Stichting Bedrijfstakpensioenfonds voor De Groothandel in Vlakglas, de Groothandel in Verf, het Glasbewerkings- en het Glazeniersbedrijf

Incidenten- en klokkenluidersregeling

Versie 2.0 23 september 2019

Inleiding

Incidenten kunnen een gevaar vormen voor de integere en beheerste bedrijfsvoering van het fonds. Deze incidenten- en klokkenluidersregeling geeft aan welke stappen worden gevolgd als het vermoeden bestaat dat er sprake is van een incident binnen het fonds. Het doel van deze regeling is het voorkomen van schade aan de beheerste en integere bedrijfsvoering en goede naam van het fonds, alsmede het beperken van mogelijke gevolgschade.

De regeling geeft aan hoe verbonden personen incidenten kunnen melden en hoe met een melding zal worden omgegaan. De regeling bevat waarborgen voor de bescherming van de verbonden persoon die te goeder trouw melding maakt van een incident.

Deze regeling is een onderdeel van het integriteitsbeleid van het fonds.

Artikel 1. Definities

In deze incidenten- en klokkenluidersregeling wordt verstaan onder:

1.1 Bestuur:
Het bestuur van het fonds.

1.2 Bestuursbureau:
Het bestuursbureau dat het bestuur ondersteunt bij het uitoefenen van zijn taken.

1.3 Compliance officer:
De persoon bedoeld in artikel 14 van de gedragscode van het fonds.

1.4 Dagelijks bestuur:
Het dagelijks bestuur van het fonds.

1.5 Fonds:
Stichting Bedrijfstakpensioenfonds voor de Groothandel in Vlakglas, de Groothandel in Verf, het Glasbewerkings- en het Glazeniersbedrijf.

1.6 Incident:
Een gedraging of gebeurtenis die een gevaar vormt voor de integere en beheerste bedrijfsuitoefening van het fonds met inbegrip van de bij het fonds betrokken (rechts)personen. Hierbij ontstaat schade door een ontoereikend of falend intern proces, persoon of systeem of door een externe gebeurtenis. Onder een incident 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 fonds;
- (een dreiging van) het achterhouden, vernietigen of manipuleren van informatie met betrekking tot incidenten;
- een gebeurtenis die kan leiden tot reputatieschade voor het fonds;
- strafbare handelingen door een verbonden persoon die gevolgen kunnen hebben voor de geschiktheid van de betreffende persoon voor een functie bij het fonds, waaronder fraude, misleiding, bedrog, verduistering of diefstal;
- een gedraging of gebeurtenis die valt onder de definitie van zogenoemde datalekken zoals beschreven in artikel 33 en 34 AVG. Ten aanzien van datalekken en het operationele en urgente karakter van een datalek is bijlage -1- aan deze regeling toegevoegd. Deze bijlage bevat de operationele procedure waarlangs het fonds werkt in geval van een datalek.

1.7 Raad van toezicht:
de raad van toezicht van het fonds.

1.8 Toezichthouder:
Een publiek (toezichts)orgaan met jurisdictie ten aanzien van (de activiteiten van) het fonds, waaronder De Nederlandsche Bank (DNB), de Autoriteit Financiële Markten (AFM), Autoriteit Persoonsgegevens (AP) en de Autoriteit Consument en Markt (ACM).

1.9 Verbonden persoon:
a) Een medewerker van het fonds, onafhankelijk van de duur waarvoor of de juridische basis waarop hij werkzaam is;
b) Een (plaatsvervangend) bestuurslid van het fonds;
c) Een lid van het verantwoordingsorgaan van het fonds;
d) Een lid van de raad van toezicht;
e) Degene die voor het fonds werkzaamheden verricht maar niet bij het fonds in dienst is;
f) Een andere persoon die als zodanig is aangewezen door het bestuur of die behoort tot een categorie personen die als zodanig is aangewezen door het bestuur.

1.10 Waar in deze incidenten- en klokkenluidersregeling staat 'hij' of 'zijn' moet tevens worden gelezen 'zij' of 'haar'.

Artikel 2. Melden, beoordelen en vastleggen van incidenten

2.1 Iedere verbonden persoon die een (dreigend) incident of een vermoeden van een (dreigend) incident constateert is gehouden dit te melden aan het bestuursbureau of het dagelijks bestuur. Een melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan. Het bestuursbureau leidt een melding zo spoedig mogelijk door naar het dagelijks bestuur. Daarnaast kan eenieder, ook niet verbonden personen, (dreigende) incidenten of vermoedens daarvan melden aan het bestuursbureau of het dagelijks bestuur.

2.2 Het dagelijks bestuur beoordeelt de melding en bepaalt of er sprake is van een incident. Dit oordeel wordt vastgelegd. Het dagelijks bestuur legt hierover verantwoording af aan het bestuur.

2.3 Voldoet de melding niet aan de criteria zoals gesteld in deze incidenten- en klokkenluidersregeling, of is het dagelijks bestuur van mening dat een andere regeling en/of procedure van toepassing is, dan brengt het dagelijks bestuur de melder hiervan op de hoogte. Dat gebeurt binnen vijf werkdagen na ontvangst van de melding.

2.4 Meldingen van incidenten en de beoordeling van het dagelijks bestuur van het incident worden geregistreerd in het incidentenregister, dat wordt bijgehouden door het bestuursbureau. Gedurende het verdere proces worden in het dossier de naar het oordeel van de compliance officer relevante documenten opgenomen, zoals de communicatie tussen de verschillende betrokkenen, de rapportages en de resultaten van eventueel onderzoek.

2.5 Indien een melding, onderzoek of dergelijke zaken een van de leden van het dagelijks bestuur betreffen, neemt de raad van toezicht de rol van het dagelijks bestuur over.

2.6 Het kan voorkomen dat een melder melding wil maken van een (vermeend) incident, waarbij hij zelf betrokken is of betrokken is geweest. In dat geval is de melder verantwoordelijk voor zijn eigen handelen en zal hij zich niet kunnen beroepen op de bescherming tegen disciplinaire maatregelen en/of strafrechtelijke vervolging.

Artikel 3. Behandeling van incidenten

3.1 Indien het dagelijks bestuur van mening is dat er sprake is van een incident:
- stuurt het binnen vijf werkdagen na ontvangst van de melding een bevestiging aan de melder; en
- brengt het binnen vijf werkdagen na ontvangst van de melding de compliance officer en het bestuur op de hoogte; en
- indien een bestuurslid betrokken is bij het incident, brengt het dagelijks bestuur binnen vijf werkdagen na ontvangst van de melding de raad van toezicht op de hoogte.

3.2 Het dagelijks bestuur coördineert de afhandeling van het incident. Op verzoek biedt het bestuursbureau hierbij ondersteuning. Tijdens het onderzoek naar een incident worden, als een onderzoek naar een of meerdere verbonden personen deel uitmaakt van de werkzaamheden, de regels in acht genomen die gelden voor het verrichten van een persoonsgericht onderzoek als beschreven in artikel 7.

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

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

3.5 Het dagelijks bestuur rapporteert de onderzoeksresultaten (van elkaar gescheiden) aan zowel het bestuur als de melder. De rapportage bevat een kort relaas van feiten en omstandigheden, de bewijsvoering in hoofdlijnen, alsmede het advies met betrekking tot de te nemen maatregel(en). De raad van toezicht ontvangt een kopie van deze rapportage nadat het bestuur en de melder hiervan kennis hebben genomen en binnen een redelijke termijn in staat zijn geweest te reageren.

3.6 Na de behandeling van elk incident worden, ter afronding, door het fonds 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 waarheidsvinding, 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.

3.7 In geval sprake is van strafbare overtredingen wordt in beginsel aangifte gedaan bij justitie of politie.

Artikel 4. Rapportage

4.1 De voortgang van de afhandeling van incidenten wordt periodiek in de vergadering van het bestuur geagendeerd. Het bestuur is eindverantwoordelijk voor het toezien op de opvolging van de genomen acties. Namens het bestuur kan het bestuursbureau toezien op de daadwerkelijke opvolging.

4.2 In de rapportage(s), zoals die periodiek door het dagelijks bestuur 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 5. Spoedeisende gevallen

5.1 Indien de aard van het incident snel handelen vereist is het dagelijks bestuur bevoegd om namens het bestuur een (voorlopig) besluit te nemen. Indien het incident op een bestuurslid betrekking heeft treedt de raad van toezicht in zijn plaats.

5.2 Het dagelijks bestuur dan wel de raad van toezicht is gehouden om de overige bestuursleden 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 6. Melden toezichthouder en overige communicatie

6.1 Door of namens het bestuur worden incidenten onverwijld schriftelijk gemeld aan de relevante toezichthouder, de raad van toezicht en de risicomanagementcommissie. Indien het dagelijks bestuur het incident conform artikel 3 aan de raad van toezicht heeft gemeld, is de raad van toezicht verantwoordelijk voor melding aan de betreffende toezichthouder.

6.2 De toezichthouder, de raad van toezicht en de risicomanagementcommissie 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.

6.3 Het bestuur beslist over de communicatie, zowel intern als extern, met betrekking tot incidenten.

Artikel 7. Persoonsgericht onderzoek

7.1 Als er een redelijk vermoeden bestaat dat een verbonden persoon verantwoordelijk is voor of 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.

7.2 Een persoonsgericht onderzoek wordt ingesteld binnen een redelijke termijn, nadat er voldoende aanwijzingen bekend geworden zijn over de (mogelijke) betrokkenheid van de betreffende verbonden persoon bij het incident.

7.3 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.

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

7.5 Indien het onderzoek en/of het belang van het fonds 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 door het bestuur een belangenafweging gemaakt. Voor het inzien van persoonlijke informatie is toestemming van het bestuur vereist.

7.6 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 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.

7.7 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.

7.8 Alle relevante documenten, daaronder begrepen de zienswijze van de verschillende betrokkenen, rapportages en het op schrift gestelde advies worden opgenomen in een dossier dat wordt bewaard door het bestuursbureau.

Artikel 8. Meldingen en geheimhouding

8.1 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 verbonden persoon is hiertoe niet verplicht.

8.2 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.

8.3 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 en het dagelijks bestuur toegang hebben tot deze gegevens.

8.4 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.

8.5 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 9. Melden bij een vertrouwenspersoon

9.1 Indien een verbonden persoon van mening is dat door melding van een incident het belang van zijn organisatie, van derden of zijn eigen positie in het geding is, kan deze een incident melden aan de vertrouwenspersoon van het fonds.

9.2 Het bestuur heeft de compliance officer aangewezen als vertrouwenspersoon.

9.3 De keuze om te melden aan de vertrouwenspersoon, in plaats van aan het dagelijks bestuur of het bestuursbureau, is aan de melder. De melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan.

9.4 Het is mogelijk om een incident anoniem te melden aan de vertrouwenspersoon. Hierbij worden, voor zover mogelijk, afspraken gemaakt over de wijze waarop de vertrouwenspersoon resultaten van zijn onderzoek zal terugkoppelen aan de melder.

9.5 De vertrouwenspersoon besluit na eigen onderzoek binnen twee weken of mogelijk sprake is van een incident en deelt dit schriftelijk mee aan het dagelijks bestuur en indien mogelijk aan de melder. De identiteit van de melder wordt niet bekend gemaakt aan het dagelijks bestuur.

9.6 De melding van het (mogelijke) incident wordt vervolgens afgehandeld conform deze incidenten- en klokkenluidersregeling.

Artikel 10. Rechtsbescherming

10.1 Het bestuur 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.

10.2 Het bestuur 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 fonds benadeeld wordt, voor zover te goeder trouw gehandeld is.

10.3 Het bestuur draagt er zorg voor dat niemand wordt benadeeld in zijn of haar positie bij het fonds vanwege het uitoefenen van de taken en/of verplichtingen uit deze regeling.

10.4 In geval van intrekking van een melding zal het bestuur, 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.

10.5 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 beschermingsmaatregelen zoals die gelden voor een te goeder trouw handelende verbonden persoon.

Artikel 11. Slotbepalingen

11.1 Deze incidenten- en klokkenluidersregeling die kan worden aangehaald als "Incidenten- en klokkenluidersregeling 2018" is laatstelijk gewijzigd door het bestuur op 22 juni 2018. De wijziging treedt in werking per 25 mei 2018.

11.2 Deze incidenten- en klokkenluidersregeling kan door het bestuur worden gewijzigd.

Bijlage 1: Procedure datalekken

Inleiding
Iedereen heeft recht op eerbiediging en bescherming van zijn persoonlijke levenssfeer en een zorgvuldige omgang met zijn persoonsgegevens. De regels hiervoor zijn vastgelegd in de Wet Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG), welke per 25 mei 2018 in werking zijn getreden. Het fonds hecht grote waarde aan de (bescherming van de) privacy van haar deelnemers, pensioen- en andere aanspraakgerechtigden en aan adequate beveiliging van haar data en heeft hier dan ook passende organisatorische maatregelen voor getroffen. Toch kan het voorkomen dat er een datalek optreedt binnen het fonds of bij één van haar uitbestedingsrelaties.

In deze procedure datalekken worden de volgende begrippendefinities gehanteerd:

Datalek:	een Inbreuk op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 33 en 34 AVG);
Inbreuk:	een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;
Persoonsgegevens:	elk gegeven betreffende een geïdentificeerde of naar een te identificeerbare persoon te herleiden gegeven zoals NAW gegevens, IP-adressen en foto's;
Meldplicht:	indien de Inbreuk een risico inhoudt voor de rechten en vrijheden van de Betrokkene, geldt de wettelijke plicht om de Inbreuk of een vermoeden hiervan binnen 72 uur na ontdekking te melden bij de Autoriteit Persoonsgegevens (AP). Indien de Inbreuk een hoog risico inhoudt voor de betreffende Betrokkene, dient deze Betrokkene tevens onverwijld op de hoogte te worden gesteld;
Betrokkene(n):	de persoon van wie de Persoonsgegevens zijn gelekt en (indien van toepassing) de persoon die ongevraagd kennis heeft genomen van de Persoonsgegevens van een ander.

In deze procedure is uitgewerkt hoe er moet worden gehandeld als een mogelijk datalek wordt geconstateerd door het fonds of wordt gemeld aan het fonds. Uitgangspunt is dat in alle gevallen van een (mogelijk) datalek de desbetreffende uitbestedingspartij het datalek zo spoedig mogelijk, doch uiterlijk binnen 48 uur, meldt aan het fonds en (de daartoe aangewezen persoon door) het fonds het datalek binnen 72 uur meldt aan de Autoriteit Persoonsgegevens en, indien nodig, de betrokkene(n). Het bestuur van het fonds is verantwoordelijk voor de vaststelling van deze procedure, en de opvolging ervan.

Datalekken bij het fonds
1. Als er een datalek wordt geconstateerd of er een vermoeden is dat hiervan sprake is, wordt het datalek per omgaande per e-mail gemeld bij het dagelijks bestuur, het bestuursbureau en de privacy officer van het fonds. De voorzitter van het fonds wordt tevens telefonisch op de hoogte gebracht. Bij afwezigheid van de voorzitter wordt een van de andere leden van het dagelijks bestuur telefonisch op de hoogte gebracht. In dat geval treedt dat andere lid voor de verdere stappen van de procedure in de plaats van de voorzitter.

2. De voorzitter van het fonds neemt onverwijld contact op met de privacy officer over het mogelijke datalek.

3. De voorzitter beoordeelt in samenspraak met de privacy officer of er daadwerkelijk sprake is van een datalek en zo ja, of er sprake is van een datalek waarvan melding gedaan moet worden bij de AP. Bij twijfel wordt er contact gezocht met de AP.

Wanneer is er sprake van een datalek?
Er is sprake van een datalek als er een inbreuk op de beveiliging heeft plaatsgevonden die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.
Voorbeelden van datalekken zijn: een kwijtgeraakte laptop/USB-stick met persoonsgegevens, een inbraak in een databestand door een hacker of het abusievelijk versturen van een persoonlijke pensioenopgave naar een andere deelnemer dan voor wie deze bedoeld is.

Wanneer moet een datalek worden gemeld aan de AP?
Een datalek moet worden gemeld aan de AP indien de datalek een risico inhoudt voor de rechten en vrijheden van de betrokkene(n).

Hiervan is sprake als:
er persoonsgegevens zijn gelekt van gevoelige aard (waaronder gegevens over de financiële of economische situatie van betrokkene, gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene, gebruikersnamen, wachtwoorden, gegevens die misbruikt kunnen worden voor (identiteits-)fraude);
de aard en omvang van het datalek tot (een aanzienlijke kans op) ernstige nadelige gevolgen leidt.

Hierbij is van belang:
Gaat het om veel of gevoelige persoonsgegevens per persoon of om gegevens van grote groepen?
Zijn de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpend?
Worden de persoonsgegevens binnen ketens (zoals binnen de overheid) gedeeld?
Gaat het om persoonsgegevens van kwetsbare groepen?

4. De voorzitter verstrekt de beoordeling of er sprake is van een datalek en, zo ja, of die gemeld moet worden aan de AP, per e-mail aan het bestuur en aan de sleutelfunctiehouder risicobeheer. Het bestuur wordt verzocht binnen 24 uur akkoord te gaan met de beoordeling. Het bestuur heeft met de beoordeling ingestemd, indien een meerderheid van de bestuursleden per e-mail heeft laten weten daarmee akkoord te gaan. Indien er binnen 24 uur geen reactie is ontvangen, wordt het betreffende bestuurslid geacht akkoord te zijn met de beoordeling.

5. Indien uit de beoordeling blijkt dat er sprake is van een datalek dat gemeld moet worden, doet de privacy officer deze melding aan de AP – in overleg met de voorzitter - zonder onredelijke vertraging en indien mogelijk, uiterlijk binnen 72 uur nadat hij kennis van het (mogelijke) datalek heeft genomen. Indien de melding aan de AP niet binnen 72 uur plaatsvindt, gaat de melding vergezeld van een motivering voor de vertraging.

Bij de melding wordt gebruik gemaakt van het webformulier van de AP: **https://datalekken.autoriteitpersoonsgegevens.nl/actionpage**.

Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt. Een melding van een datalek kan achteraf worden ingetrokken als blijkt dat er geen meldplicht bestond.

Inhoud melding

In de melding wordt ten minste het volgende omschreven of meegedeeld:

de aard van de Inbreuk, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;

de naam en de contactgegevens van de voorzitter of een ander contactpunt waar meer informatie kan worden verkregen;

de waarschijnlijke gevolgen van de inbreuk;

de maatregelen die het fonds heeft voorgesteld of genomen om de Inbreuk aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Termijn melding aan AP

Het datalek moet zonder onredelijke vertraging, uiterlijk binnen 72 uur na ontdekking, worden gemeld aan de AP. De termijn voor het melden begint te lopen op het moment dat de verantwoordelijke of een bewerker op de hoogte raakt van een datalek dat mogelijk onder de meldplicht valt. De verantwoordelijke mag, na het ontdekken van het datalek, enige tijd nemen voor nader onderzoek teneinde een onnodige melding te voorkomen. Wat in een concreet geval als ‘zonder onredelijke vertraging’ moet worden aangemerkt zal afhangen van de omstandigheden van het geval.

6. Indien er sprake is van een datalek, beoordeelt de voorzitter in samenspraak met het dagelijks bestuur van het fonds en de privacy officer of het datalek ook aan de Betrokkene(n) moet(en) worden gemeld. Uitgangspunt daarbij is dat er een melding plaatsvindt aan Betrokkene(n). Indien het datalek is ontstaan bij een uitbestedingsrelatie van het fonds, dan kan aan deze uitbestedingsrelatie worden verzocht Betrokkene(n) te informeren. Als er tevens sprake is van een Betrokkene die ongevraagd kennis heeft genomen van de persoonsgegevens van een ander, dan wordt deze Betrokkene door de uitvoeringsorganisatie verzocht de ongevraagd ontvangen informatie terug te sturen (indien deze per post is ontvangen), danwel te vernietigen en dit te bevestigen (indien deze per e-mail is ontvangen). Bij het uitblijven van een reactie zal de uitvoeringsrelatie eenmaal een rappel sturen.

Wanneer melden aan betrokkene(n)?

Het datalek moet onverwijld worden gemeld aan betrokkene(n) indien het waarschijnlijk ongunstige gevolgen zal hebben voor zijn/haar/hun persoonlijke levenssfeer. Het fonds mag na het ontdekken van een mogelijk datalek enige tijd nemen voor nader onderzoek zodat betrokkene(n) op een behoorlijke en zorgvuldige manier kan/kunnen worden geïnformeerd. Als er persoonsgegevens van gevoelige aard zijn gelekt, moet dit in ieder geval worden gemeld.

Het datalek hoeft niet te worden gemeld aan de betrokkene(n) indien één van de volgende situaties zich voordoet:

Er zijn passende technische- en organisatorische beschermingsmaatregelen genomen en deze beschermingsmaatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk betrekking heeft. Met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden zoals adequate encryptie, versleuteling en hashing. Vragen die hierbij relevant zijn:

- Zijn de persoonsgegevens blootgesteld aan vernietiging of aantasting?
- Waren de persoonsgegevens versleuteld op het moment van de inbreuk?
- Is de versleuteling adequaat?
- Is het restrisico acceptabel?

Het datalek zal waarschijnlijk geen ongunstige gevolgen hebben voor de persoonlijke levenssfeer van betrokkene(n).

Er zijn zwaarwegende redenen om de melding aan de betrokkene(n) achterwege te laten. Bijvoorbeeld de mededeling zou onevenredige inspanningen vergen (administratieve lasten zodanig disproportioneel). In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkene(n) even doeltreffend worden geïnformeerd.

7. Indien uit de beoordeling volgt dat de Betrokkene(n) van wie de Persoonsgegevens zijn gelekt geïnformeerd moet/moeten worden, wordt/worden de betrokkene(n) telefonisch en/of door de voorzitter geïnformeerd.
   De verplichting om de betrokkene(n) te informeren kan ook door de AP worden opgelegd. Het fonds zal hieraan gevolg geven.

<u>Inhoud melding aan betrokkene(n)</u>

In de kennisgeving aan de betrokkene(n) moet in ieder geval in duidelijke en eenvoudige taal worden gemeld:

de aard van het datalek;

de instanties waar de betrokkene(n) meer informatie over het datalek kan/kunnen krijgen;

de waarschijnlijke gevolgen van het datalek;

de maatregelen die zijn aanbevolen of genomen om het datalek aan te pakken, waaronder in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen van het datalek.

8. De voorzitter onderzoekt in samenspraak met het dagelijks bestuur en de privacy officer of:
   a) er maatregelen genomen moeten worden om de gevolgen van het datalek (onafhankelijk of deze moest worden gemeld of niet) te beperken.
   b) procedures aangepast moeten worden om nieuwe datalekken te voorkomen.

9. De voorzitter rapporteert de afhandeling van het datalek aan het bestuur in de eerstvolgende bestuursvergadering en informeert het bestuur over de eventueel genomen/nog te nemen maatregelen ter voorkoming van datalekken.

10. De privacy officer documenteert het datalek in een datalekregister, mede op basis van de verkregen input van de uitbestedingsrelatie. Hierin staan in ieder geval de feiten en gegevens van het datalek (oorzaak datalek, soort gegevens die gelekt zijn, het moment van ontdekking van het datalek, op welke wijze het datalek gedicht is, de melding aan de betrokkene(n) e.d.) en verstrekt het datalekregister aan het bestuursbureau en de uitbestedingsrelatie.

11. Het bestuursbureau bewaart de gegevens zoals genoemd in onderdeel 10 minimaal een jaar nadat het datalek aan betrokkene(n) is gemeld. Als er gebruik is gemaakt van de zwaarwegende redenen (en er dus niet is gemeld aan betrokkene(n)) worden de gegevens minimaal drie jaar bewaard. In dit geval wordt minimaal eenmaal per jaar geëvalueerd of het datalek alsnog aan de betrokkene(n) moet worden gemeld of niet.

Datalekken bij uitbestedingsrelaties

Een datalek kan zich ook voordoen bij een partij aan wie het fonds werkzaamheden heeft uitbesteed. Het fonds heeft schriftelijke afspraken gemaakt met de uitbestedingsrelaties over hoe om te gaan met datalekken. Daarbij heeft het fonds vastgesteld dat haar uitbestedingsrelaties procedures hebben opgesteld, zodat het fonds kan voldoen aan de wet- en regelgeving op het gebied van datalekken.

Uitgangspunt blijft dat (het bestuur van) het fonds verantwoordelijk is voor het melden van datalekken.