een dossier, zoals de zienswijze van de verschillende Betrokkenen, rapportages en het op schrift gestelde advies.

6. Standpunt Bestuur en maatregelen

6.1 Het Bestuur (of Raad van Toezicht) neemt op basis van het onderzoeksrapport een standpunt in. Indien het standpunt afwijkt van de conclusies en aanbevelingen of van het dringend advies van de Onderzoekscommissie, dan onderbouwt hij zijn standpunt.

6.2 Alleen in het geval van Operationele Incidenten die niet als Zwaar Incident kwalificeren kan het Dagelijks Bestuur een standpunt innemen en het Incident zonder aanvullend onderzoek sluiten.

6.3 Na de behandeling van elk Incident wordt besloten of en welke maatregelen genomen dienen te worden om herhaling in de toekomst te voorkomen. 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.

De eindverantwoordelijkheid voor de afronding van het Incident en de eventuele getroffen maatregelen ligt bij het Bestuur.

6.4 Zowel het Meldpunt als de Melder worden binnen redelijke termijn maar maximaal 1 week na afronding geïnformeerd over het standpunt van het Bestuur en de eventueel genomen of te nemen maatregelen.

6.5 Indien een Integriteitsincident veroorzaakt is door een Verbonden Persoon, wordt bij het bepalen van de maatregel(en) en sancties in overweging genomen dat een Integriteitsincident als een ernstige schending wordt beschouwd van de vertrouwensrelatie tussen SPF enerzijds en de Verbonden Persoon anderzijds.

6.6 Het veroorzaken van een Integriteitsincident of anderszins daarbij betrokken zijn, kan leiden tot ontheffing uit de functie die de Verbonden Persoon bij SPF vervult dan wel het aanspreken van de uitvoerder aan wie de werkzaamheden zijn uitbesteed. Indien mogelijk sprake is van opzettelijk en ernstige strafbare feiten, zoals misdrijven genoemd in het Wetboek van Strafrecht en de Wet op de economische delicten, wordt in beginsel aangifte gedaan bij justitie of de politie.

7. Escalatie

7.1 Indien de Melder het gedurende het proces niet eens is met het standpunt van het Meldpunt of het Bestuur, dan kan hij het vermoeden van een Zwaar Incident, eventueel met tussenkomst van de Vertrouwenspersoon, melden bij de Raad van Toezicht.

7.2 In plaats van of na het doen van een interne Melding van een vermoeden van een Zwaar Incident, kan de Melder ook direct een externe Melding doen bij een Bevoegde Autoriteit indien:

a. De Melding niet-ontvankelijk is verklaard en de Melder zich niet in de motivatie hiervan kan vinden;
b. De Melder zich benadeeld voelt naar aanleiding van de Melding;
c. De voorgeschreven termijnen worden overschreden zonder bericht waarom deze in redelijkheid worden overschreden;
d. Een eerdere Melding het Zwaar Incident niet heeft weggenomen.

7.3 De Betrokkene kan ook direct een Melding doen bij een Bevoegde Autoriteit wanneer het eerst doen van een interne Melding in redelijkheid niet van hem kan worden gevraagd. Bijvoorbeeld door betrokkenheid van zowel Bestuur als Raad van Toezicht bij het Incident.

8. Bescherming van de Melder tegen benadeling

8.1 SPF zal de Melder niet benadelen in verband met het te goeder trouw en naar behoren intern melden van een (vermoeden van een) Incident, het doen van een Melding bij een Bevoegde Autoriteit of het openbaar maken van dit (vermoeden van) Incident indien aan de voorwaarden van artt. 17e en f Wet bescherming klokkenluiders wordt voldaan.

8.2 Onder benadeling als bedoeld in lid 1 wordt in ieder geval verstaan het nemen van een benadelende maatregel, zoals:

a. Het tussentijds beëindigen of het niet verlengen van een opdracht;
b. Het treffen van een disciplinaire maatregel;
c. Het opleggen van een onderzoek-, spreek-, werkplek- en/of contactverbod aan de Melder of collega's van de Melder;
d. Het uitbreiden of beperken van de taken van de Melder, anders dan op eigen verzoek.

8.3 Artikel 8.1 en 8.2 zijn ook van toepassing op benadeling van Betrokken Derden.

9. Melden aan toezichthouder(s) en overige communicatie

9.1 Zware Incidenten worden onverwijld en tijdig door de bestuursvoorzitter aan de relevante autoriteiten gemeld onder opgaaf van de feiten en omstandigheden van het Incident. De voorzitter informeert de relevante toezichthouder(s) tevens over de maatregelen die naar aanleiding van het Incident zijn genomen of nog zullen worden genomen.

9.2 Het Bestuur beslist over communicatie, zowel intern als extern, met betrekking tot Incidenten. Door het Bestuur wordt besloten of en wanneer andere organen van het fonds, stakeholders en overige belanghebbenden op de hoogte worden gebracht van een Incident.

9.3 De identificatiegegevens van de Melder worden niet opgenomen in communicatie. De identiteit van de Melder zal alleen worden vrijgegeven indien daartoe een wettelijke verplichting bestaat.

10. Incidentenregister

10.1 Het Meldpunt houdt door middel van een incidentenregister een registratie bij van alle binnengekomen Meldingen (inclusief datalekken), de wijze van opvolging, ingestelde onderzoeken, onderzoeksresultaten, de genomen preventieve en repressieve maatregelen en de Meldingen aan de toezichthouder(s).

10.2 Incidentregistraties en onderliggende dossiers worden na afronding van het onderzoek 5 jaar bewaard en vervolgens vernietigd met inachtneming van de rechten van Betrokkenen. Het Bestuur kan besluiten hier om dringende redenen van af te wijken met inachtneming van de rechten van Betrokkenen.

10.3 Het Meldpunt rapporteert jaarlijks aan het Bestuur over het omgaan met het melden van (vermoedens van) Incidenten en de uitvoering van deze Regeling. Deze jaarrapportage bevat in ieder geval:

a. Informatie over het in het afgelopen jaar gevoerde beleid aangaande het omgaan met het melden van (vermoedens van) Integriteitsincidenten en advies over het in het komende jaar te voeren beleid op dit vlak;
b. Informatie over het aantal Meldingen, inclusief de niet-ontvankelijk verklaarde, en een indicatie van de aard van de Meldingen, de uitkomsten van de onderzoeken en de standpunten van SPF;
c. Algemene informatie over de ervaringen met het tegengaan van benadeling van Melders;

d. Informatie over het aantal verzoeken om onderzoek naar benadeling in verband met het doen van een Melding en een indicatie van de uitkomsten van de onderzoeken en de standpunten van SPF.

De rapportage wordt tevens aan het VO, de RvT en de Compliance Officer ter beschikking gesteld.

12. Inwerkingtreding

12.1 Deze Regeling is door Bestuur vastgesteld in de bestuursvergadering van 19 mei 2022 en treedt per deze datum in werking. Deze Regeling vervangt alle voorgaande regelingen.

12.2 Deze Regeling zal op de website van SPF geplaatst worden.

BIJLAGE 1 Procedure datalekken

De meldplicht datalekken houdt in dat Pensioenfonds datalekken onverwijld moet melden aan:

- De Autoriteit Persoonsgegevens (AP),
- In bepaalde gevallen aan de Betrokkene(n), en,
- In bepaalde gevallen aan De Nederlandsche Bank.

Deze procedure beschrijft hoe te handelen binnen Pensioenfonds indien er sprake is van een Datalek of wanneer een Datalek vermoed wordt. De procedure is mede gebaseerd op de beleidsregels van de AP inzake de meldplicht datalekken in de Algemene verordening gegevensbescherming. Per gemeld Datalek wil SPF zich de vrijheid voorbehouden om te beoordelen of de procedure gevolgd kan worden, dan wel afwijking van deze procedure gerechtvaardigd is.

Definities

AP
Autoriteit Persoonsgegevens.

Betrokkene
De geïdentificeerde of identificeerbare natuurlijk persoon op wie een persoonsgegeven betrekking heeft.

Beveiligingslek
Een inbreuk op de beveiliging waarbij persoonsgegevens niet worden blootgesteld aan verlies of onrechtmatige verwerking; er is dan geen sprake van een Datalek.

Datalek
Een inbreuk op de beveiliging (zoals bedoeld in de AVG) waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking; dus blootgesteld aan datgene waartegen beveiligingsmaatregelen bescherming moesten bieden.

Incident
Een mogelijk beveiligingsincident, waardoor de bescherming van Persoonsgegevens op enig moment is doorbroken en waardoor de Persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Het is daarbij niet van belang of de verantwoordelijke passende technische of organisatorische beschermingsmaatregelen heeft getroffen of niet. Ieder Datalek is een Incident, niet ieder Incident is een Datalek.

Persoonsgegeven
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

AVG
Algemene Verordening Gegevensbescherming.

Verwerkingsverantwoordelijke
De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. SPF is de verwerkingsverantwoordelijke.

Verwerking van persoonsgegevens
Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

1. Identificeren Datalek

Met verbonden personen en derden (uitvoerders) is afgesproken om zonder onnodige vertraging, doch uiterlijk binnen 48 uur nadat de Verbonden Persoon of derde (uitvoerder) een (mogelijk) Datalek heeft geconstateerd het Meldpunt bij Pensioenfonds hiervan in kennis te stellen. De Melding omvat:

a. De geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens en (kring van) de Betrokkenen;
b. De maatregelen die zijn getroffen of worden getroffen om de (negatieve) gevolgen van de inbreuk te beperken en te verhelpen.

c. Desgevraagd aanvullende gegevens die SPF nodig heeft om een eventuele Melding bij de toezichthouder te kunnen verrichten.

2. Beoordeling Datalek ja/nee

Op basis van de verkregen informatie en bij vermoeden van een datalek wordt - na advies van de functionaris voor gegevensbescherming (FG) / privacy officer (PO) van het fonds - door het Dagelijks Bestuur zo spoedig mogelijk de beoordeling gemaakt of er daadwerkelijk sprake is van een Datalek. 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 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. Evenmin is een Melding aan de AP nodig als er weliswaar sprake is van een Datalek, maar het Datalek geen beperking oplevert voor de rechten en vrijheden van de Betrokkene. Wel overlegt het Dagelijks Bestuur dan of het zinvol is om het Incident te onderzoeken om herhaling te voorkomen.

Melden aan de Autoriteit Persoonsgegevens

De FG/PO verzorgt namens de verwerkingsverantwoordelijke de tijdige (onverwijld, zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking van het Datalek) elektronische melding bij de AP volgens het online meldingsformulier van de AP. De FG/PO 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 verwerker die betrokken is bij het incident vragen de Melding aan de Autoriteit Persoonsgegevens namens de verwerkingsverantwoordelijke te doen en het Dagelijks Bestuur op de hoogte te houden van de Melding.

3. Beoordeling of Datalek gemeld dient te worden aan Betrokkene(n)

Het Dagelijks Bestuur stelt na advies van de FG/PO vast of het Datalek ook moeten worden gemeld aan degenen om wiens gegevens het gaat.

4. Oorzaken en verbetermaatregelen

De Verbonden Persoon of derde (uitvoerder) is verplicht om bij constatering van een (mogelijk) Datalek, in goed overleg met SPF, alle noodzakelijke maatregelen binnen zijn invloedsfeer te nemen om het (mogelijk) Datalek te dichten en de schade die hieruit voortvloeit of kan vloeien te beperken. De Verbonden Persoon of derde (uitvoerder) zal SPF volledig op de hoogte houden en blijven houden van de ontwikkelingen met betrekking tot een (mogelijk) 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 en op advies van de FG/PO beoordelen of het noodzakelijk is aan de Verbonden Persoon of derde (uitvoerder) te vragen bepaalde aanvullende beveiligingsmaatregelen te treffen. De FG/PO bewaakt de voortgang ten aanzien van eventuele aanvullende beveiligingsmaatregelen.

5. Registratie

De verwerkingsverantwoordelijke houdt een registratie bij van ieder Datalek.