



Stichting Bedrijfstakpensioenfonds voor de Houthandel

Reglement incidentenregeling

Artikel 1 Definities

- Pensioenfonds:* Stichting Bedrijfstakpensioenfonds voor de Houthandel;
- Incident:* een gedraging, datalek of een gebeurtenis die een ernstig gevaar vormt voor de beheerste en integere bedrijfsvoering van het pensioenfonds;
- Compliance officer:* degene die door het pensioenfonds als compliance officer is benoemd;
- Dagelijks bestuur:* de voorzitter en secretaris van het bestuur van het pensioenfonds;
- Verbonden personen:* diegene die een melding doet van een incident of een vermoeden van een incident, zijnde:
- leden en plaatsvervangende leden van het bestuur van het pensioenfonds;
 - leden van het verantwoordingsorgaan van het pensioenfonds;
 - leden van de raad van toezicht van het pensioenfonds;
 - sleutelfunctiehouders en -vervullers
- DNB:* De Nederlandsche Bank.

Artikel 2 Melding Incident

- Elke verbonden persoon is verplicht een incident of een vermoeden van een incident direct te melden aan het dagelijks bestuur. Na beoordeling van het incident of een vermoeden van een incident wordt de compliance officer op de hoogte gebracht. Voor houders van sleutelfuncties geldt de meldingsplicht aan het dagelijks bestuur 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 het dagelijks bestuur over melding aan de toezichthouder. Een dergelijke melding wordt niet afgehandeld conform de hieronder beschreven procedure. Artikel 4 van de klokkenluidersregeling is van overeenkomstige toepassing in geval van melding aan de toezichthouder.
- De melding wordt bij voorkeur schriftelijk of elektronisch gedaan. Een mondelinge melding is ook mogelijk.
- Een melding van een incident of een vermoeden van een incident kan op verzoek van de verbonden persoon anoniem blijven binnen de rest van de organisatie van het pensioenfonds. Anders dan lid 1 geschiedt in geval van een anonieme melding, de melding aan de compliance officer. De compliance officer bespreekt met het dagelijks bestuur de anonieme melding.



4. Elke verbonden persoon is verplicht iedere andere gedraging of gebeurtenis die gevolgen heeft of kan hebben voor de bedrijfsvoering van het pensioenfonds, direct te melden aan de compliance officer. Het kan gaan om een onregelmatigheid van algemene, operationele of financiële aard.
5. Het kan gaan om een gedraging of gebeurtenis zowel binnen het pensioenfonds als bij partijen aan wie werkzaamheden zijn uitbesteed.
6. Onder incident wordt in ieder geval, maar niet uitsluitend, verstaan:
 - a. een gebeurtenis waarbij directe of indirecte financiële schade of reputatieschade ontstaat door ontoereikende of falende interne processen, door verbonden personen of door systemen of door externe gebeurtenissen;
 - b. een (dreigende) bewuste schending van wet- en regelgeving;
 - c. een (dreiging van) bewust onjuist informeren van een publiek orgaan;
 - d. een (dreigende) schending van gedragsregels van het pensioenfonds;
 - e. (een dreiging van) het bewust achterhouden, vernietigen of manipuleren van informatie over deze feiten;
 - f. een gedraging of gebeurtenis die kan leiden tot een groot afbreukrisico in de media;
 - g. fraude, misleiding, bedrog, verduistering of diefstal door een of meer personen in zijn/hun hoedanigheid van verbonden persoon;
 - h. overige (dreigende) strafbare feiten.
7. Indien aanvullende informatie nodig is in het belang van het onderzoek, kan de verbonden persoon worden verzocht zijn medewerking hieraan te verlenen.
8. De compliance officer is belast met het toezicht op de naleving van deze regeling en de behandeling van het incident of het vermoeden van een incident. De melding van een incident of een vermoeden van een incident wordt vertrouwelijk en met grote zorgvuldigheid behandeld.
9. Het dagelijks bestuur beoordeelt in overleg met de compliance officer de melding en neemt vervolgens zo nodig het besluit een nader onderzoek in te (doen) stellen. Indien de melding betrekking heeft op een van de leden van het dagelijks bestuur, dan treedt het plaatsvervangend lid in het kader van deze regeling in zijn plaats.
10. Indien een onderzoek wordt ingesteld, wordt het bestuur daarvan in kennis gesteld.
11. Indien er naar het oordeel van het dagelijks bestuur geen sprake is van een incident, wordt de verbonden persoon hierover direct geïnformeerd.
12. Indien het incident een datalek betreft, dan geldt ook hetgeen in de bijlage opgenomen is.

Artikel 3 Onderzoek

1. 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. het beperken van de (potentiële) schade naar een beheersbaar niveau; en



- c. het herstel van de bedrijfsvoering, voor zover het incident daarop enige invloed had.
2. Het onderzoek naar het incident wordt uitgevoerd door interne en/of externe deskundigen. Als de melding betrekking heeft op een incident bij een partij aan wie werkzaamheden zijn uitbesteed, wordt het onderzoek verricht in overleg met deze partij.
3. De onderzoekers rapporteren de onderzoeksresultaten aan de compliance officer en het dagelijks bestuur. 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).

Artikel 4 Maatregelen

1. Op basis van de onderzoeksresultaten beoordeelt het dagelijks bestuur het incident en besluit in overleg met het bestuur over de te nemen maatregel(en), zoals:
 - a. disciplinaire maatregelen;
 - b. civielrechtelijke maatregelen, zoals regres;
 - c. interne en externe openbaarmaking;
 - d. aanpassing van procedures; en/of
 - e. overige maatregelen voor het herstel van de bedrijfsvoering.
2. Indien een incident veroorzaakt is door een verbonden persoon, wordt bij het bepalen van de maatregel(en) en sancties betrokken dat een incident als een ernstige schending wordt beschouwd van de vertrouwensrelatie tussen het pensioenfonds enerzijds en de verbonden persoon anderzijds.
3. Het veroorzaken van een incident of anderszins daarbij betrokken zijn, kan leiden tot ontslag uit de functie die de verbonden persoon bij het pensioenfonds vervult. Indien 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.
4. Het dagelijks bestuur ziet toe op de implementatie en naleving van nieuwe procedures en maatregelen, die naar aanleiding van het incident getroffen worden.

Artikel 5 Rapportage aan de toezichthouder

1. Het dagelijks bestuur meldt een incident direct aan DNB, onder opgave van de feiten en omstandigheden van het incident, alsmede de informatie over de functie van de betrokken persoon die het incident heeft veroorzaakt.
2. Het dagelijks bestuur informeert DNB tevens over de maatregelen die naar aanleiding van het incident zijn genomen of noch zullen worden genomen.



Artikel 6 Incidentenregister

1. De compliance officer houdt door middel van een incidentenregister een registratie bij van alle binnengekomen meldingen, de wijze van opvolging, ingestelde onderzoeken, onderzoeksresultaten, de genomen preventieve en repressieve maatregelen en de meldingen aan DNB.
2. Het dagelijks bestuur informeert de compliance officer over de maatregelen die naar aanleiding van het incident zijn genomen, alsmede over de meldingen aan DNB.

Artikel 7 Afhandelen melding incident

1. Indien sprake is van een incident wordt binnen een periode van vier weken, vanaf het moment van melding aan het dagelijks bestuur, de verbonden door of namens het dagelijks bestuur schriftelijk op de hoogte gebracht van een inhoudelijk standpunt over het gemelde incident. Daarbij wordt aangegeven welke maatregelen zijn genomen naar aanleiding van het incident.
2. Indien binnen vier weken geen inhoudelijk standpunt over het gemelde incident kan worden gegeven, wordt de verbonden persoon door of namens het dagelijks bestuur hiervan schriftelijk op de hoogte gebracht. Hierbij wordt aangegeven binnen welke termijn een standpunt tegemoet kan worden gezien.

Artikel 8 Rechtsbescherming

Indien het belang van het pensioenfonds, van derden of de bescherming van de eigen positie van de verbonden persoon dit vraagt, wordt het incident door de verbonden persoon gemeld bij de vertrouwenspersoon als misstand conform de klokkenluidersregeling.

Artikel 9 Inwerkingtreding

Dit reglement treedt in werking met ingang van 1 januari 2015 en is laatstelijk gewijzigd op 13 maart 2019



Proces rondom datalek

Definities

<i>AP:</i>	Autoriteit Persoonsgegevens, zijnde het College Bescherming persoonsgegevens als bedoeld in de Wbp;
<i>Beveiligingslek:</i>	een inbreuk op de beveiliging, bedoeld in de Wbp, waarbij persoonsgegevens niet worden blootgesteld aan verlies of onrechtmatige verwerking;
<i>Bewerker:</i>	degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen, bedoeld in Wbp. Hieronder wordt in ieder geval verstaan: organisaties waaraan het pensioenfonds activiteiten of processen uitbesteedt;
<i>Datalek:</i>	een inbreuk op beveiliging, bedoeld in de Wbp, waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking;
<i>Persoonsgegeven:</i>	elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon bedoeld in de Wbp;
<i>Verwerking van Persoonsgegevens:</i>	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 als bedoeld in de Wbp;
<i>Wbp:</i>	Wet bescherming persoonsgegevens.

Melding datalek

1. Met de bewerker wordt een overeenkomst gesloten waarin de procedure datalek beschreven wordt en waarin heldere afspraken worden vastgelegd over de periodieke rapportage, datalek, vervolg uitvoering en monitoring. De inhoud van de overeenkomst voorziet erin dat het bestuur een mogelijk datalek tijdig, doch niet later dan 72 uur na ontdekking van het datalek, kan melden bij de AP.

2. In de overeenkomst worden in ieder geval vastgelegd:

- welke maatregelen zijn genomen om data te beveiligen;
- de maatregelen die de bewerker zal treffen, indien een datalek wordt ontdekt;
- dat de bewerker bij constatering van een datalek, in goed overleg met het pensioenfonds, voor eigen rekening en risico alle noodzakelijke maatregelen zal nemen om het datalek te dichten en de schade die hieruit voortvloeit of kan voortvloeien te beperken;
- dat de bewerker het fonds volledig op de hoogte houdt en blijft houden van de



ontwikkelingen met betrekking tot een datalek en de genomen of te nemen maatregelen om de gevolgen hiervan te beperken en herhaling te voorkomen;

- dat de bewerker het datalek tijdig, doch niet later dan 48 uur na de ontdekking van het datalek, meldt bij het pensioenfonds.

Vaststelling datalek

1. Op basis van de verkregen informatie en bij vermoeden van een datalek wordt door het bestuur zo spoedig mogelijk vastgesteld of er daadwerkelijk sprake is van een datalek. De vaststelling of er sprake is van een datalek, dat gemeld moet worden aan de AP komt tot stand met behulp van de schema's te vinden in de beleidsregels "Meldplicht datalekken in de Wet bescherming persoonsgegevens" van de AP.

2. 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.

3. Er is sprake van een beveiligingslek ingeval het datalek niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens. Melding aan de AP is dan niet aan de orde. Het bestuur overlegt of het zinvol is om het beveiligingslek te onderzoeken ten einde herhaling te voorkomen.

Beoordeling of datalek gemeld dient te worden aan betrokkene(n)

1. Het bestuur stelt vast of datalek gemeld moet worden aan betrokkene(n).

2. Het bestuur maakt gebruik van de schema's in de beleidsregels "Meldplicht datalekken in de Wet bescherming persoonsgegevens van de AP".