pensioenfonds
Citigroup

PROCEDURE MELDPLICHT DATALEKKEN

STICHTING PENSIOENFONDS
CITIGROUP NEDERLAND

9 MEI 2022

pensioenfonds
citigroup

Inhoudsopgave

1. Inleiding

Sinds 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Organisaties (zowel bedrijven als overheden) dienen onverwijld een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra zij een (ernstig) datalek hebben. In een aantal gevallen moet het datalek ook worden gemeld aan de betrokkenen (de personen van wie de persoonsgegevens zijn gelekt). De AVG stelt daarnaast eisen aan de eigen registratie van datalekken die zich bij organisaties hebben voorgedaan.

Omdat Stichting Pensioenfonds Citigroup Nederland (hierna: het pensioenfonds) en haar ingeschakelde (sub)verwerkers werken met persoonsgegevens is de AVG van toepassing en derhalve ook de meldplicht datalekken.

Het pensioenfonds) is op basis van de AVG verplicht om alle datalekken te documenteren. Met deze documentatie moet de AP kunnen controleren of het pensioenfonds aan de meldplicht heeft voldaan.

Het doel van de procedure meldplicht datalekken is vast te leggen welke stappen door Het pensioenfonds genomen moeten worden bij het vermoeden van of kennis nemen van een incident dat (mogelijk) aangemerkt kan worden als een datalek.
Het volgende resultaat wordt hiermee nagestreefd:

- het steeds volgen van een eenduidige procedure;
- het zorgvuldig waarborgen van de belangen van het pensioenfonds, het individu dan wel een ander bedrijf dat betrokken is bij het incident, zijnde (mogelijk) datalek;
- het op zorgvuldige en systematische wijze analyseren van een incident, zijnde mogelijk datalek, zodat aanwezige risicomomenten in het proces zichtbaar worden. Centraal staat hierbij het vaststellen van de onvolkomenheden in de (toepassing van) technische en organisatorische beveiligingsmaatregelen, die (mogelijk) hebben kunnen leiden tot het incident;
- het bevorderen van het nemen van passende verbetermaatregelen en het structureel borgen van deze verbetermaatregelen;
- het realiseren van een voldoende en eenduidige interne en op verzoek externe verantwoording over de afhandeling van een incident, zijnde een (mogelijk) datalek.

In de onderstaande procedurebeschrijving zijn de te doorlopen stappen verwoord.

Het Bestuur evalueert driejaarlijks of de procedure meldplicht datalekken bijstelling behoeft. Jaarlijks, of na elke relevante wijziging van omstandigheden, wordt deze procedure door de Uitvoerend Bestuurders beoordeeld en indien noodzakelijk geactualiseerd. Mochten daaruit beleidswijzigingen voortkomen, worden deze voorgelegd aan het Bestuur en wordt daarmee een evaluatie.
De procedure meldplicht datalekken is laatstelijk gewijzigd op 9 mei 2022 door de Uitvoerend Bestuurders en vervangt alle voorgaande versies.

2. Datalek

De AP omschrijft een datalek als volgt:

Bij een datalek gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens bij een organisatie. Of om vernietiging, verlies, wijziging of vrijkomen van persoonsgegevens. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens en verlies van (toegang tot) persoonsgegevens.

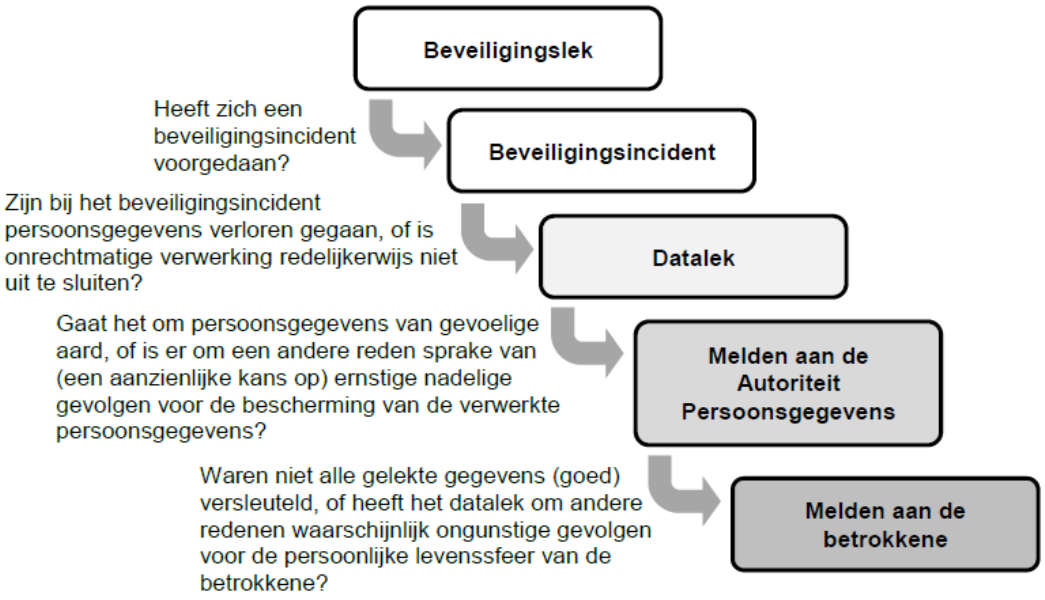
Er zijn drie categorieën datalekken te onderscheiden:

- *Inbreuk op de vertrouwelijkheid*
  Wanneer er sprake is van een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens.
- *Inbreuk op de integriteit*
  Wanneer er sprake is van een onbevoegde of onopzettelijke wijziging van persoonsgegevens.
- *Inbreuk op de beschikbaarheid*
  Wanneer er sprake is van een onbevoegd of onopzettelijk verlies van toegang tot, of vernietiging van, persoonsgegevens

Niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als de onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs is uit te sluiten. Als alleen sprake is van ontdekking van een zwakke plek in de beveiliging, dan is geen sprake van een datalek, maar van een beveiligingslek. In dat geval hoeft geen melding te worden gedaan aan de Autoriteit Persoonsgegevens.

3. Wanneer melden?

De persoon die binnen Het pensioenfonds een mogelijk datalek ontdekt, dient dit te melden aan de Uitvoerend Bestuurders. De Uitvoerend Bestuurders melden het datalek onverwijld en schriftelijk aan de Functionaris gegevensbescherming (FG). De FG beoordeelt of daadwerkelijk sprake is van een datalek en of, in het geval daarvan sprake is, een melding moet worden gedaan aan de AP en betrokkene(n). Voor een gedetailleerde beschrijving van de afweging die moet worden gemaakt bij de beoordeling of een melding aan de AP en betrokkene(n) moet worden gedaan, wordt verwezen naar de Beleidsregels van de AP. Het onderstaande schema geeft in het kort deze afwegingen weer.



NB. Er is een overzicht met voorbeelden beschikbaar waarin aan de hand van stroomschema´s (het melden van) een datalek nader wordt uitgewerkt (bijlage 3).

4. Melden aan de Autoriteit Persoonsgegevens

Niet ieder datalek hoeft te worden gemeld aan de AP. Wanneer een datalek mogelijk ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens dient een melding van aan de AP te worden gedaan.

De Algemene verordening gegevensbescherming (AVG) geeft aan dat een persoonsgegeven alle informatie is over een geïdentificeerde of identificeerbare natuurlijke persoon.

Een factor die een rol speelt, is de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is over het algemeen een melding noodzakelijk. Persoonsgegevens van gevoelige aard zijn bijvoorbeeld:

- Bijzondere persoonsgegevens zoals bedoeld in artikel 9 AVG.
  Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag..
- Gegevens over de financiële of economische situatie van de betrokkene.
  Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris, pensioen en betalingen.
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene.
  Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- Gebruikersnamen, wachtwoorden en andere inloggegevens.
  De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- Gegevens die kunnen worden misbruikt voor (identiteit)fraude. Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (BSN).

Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. Maar let op: als de aard van de gelekte gegevens daar aanleiding toe geeft, is het zelfs mogelijk dat een datalek moet worden gemeld waarbij de persoonsgegevens van slechts één persoon betrokken zijn.

De melding moet worden gedaan zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek. Indien de melding aan de AP niet binnen 72 uur plaatsvindt, gaat de melding vergezeld van een motivering voor de vertraging. Een melding wordt gedaan via het meldloket datalekken van de AP. Via dit loket kan de melding later nog worden aangevuld of ingetrokken.

5. Melden aan betrokkenen

Indien een datalek moet worden gemeld aan de AP, betekent dit niet automatisch dat dit datalek ook moet worden gemeld aan de betrokkene(n). Een datalek dient te worden gemeld aan de betrokkene(n) als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

De melding aan de betrokkene dient onverwijld te worden gedaan, zodat de betrokkene(n) naar aanleiding van de melding maatregelen kan (kunnen) nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder de betrokkene daarover geïnformeerd is, hoe eerder deze in actie kan komen. Bij onevenredige grote inspanning om per individu te informeren, mag een "openbare mededeling" worden gedaan, denk daarbij aan melding via de website van het pensioenfonds. De keuze hieromtrent zal afhangen van de risico's die betrokkenen lopen.

Als er passende technische beschermingsmaatregelen zijn genomen (zoals encryptie en hashing), waardoor de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kan de melding aan de betrokkene(n) achterwege blijven.

Een melding aan betrokkene dient ten minste de volgende onderdelen te bevatten (eventueel gefaseerd, voor zover informatie nog niet voorhanden is):

- Wat voor soort datalek het betreft;
- Of er gegevens in handen van onbevoegden zijn gekomen, verloren zijn gegaan, of anderszins gegevens zijn gelekt;
- Of vaststaat dat er gegevens zijn gelekt. Indien dit niet het geval is, hoe waarschijnlijk of onwaarschijnlijk het is dat gegevens zijn gelekt;
- De aard van de gegevens zijn gelekt: "gewone" (NAW) gegevens of "gevoelige" gegevens (pensioen- of salarisgegevens, BSN);
- Hoeveel (bij benadering) personen het betreft;
- Uit welke bestanden gegevens zijn gelekt;
- Het mogelijke misbruik dat iemand van de gelekte gegevens zou kunnen maken
- hoe groot het risico is dat dit ook daadwerkelijk gebeurt;
- Welke maatregelen zijn getroffen om de eventuele nadelige gevolgen te beperken;
- Welke maatregelen er zijn getroffen/ welke voorgenomen maatregelen zijn er om het datalek te verhelpen?

NB: Er is een standaardbrief beschikbaar om betrokkene(n) te informeren in verschillende situaties (bijlage 2).

6. Vervolgstappen

Zodra de melding aan de AP en eventueel aan de betrokkene(n) is gedaan, is voldaan aan de meldplicht en zal de FG het privacy-incident afsluiten. Indien een melding aan de AP wordt gedaan, wordt eveneens het bestuur hiervan op de hoogte gesteld.

Indien nodig zullen de Uitvoerend Bestuurders verder onderzoek laten doen naar oorzaken van het datalek en de maatregelen die moeten worden getroffen om de beveiliging aan te scherpen. In het geval een dergelijk nader onderzoek nodig is zal de FG het security-incident pas afsluiten na afronding van het onderzoek.

De FG houdt een register datalekken bij van alle gemelde datalekken en de actuele status daarvan. Het register datalekken wordt digitaal gearchiveerd en wordt gedurende één jaar na afsluiting bewaard. Indien er om zwaarwegende redenen geen melding is gedaan aan betrokkene(n) worden de gegevens minimaal drie jaar bewaard.

7. Melden bij De Nederlandsche Bank

De Nederlandsche Bank (DNB) hanteert de volgende algemene formulering met betrekking tot incidenten die door het pensioenfondsen dienen te worden gemeld bij DNB:

Volgens artikel 19a van het Besluit financieel toetsingskader is een incident een gedraging of gebeurtenis, die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van een fonds. Naast incidenten die plaatsvinden bij het fonds zelf, kunnen ook incidenten bij de pensioenuitvoeringsorganisatie (PUO) een ernstig gevaar vormen voor de integere uitoefening van het bedrijf van het fonds. Als zich bij de PUO een incident voordoet, dan zou dit aan het fonds gemeld moeten worden. Fondsen kunnen een meldingsplicht in de overeenkomst tot uitbesteding regelen.

Als toelichting geeft DNB daar de volgende uitleg bij.

1. *Incidenten met betrekking tot een beheerste en integere bedrijfsvoering.* Denk bijvoorbeeld aan het overtreden van toezichtwetgeving of de betrokkenheid van het bestuur of een werknemer van uw onderneming bij een ernstig strafbaar feit, zoals fraude, corruptie of belangenverstrengeling.

2. *IT-incidenten.* Denk bijvoorbeeld aan de verstoring van internetbankieren door een aanval van cybercriminelen en/of het uitlekken van persoonlijke informatie van klanten door een beveiligingslek.

3. *Bestuurscrisis/ governance*. Denk bijvoorbeeld aan een onverwacht vertrek van een bestuurder of commissaris.

4. *Relatie met de toezichthouder*. Bijvoorbeeld als de instelling DNB doelbewust niet of onjuist informeert over onderwerpen die relevant zijn voor het toezicht.

Met name bullit 1 en 2 zijn van belang in relatie tot de meldplicht datalekken volgens de AVG. Hierbij kan worden gedacht aan:

- Een werknemer die persoonsgegevens ontvreemd;
- Een USB stick met gevoelige persoonsgegevens die wordt verloren;
- Malware, ransomware, hacking, etc op de systemen van (sub)verwerkers waarbij gevoelige persoonsgegevens worden buitgemaakt

Incidenten dienen "onverwijld" aan DNB te worden gemeld, zoals dit is omschreven door DNB.

De wettelijke meldplicht treedt in werking zodra een betaalinstelling op de hoogte raakt van het incident. Betaalinstellingen kunnen incidenten aan DNB melden via **infobetaalinstelling@dnb.nl** of de eigen accountmanager van DNB benaderen voor vragen.

8. Procedure meldplicht datalekken

Tussen het pensioenfonds, haar (sub)verwerkers en de FG zijn met betrekking tot de meldplicht datalekken de volgende afspraken gemaakt:

1. (sub)verwerker registreert alle beveiligingsincidenten en datalekken;
2. In geval van een datalek informeert (sub)verwerker de FG en het pensioenfonds zelf zo spoedig mogelijk na ontdekking van het (mogelijke) datalek, doch uiterlijk binnen 36 uur en zal de (sub)verwerker de relevante informatie over het incident melden aan de hand van de hieronder opgenomen vragenlijst. Deze vragenlijst is gebaseerd op het meldformulier van de AP.

   Onder "informeert", wordt verstaan:
   a. Een email bericht naar de contactpersonen van het pensioenfonds en de FG, waarbij het formulier digitaal wordt ingevuld en meegezonden
   b. Een telefonisch contact met zowel één van de contactpersonen van het pensioenfonds als de FG
3. De FG zal beoordelen of een melding verricht dient te worden bij de AP. De FG zal daarbij in overleg treden met het pensioenfonds en ook (sub)verwerker;
4. Indien de FG oordeelt dat tevens betrokkenen geïnformeerd dienen te worden, zal de FG de inhoud van die informatie met het pensioenfonds en ook de (sub)verwerker bespreken. Het pensioenfonds zal de betrokkene informeren middels het aan de procedure meldplicht datalekken gehechte modelbrief 'melden datalek betrokkene';
5. De Uitvoerend Bestuurders besluiten of zij het advies van de FG al dan niet volgen (indien nodig wordt bij dit besluit het voltallige Bestuur betrokken);
6. Indien noodzakelijk meldt de FG het geconstateerde datalek bij de AP, binnen 72 *) uur na constatering door de (sub)verwerker;
7. De FG vult het formulier in met tijdstippen van de diverse meldingen, opvolgende acties, etc.;
8. De FG deelt de documenten met het pensioenfonds en ook de verwerker;
9. De FG werkt het register datalekken bij (ook voor datalekken die niet bij de AP hoeven te worden gemeld) en deelt deze met het pensioenfonds;
10. Er wordt vastgesteld of er een meldplicht van het datalek bij De Nederlandsche Bank (DNB) is. Het pensioenfonds verzorgt de melding bij DNB, zo nodig met input vanuit de FG.

*) De genoemde periode van 72 uur, betekent niet dat het eventuele onderzoek volledig dient te zijn afgerond. Het betreft dus alleen de melding bij de AP. In voorkomende gevallen kan een eerder bij de AP gemeld datalek op een later tijdstip nog worden aangepast, dan wel verwijderd.

De contactpersonen bij Stichting Pensioenfonds Citigroup Nederland voor de meldplicht datalekken zijn:

Vanuit bestuur:
Naam: Linda Gastelaars (Uitvoerend Bestuurder)
Email: **linda.gastelaars@gprmanagement.nl**
Telefoon: 06-4742 6263

Naam: Hedwig Peters (Uitvoerend Bestuurder)
Email: **info@hedwigpetersconsulting.nl**
Telefoon: 06- 5589 5860

Functionaris Gegevensbescherming
Naam: Jan Schilt
Email: **JanSchilt@p1p2.nl**
Telefoon: 06-33376833
Adres: Weegschaalstraat 3
5632 CW Eindhoven

Backup FG
Naam: Hubert Jan Lambooy
Email: **h.lambooy@icloud.com**
Telefoon: 06-31681078

pensioenfonds
Citigroup

Bijlage 1

Vragenlijst melding datalek Stichting Pensioenfonds Citigroup Nederland – bij procedure meldplicht datalekken.

Document digitaal invullen (in Word versie)

Melder:
Naam : .....
Functie : .....
Telefoonnummer: .....
e-mail : .....

Tijdlijn

Duurt de inbreuk op dit moment nog voort?
Kies er een

Wanneer werd de inbreuk ontdekt?

Aard van de inbreuk

Inbreuk op de vertrouwelijkheid van de gegevens (ongeoorloofde of onbedoelde toegang tot gegevens)
Kies er een

Inbreuk op de integriteit van de gegevens (ongeoorloofde of onopzettelijke wijziging van gegevens)
Kies er een

Inbreuk op de beschikbaarheid van de gegevens (ongeoorloofde of onopzettelijke verlies van toegang tot gegevens of verlies van gegevens zelf)

Kies er een

Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?
Kies er een

pensioenfonds
citigroup

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest (graag duidelijk omschrijven zodat de leze goed begrijpt wat er is voorgevallen). Graag geen persoonsgegevens zoals naam, adres, etc vermelden.

Persoonsgegevens die betrokken zijn bij het datalek

Persoonsgegevens in het algemeen

Naam
Kies er een

Geslacht, geboortedatum en/of leeftijd
Kies er een

Burgerservicenummer (BSN)
Kies er een

Contactgegevens
Kies er een

Toegangs- of identificatiegegevens
Kies er een

Financiële gegevens
Kies er een

(Kopieën van) paspoorten of andere legitimatiebewijzen
Kies er een

Locatiegegevens
Kies er een

Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen
Kies er een

Onbekend / anders, namelijk:

Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt
Kies er een

Persoonsgegevens waaruit iemands politieke opvattingen blijken
Kies er een

Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken
Kies er een

Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt
Kies er een

Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid
Kies er een

Gegevens over iemands gezondheid
Kies er een

Genetische gegevens
Kies er een

Biometrische gegevens
Kies er een

Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk

De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

Werknemers (inclusief gewezen deelnemers/ partners/ gepensioneerden)
Kies er een

Klanten (huidig en potentieel)
Kies er een

Minderjarigen
Kies er een

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

pensioenfonds
Citigroup

Bijlage 2

Modelbrief melden datalek betrokkene – bij procedure meldplicht datalekken.

[OP BRIEFPAPIER FONDS]

Aan:
Naam
Adres

Plaats, datum

Betreft: Mogelijk verlies van uw persoonsgegevens

Geachte [heer/mevrouw] [naam betrokkene],

Bij dezen informeren wij u over het volgende. Op [datum] heeft er bij één van de bedrijven die diensten aan ons pensioenfonds verleent, een beveiligingsincident plaatsgevonden. Het incident achten wij dusdanig ernstig dat wij hebben gemeend u hier persoonlijk van op de hoogte te moeten stellen. Wij hebben helaas moeten constateren dat [omschrijving incident, bijvoorbeeld portal is gehackt, mailing aan verkeerde personen, etc]. Wij bieden u onze welgemeende excuses aan.

Wij hebben direct de volgende maatregelen genomen: [maatregelen die zijn genomen bijvoorbeeld: Het personeel geïnformeerd]. Hiermee hebben wij beoogd dat een verdere verspreiding van of toegang tot uw persoonsgegevens onmogelijk is.

>*Variant 1*: Wij kunnen echter niet volledig uitsluiten dat hierbij uw persoonsgegevens [benoem welke gegevens] in handen zijn gekomen van onbevoegde personen. Dat betekent dat u risico loopt op identiteitsfraude, hacking, toegang tot uw email, etc. Om deze reden verzoeken wij u om gebruikersnamen en/ of wachtwoorden aan te passen. Mocht het zo zijn dat u één gebruikersnaam/ wachtwoord heeft voor al uw accounts bij alle dienstverleners waar u gebruik van maakt, dan dient u deze allemaal aan te passen.

>*Variant 2*: Helaas hebben wij moeten vaststellen dat hierbij uw persoonsgegevens [benoem welke gegevens] waarschijnlijk in handen zijn gekomen van onbevoegde personen. Wij hebben, voor zover mogelijk, de betreffende persoon/ personen geïnformeerd over de situatie. Wij hebben gevraagd of zij de gegevens als niet verzonden willen beschouwen en de gegevens die men ten onterechte heeft ontvangen wil vernietigen.

Wij hebben het incident bij de Autoriteit Persoonsgegevens gemeld. Mocht u meer informatie wensen of vragen hebben, neemt u dan gerust contact op met de <naam/ FG>, deze is bereikbaar op telefoonnummer <nummer> of per e-mail: <e-mailadres>.

Met vriendelijke groet,
Stichting Pensioenfonds Citigroup Nederland

<Naam> (voorzitter)

Bijlage 3

Voorbeelden van datalekken

Nr	Korte beschrijving (mogelijke) gebeurtenis	Is er sprake van een datalek?	Melden aan AP/ betrokkene en zo ja; wie meldt aan wie?	Mogelijke maatregelen/ verbeteracties?
	PERSOONSVERWISSELINGEN			
1	Een brief met daarin persoonsgegevens wordt naar een verkeerd adres gestuurd. De brief wordt ongeopend retour ontvangen.	Er is geen sprake van een datalek omdat er geen gegevens verloren zijn gegaan en ook redelijkerwijs valt uit te sluiten dat er persoonsgegevens onrechtmatig zijn verwerkt (lees: ingezien door een onbevoegde).	Dit hoeft niet gemeld te worden aan de AP. Dit hoeft ook niet gemeld te worden aan de betrokkene.	Herzien procedure voor omgang met gegevens van betrokkene. Eventueel, bij recidive, disciplinaire maatregel treffen.
2	Een email met persoonsgegevens wordt verzonden aan de verkeerde ontvanger.	Er is sprake van een datalek, de gegevens van een persoon zijn immers bij de verkeerde (onbevoegde) persoon terecht gekomen	Dit dient, in beginsel, te worden gemeld bij de AP (overleg met de FG). Dit hoeft niet te worden gemeld aan betrokkene, tenzij er een hoog risico is op rechten en vrijheden van de betrokkene.	Medewerkers nogmaals wijzen op hoe om te gaan met persoonsgegevens.
	ONBEVEILIGDE GEGEVENSUITWISSELING			
3	Het pensioenfonds ontvangt van een werkgever regelmatig bestanden met persoonsgegevens die bestemd zijn voor de adviseur van de werkgever. Na meerdere keren aan de bel te hebben getrokken bij de werkgever, zowel telefonisch als per mail, neem het aantal af, maar stopt het niet.	Dit is een datalek. Het betreft hier twee aspecten: (1) Verzending van persoonsgegevens (2) inzicht in gegevens van betrokkene waar het pensioenfonds geen "relatie" mee heeft.	Het pensioenfonds meldt het geconstateerde datalek bij de werkgever. De werkgever moet melding maken van het datalek bij de AP. De werkgever moet het datalek beoordelen of betrokkene geïnformeerd moet worden.	Nee, het betrof de constatering van een datalek bij een externe partij.

	VERLIES, ONTVREEMDING			
4	Een medewerker van Het pensioenfonds verliest een laptop met onversleutelde persoonlijke gegevens van (betrokkene van) van het pensioenfonds.	Er is sprake van een datalek. Onrechtmatige verwerking van persoonsgegevens valt in dit voorbeeld niet uit te sluiten omdat de gegevens niet waren versleuteld.	Het pensioenfonds meldt aan de AP omdat persoonsgegevens zijn gelekt (onbevoegde kennisname). Het Pensioenfonds meldt aan de betrokken omdat het datalek ongunstige gevolgen kan hebben voor de persoonlijke levenssfeer van betrokkene.	Naar aanleiding van dit incident de overige laptops adequaat versleutelen. Realiseer een back-up voor alle laptops in gebruik. Diefstal van een, al dan niet versleutelde, laptop met gegevens van betrokkene waarvan geen back-up aanwezig is, vormt ook een datalek omdat persoonsgegevens verloren zijn gegaan.
	SAMENWERKINGSVERBANDEN/ SUBVERWERKERS			
5	Een medewerker van het schoonmaakbedrijf dat is gecontracteerd door het pensioenfonds is bij de werkzaamheden alleen (zonder andere aanwezigen) in een ruimte geweest waar dossiers van betrokkene ter inzage lagen of een computerscherm met een deel van een dossier betrokkene openstond.	Dit is een datalek. Onrechtmatige verwerking van persoonsgegevens (kennisneming door onbevoegden) valt redelijkerwijs niet uit te sluiten.	Het pensioenfonds meldt aan de AP, want er valt niet uit te sluiten dat gegevens van gevoelige aard zijn ingezien door een onbevoegde. Het pensioenfonds meldt aan de betrokkene.	Instrueren van medewerkers van Het pensioenfonds over het belang van vergrendelen bij vertrek dan wel het archiveren van dossiers achter slot en grendel. Aanpassen PC instellingen Automatisch afmelden. Een geheimhoudingsclausule opnemen in de overeenkomst met het schoonmaakbedrijf.

	ICT - GERELATEERD			
6	Een ICT-leverancier van een informatiesysteem meldt het Pensioenfonds dat door een onvolkomenheid in de beveiliging van hun systemen derden gedurende een korte periode, potentieel inzage hebben gehad in de gegevens van betrokkene(n).	Er is sprake van een datalek gedurende een zekere periode. Kennisneming door onbevoegden kan redelijkerwijs niet meer worden uitgesloten.	Het Pensioenfonds meldt aan de AP, want hier is sprake van 'gevoelige gegevens' en verlies van controle daarover. Het Pensioenfonds maakt vooralsnog geen melding van het incident aan zijn betrokkene, tenzij de AP hier anders over oordeelt. Zwaarwegende reden in deze kwestie lijkt dat er geen concrete aanwijzing is voor feitelijke inzage door een onbevoegde. Door geen melding te maken aan betrokkenen kan onnodige onrust onder een grote groep betrokkene worden voorkomen. Dit zal van geval tot geval verschillen.	Verhelpen van het beveiligingslek. Controleren via de logbestanden. In de bewerkersovereenkomst - tussen de ICT-leverancier (verwerker) en het Pensioenfonds (verantwoordelijke) – kan worden opgenomen wie van beide partijen aan de AP meldt.
7	Er is een phishing mail binnengekomen bij een medewerker waarbij een gebruikersnaam en wachtwoord lijken te zijn buitgemaakt. Er is daarom een risico dat ongeoorloofd gebruik van systemen.	Alhoewel er nog geen directe sprake van een datalek hoeft te zijn, is dit een kritieke situatie.	Indien de IT afdeling kan bevestigen en aantonen dat er geen gebruik is gemaakt van het betreffende account door anderen dan de eigenaar zelf, is er geen sprake van een datalek.	Wachtwoord zo snel mogelijk aanpassen en medewerkers informeren over risico's phishing mails.