



---

# Incidentenregeling

---

Versie 0.5

[24-09-2024]

## Document management

| Datum      | Verandering                                  | Auteur                | Review  | Versie |
|------------|----------------------------------------------|-----------------------|---------|--------|
| 21-9-2020  | Eerste versie                                | Bestuursondersteuning |         | 0.1    |
| 12-2-2021  | Initiële definitieve versie                  | Communicatiecommissie | Bestuur | 0.2    |
| 30-1-2023  | Aanpassen nav bestuursvergadering 12-02-2021 | Bestuursondersteuning | CC      | 0.3    |
| 26-08-2024 | Actualiseren nav DORA                        | Bestuursondersteuning | DB      | 0.4    |
| 24-09-2024 | Aanpassing na review DB                      | Bestuursondersteuning | Bestuur | 0.5    |

## Inhoudsopgave

|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| Inleiding .....                                                               | 4  |
| Definities .....                                                              | 5  |
| Melden incidenten .....                                                       | 6  |
| Melding en registratie van de melding.....                                    | 6  |
| Behandeling van de melding .....                                              | 7  |
| Afhandelen incidenten .....                                                   | 7  |
| Persoonsgericht onderzoek.....                                                | 9  |
| Informatieverschaffing aan de toezichthouder(s) en overige communicatie ..... | 9  |
| Rechtsbescherming .....                                                       | 10 |
| Rapportage .....                                                              | 10 |
| Onvoorziene omstandigheden .....                                              | 11 |
| Wijzigingen in deze regeling .....                                            | 11 |

## Inleiding

Incidenten kunnen een gevaar vormen voor de integere en beheerste bedrijfsvoering van de Stichting Pensioenfonds Capgemini Nederland (hierna: het fonds).

Deze Incidentenregeling geeft aan welke stappen gevolgd worden als er 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 het fonds, alsmede het beperken van mogelijke gevolgschade. Daarnaast wil het Fonds leren van Incidenten om herhaling van dezelfde Incidenten of vergelijkbare situaties te voorkomen. Het Fonds streeft er naar een betrouwbare, transparante en lerende organisatie te zijn. Daarbij past een cultuur waarin Incidenten kunnen worden gemeld, eventueel anoniem, en waarin helder is hoe met deze meldingen zal worden omgegaan.

De Pensioenwet schrijft voor dat een pensioenfonds zijn organisatie zodanig inricht dat deze een beheerste en integere bedrijfsvoering waarborgt. Onderdeel hiervan is het beheerst omgaan met incidenten en de bijbehorende risico's. Hierbij versterkt de Digital Operational Resilience Act (DORA) de beheerste en integere bedrijfsvoering op gebied van ICT.

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 artikel 19a van het Besluit Financieel Toetsingskader Pensioenfondsen (Besluit FTK) en de bijbehorende toelichting is dit nader uitgewerkt. Het Besluit FTK voor pensioenfondsen stelt dat pensioenfondsen een systematische analyse moeten maken van integriteitrisico's en dat ten minste beleid, procedures en maatregelen aanwezig moeten zijn ten aanzien van integriteitgevoelige functies en Incidenten.

De Code Pensioenfondsen bepaalt dat een bestuur er voor zorg 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 onregelmatigheden van algemene, operationele en financiële aard. Dit kan gaan om onregelmatigheden zowel binnen het pensioenfonds 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.

## Inwerkingtreding

Deze regeling is door het Dagelijks Bestuur vastgesteld en treedt in werking op 4 oktober 2024 en is laatstelijk gewijzigd op [26-08-2024]

## Definities

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fonds                    | Stichting Pensioenfonds Capgemini Nederland                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Dagelijks bestuur        | Het Dagelijks bestuur en de commissies (CUUC en BAC) zien toe op de beheersing van risico's ten aanzien van incidenten in de dagelijkse uitvoering van de processen ('businesslijn'). Hierbij zijn het dagelijks bestuur en de commissies eerstverantwoordelijk voor het onderhoud van het Incidentenregeling en de implementatie en uitvoering van dit beleid. Hierbij wordt zij ondersteund door bestuursondersteuning en de IT-Officer van het fonds.                                                                                              |
| IT-officer               | De functionaris die als IT-Officer, door het bestuur van het Fonds is benoemd.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Incidenten               | Een gedraging of gebeurtenis die een ernstig (mogelijk) gevaar vormt voor de integere bedrijfsuitoefening van het fonds. Incidenten die optreden bij de uitvoeringsorganisatie, waaraan het Fonds werkzaamheden heeft uitbesteed, worden gemeld aan het Fonds, indien deze incidenten een ernstig gevaar vormen voor de integere bedrijfsvoering van het fonds, dan worden incidenten bij de uitvoeringsorganisatie aangemerkt als een Incident van het Fonds. Er wordt een onderscheid gemaakt tussen Operationele Incidenten en Overige Incidenten. |
| Melder                   | En verbonden persoon die melding doet van een Incident binnen het Fonds of een persoon die anderszins betrokken is bij het Fonds, maar niet als verbonden persoon is aan te merken en die melding doet van een Incident binnen het Fonds.                                                                                                                                                                                                                                                                                                             |
| Operationele Incidenten  | Een Incident dat plaats heeft gevonden in de dagelijkse uitvoering van de werkzaamheden door het Fonds en waarbij er een inbreuk is geweest op de integere bedrijfsvoering. Onder Operationele Incidenten vallen ICT- en cyberincidenten.                                                                                                                                                                                                                                                                                                             |
| Operationele gebeurtenis | Een gebeurtenis die heeft plaatsgevonden in de dagelijkse uitvoering van de werkzaamheden van het Fonds en waarbij er geen inbreuk is gemaakt op de integere en/of beheerste bedrijfsvoering                                                                                                                                                                                                                                                                                                                                                          |
| DORA                     | Digital Operational Resilience Act                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Ernstige ICT-Incidenten  | Een ICT-gerelateerd incident met grote nadelige gevolgen voor de netwerk- en informatiesystemen die kritieke of belangrijke functies van het Fonds ondersteunen, als bedoeld in de DORA. Dit is verder uitgewerkt in de Procedure Ernstige ICT-Incidenten.                                                                                                                                                                                                                                                                                            |
| Overige Incidenten       | Alle Incidenten, die niet beschouwd kunnen worden als Operationele Incidenten. Onder overige Incidenten worden in ieder geval verstaan: <ul style="list-style-type: none"><li>• een schending van wet- en regelgeving;</li><li>• een bewust onjuist informeren van publieke organen;</li><li>• een schending van binnen het Fonds geldende gedragsregels;</li><li>• het achterhouden, vernietigen of manipuleren van informatie</li></ul>                                                                                                             |

over deze feiten.

- een ernstig gevaar voor de integere bedrijfsuitoefening van het fonds;
- gebeurtenissen die kunnen leiden tot een groot afbreukrisico in de media;
- fraude, misleiding, bedrog, verduistering of diefstal door een of meer personen in zijn/hun hoedanigheid van Verbonden Persoon;
- een aanwijzing van een Toezichthouder, een last onder dwangsom of het voornemen om een bestuurlijke boete op te leggen;
- overige strafbare feiten.

Compliance Officer  
Fonds is benoemd.

De functionaris die als Compliance Officer door het bestuur van het

CUUC

Commissie Uitbesteding, Uitvoering en Communicatie.

Verbonden Personen

Degenen die conform de gedragscode van het pensioenfonds als verbonden persoon zijn aangemerkt.

## Melden incidenten

- Een Operationele gebeurtenis is geen Incident als bedoeld in deze regeling en wordt niet volgens deze regeling afgehandeld.
- Meldingen van Incidenten worden vertrouwelijk behandeld. De identificatiegegevens van de Melder worden niet opgenomen in de communicatie naar derden. Hiertoe wordt gewerkt met een geanonimiseerd 'zaaknummer'. Ook indien de Melder geen belang hecht aan anonimiteit zal zijn identiteit alleen dan worden vrijgegeven in communicatie, wanneer daartoe een wettelijke verplichting bestaat.

## Melding en registratie van de melding

- Iedere Verbonden Persoon en sleutelfunctiehouder die een (dreigend) Incident constateert is gehouden dit onverwijld te melden aan het Dagelijks bestuur en Bestuursondersteuning conform dit artikel. Ook andere personen betrokken bij het Fonds kunnen een melding doen van een (dreigend) Incident conform deze Incidentenregeling.
- Eenieder die een (dreigend) Incident constateert en zich niet vrij voelt dit te melden op grond van de Incidentenregeling, kan dit melden aan de Compliance Officer op grond van de Klokkenluidersregeling. De Incidentenregeling is van toepassing tenzij anders bepaald in de Klokkenluidersregeling.
- Voor sleutelfunctiehouders geldt deze meldingsplicht niet wanneer het Incident kwalificeert als een substantieel risico of significante inbreuk als bedoeld in artikel 143a, lid 3 van de Pensioenwet en de sleutelhouders op grond van dit artikel is gehouden tot melding aan DNB. De sleutelfunctiehouder informeert de Compliance Officer voorafgaand over de melding aan DNB. Een dergelijke melding wordt niet volgens deze regeling afgehandeld. In geval van

een wettelijke verplichte melding door een sleutelfunctiehouder aan DNB is artikel 6 van deze regeling van overeenkomstige toepassing.

- Iedere Verbonden Persoon die een (mogelijk) Datalek constateert is gehouden dit onverwijld te melden aan het Dagelijks bestuur en Privacy Officer. Een Datalek wordt beschouwd als Incident en wordt als zodanig geregistreerd. Een (mogelijk) Datalek wordt volgens de geldende Procedure Datalekken van het Fonds afgehandeld.
- Iedere Verbonden Persoon die een (mogelijk) Ernstig ICT-Incident constateert is gehouden dit onverwijld te melden aan het Dagelijks en bestuursondersteuning, die vervolgens desgewenst de IT-officer erbij betreft. Of sprake is van een Ernstig ICT-Incident wordt beoordeeld aan de hand van de criteria opgenomen in de geldende procedure Ernstige ICT-Incidenten van het Fonds. Een Ernstig ICT-Incident wordt beschouwd als Incident en wordt afgehandeld als zodanig geregistreerd.
- De bestuursondersteuning registreert meldingen van Incidenten op datum van ontvangst. Per melding wordt een dossier bijgehouden. Gedurende het verdere proces worden in het dossier relevante documenten opgenomen, zoals de communicatie tussen de verschillende partijen, de rapportages en de resultaten van eventueel onderzoek. Bestuursondersteuning bewaakt de voortgang van het meldproces en de opvolging van acties en rapporteert hierover aan het dagelijks bestuur.
- Alle identificatiegegevens van de Melder worden volgens de eisen en richtlijnen van de Algemene Verordening Gegevensbescherming en de Autoriteit Persoonsgegevens en in lijn met het Privacyreglement van het Fonds verwerkt.
- De melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan. Een mondelinge melding wordt schriftelijk vastgelegd door bestuursondersteuning indien aanvullende informatie benodigd is in het belang van het onderzoek, kan de Melder worden verzocht zijn medewerking hieraan te verlenen. De Melder is hiertoe niet verplicht.

## **Behandeling van de melding**

- De bestuursondersteuning stuurt binnen vijf werkdagen een ontvangstbevestiging aan de Melder en stelt tevens het Dagelijks bestuur van het Fonds door middel van een afschrift van de vastlegging van de melding op de hoogte van (de melding van) het Incident en de datum waarop deze is gemeld.
- Als de Melder vreest voor tegenmaatregelen of als een eerdere melding van hetzelfde Incident deze niet heeft weggenomen, bestaat de mogelijkheid om direct melding te doen aan de voorzitter van het Dagelijks bestuur. De voorzitter van het Dagelijks bestuur stuurt deze melding onverwijld door naar de Compliance Officer. Als het de voorzitter zelf betreft dan dient de Melder in een soortgelijk geval onverwijld melding te doen aan de Compliance Officer.
- Als de voorzitter van het bestuur en het Dagelijks bestuur binnen 5 werkdagen na de melding geen actie onderneemt, kan een melding worden gedaan bij de Compliance Officer.

## **Afhandelen incidenten**

- Voor de afhandeling van het Incident worden door het Dagelijks bestuur maatregelen genomen die zijn gericht op het beheersen van het optredende risico, het bevestigen van

geldende normen en het voorkomen van negatieve effecten – zowel intern als extern – om herhaling in de toekomst te voorkomen, waaronder melding aan DNB indien en voor zover dit nodig is op grond van de Pensioenwet of de DORA. Om de negatieve gevolgen van het Incident zo spoedig mogelijk te beperken, kunnen door het Dagelijks bestuur, separaat aan de afhandeling van het Incident, tussentijdse maatregelen getroffen worden.

- Het Dagelijks bestuur, ondersteund door de bestuursondersteuning, beoordeelt de melding en stelt uiterlijk binnen de wettelijke termijnen en wanneer deze er niet zijn uiterlijk binnen acht werkdagen na de ontvangen melding vast:
  - Of het een Integriteitsincident dan wel een Operationeel incident betreft;
  - Of het Incident wel of niet tevens een Datalek betreft. Indien het tevens een Datalek betreft het Procedure Datalekken van toepassing;
  - Of het Incident wel of niet tevens een Ernstig ICT-Incident betreft. Indien het mogelijk een Ernstig ICT- Incident betreft is het Procedure Ernstige ICT-Incidenten van toepassing;
  - De (mogelijke) risico-impact van het Incident. De risico-impact wordt op basis van een vaste procedure in het Risicomanagement beleid beoordeeld ingedeeld naar laag, medium en hoog. Is de risico-impact hoog, dan wordt hier melding van gedaan aan de Compliance Officer.
- De beoordeling hierboven wordt ter oordeelsvorming aan de sleutelfunctiehouder risicobeheer voorgelegd. Indien de sleutelfunctiehouder risicobeheer tot een ander oordeel komt, wordt zijn oordeel gevolgd. Van zijn oordeel kan alleen bij een gemotiveerd bestuursbesluit worden afgeweken.
- Operationele incidenten met een risicoclassificatie 'laag' of 'medium' worden door het Dagelijks bestuur en bestuursondersteuning afgehandeld. Integriteitsincidenten en operationele incidenten met een risicoclassificatie 'hoog' worden onverwijld na de beoordeling en oordeelsvorming ter afhandeling aan de voorzitter van het Dagelijks bestuur en bestuursondersteuning voorgelegd. Indien in dit geval de incidentmelding betrekking heeft op de voorzitter, treedt de vervangend voorzitter in diens plaats op.
- Indien de melding van een Operationeel Incident met risicoclassificatie 'laag' of 'medium' een van de leden van het Dagelijks bestuur betreft, wordt het Incident afgehandeld door het andere lid van het Dagelijks bestuur. Wanneer deze melding het volledige Dagelijks bestuur betreft, wordt het Incident afgehandeld door de Compliance Officer.
- De wijze waarop het Incident is afgehandeld en de gronden waarop dit is gebaseerd, worden uiterlijk binnen twee weken na de afhandeling schriftelijk aan de Melder meegedeeld. Indien het Dagelijks bestuur de melding heeft afgehandeld, ontvangt de Compliance Officer een afschrift ter informatie. Ook degene op wie de melding betrekking had wordt geïnformeerd.
- De Compliance Officer kan, bij Incidenten die ter afhandeling aan de Compliance Officer zijn voorgelegd, op basis van een zelfstandige oordeelsvorming de voorzitter adviseren een Onderzoekscommissie in te stellen. Van zijn advies kan alleen bij een gemotiveerd bestuursbesluit worden afgeweken. De Onderzoekcommissie wordt door het Dagelijks bestuur ingesteld en bestaat uit drie personen. De Onderzoekscommissie brengt en houdt de Compliance Officer en het Dagelijks bestuur op de hoogte van alle ontwikkelingen in het

onderzoek.

- Het Dagelijks bestuur dient het Incident na afgerond onderzoek, bij DNB te melden evenals de maatregelen die het Fonds heeft genomen.

## **Persoonsgericht onderzoek**

- Als er een redelijk vermoeden bestaat dat een Verbonden Persoon verantwoordelijk is voor of zich schuldig heeft gemaakt aan een Integriteitsincident, of als daar naar het oordeel van het Dagelijks bestuur aanleiding toe bestaat, kan het Dagelijks bestuur een persoonsgericht onderzoek instellen. De Verbonden Persoon op wie het persoonsgericht onderzoek zich richt wordt onverwijld op de hoogte gebracht van het persoonsgericht onderzoek.
- Een persoonsgericht onderzoek wordt ingesteld binnen een redelijke termijn, nadat er voldoende aanwijzingen bekend zijn geworden dat de betreffende verbonden persoon zich schuldig heeft gemaakt aan het Integriteitsincident.
- De Verbonden Persoon naar wie het persoonsgericht onderzoek wordt verricht, wordt in de gelegenheid gesteld zijn zienswijze kenbaar te maken. Zijn zienswijze wordt schriftelijk vastgelegd.
- Door of namens het Dagelijks bestuur worden een of meerdere personen of organisaties aangewezen die het persoonsgericht onderzoek verrichten.
- Indien het onderzoek en/of het belang van het Fonds dit vereist, kan, in overleg met het Dagelijks bestuur, door de onderzoeker(s) opdracht worden gegeven om bepaalde gegevens of zaken veilig te stellen. Daartoe wordt een belangenafweging gemaakt. Voor het inzien van persoonlijke informatie is toestemming van het Dagelijks bestuur c.q. de overige bestuursleden vereist.
- Een persoonsgericht onderzoek vindt op een integere en zorgvuldige wijze plaats. Toegezien wordt op de in acht te nemen zorgvuldigheid, waarbij de belangen van het Fonds, het belang van de Verbonden Persoon (dan wel de Verbonden Personen) naar wie het onderzoek zich richt en de belangen van overige betrokkenen redelijkerwijs in acht worden genomen. Het persoonsgericht onderzoek wordt binnen een redelijke termijn uitgevoerd.
- Na de uitvoering van een persoonsgericht onderzoek, wordt een schriftelijk advies uitgebracht aan het Dagelijks bestuur. Het op schrift gestelde advies wordt door de bestuursondersteuning en Compliance Officer bewaard.
- Alle relevante documenten, daaronder begrepen de zienswijze van de verschillende betrokkenen, rapportages en het op schrift gestelde advies worden opgenomen in een dossier dat door de bestuursondersteuning wordt bewaard.

## **Informatieverschaffing aan de toezichthouder(s) en overige communicatie**

- DNB wordt, door of namens het Dagelijks bestuur, bij een te melden Incident in ieder geval geïnformeerd binnen een termijn van vijf werkdagen nadat:
  - aangifte is of wordt gedaan bij justitiële autoriteiten;

- het voortbestaan van het Fonds wordt bedreigd of zou kunnen worden bedreigd;
  - er sprake is van een ernstige tekortkoming in de opzet en werking van de maatregelen ter bevordering of handhaving van een integere bedrijfsvoering door het Fonds;
  - mede gelet op verwachte publiciteit, rekening behoort te worden gehouden met (een ernstige mate van) reputatieschade voor het Fonds; of
  - de ernst, de omvang of de overige omstandigheden van het incident in aanmerking genomen, de toezichthouder in verband met haar toezichtstaak redelijkerwijs, of op basis van een wettelijke verplichting, behoort te worden geïnformeerd.
- De informatieverschaffing van Ernstige ICT-Incidenten aan DNB verloopt volgens de Procedure Ernstige ICT-Incidenten.
  - Van een aan DNB te melden Incident wordt tevens gelijktijdig melding gedaan aan de AFM en/of de AP indien het Incident betrekking heeft op onderdelen van de bedrijfsvoering van het Fonds waarop zij toezicht houden.
  - Het Dagelijks bestuur beslist over de communicatie, zowel intern als extern, met betrekking tot Incidenten. Door het bestuur wordt, na advies van de betrokken adviseur of Compliance Officer, besloten of en wanneer andere organen van het Fonds, stakeholders en overige belanghebbenden op de hoogte worden gebracht van een Incident.

## Rechtsbescherming

- Eenieder die uit hoofde van deze regeling informatie verkrijgt over (de melding van) een Incident, betracht daarover uiterste geheimhouding tegenover derden, tenzij op basis van deze regeling of bij of krachtens de wet de bevoegdheid of de verplichting bestaat om die informatie aan een derde te verschaffen.
- Het Fonds draagt er zorg voor dat de Melder en eventueel door de Melder betrokken perso(o)n(en) op geen enkele wijze in zijn positie bij het Fonds benadeeld wordt, voor zover te goeder trouw gehandeld is.
- Het Fonds draagt er zorg voor dat de Compliance Officer, bestuursondersteuning, en de onderzoekscommissie op geen enkele wijze in hun positie bij het Fonds benadeeld worden vanwege het uitoefenen van hun taken op grond van deze regeling.
- De Melder die willens en wetens heeft deelgenomen aan of veroorzaker is van een Incident zal bij melding hiervan geen recht kunnen ontlenen aan de beschermingsregel zoals die geldt voor een te goeder trouw handelende Melder.

## Rapportage

- De bestuursondersteuning rapporteert periodiek aan het dagelijks bestuur over de voortgang en afhandeling van Incidenten. De voortgang van de afhandeling van Incidenten met een risicoclassificatie 'hoog' wordt in de vergadering van het Dagelijks Bestuur geagendeerd. Het dagelijks bestuur is eindverantwoordelijk voor het toezien op de opvolging van de genomen acties. Namens het dagelijks bestuur kan

bestuursondersteuning toezien op de daadwerkelijke opvolging.

- In de rapportage(s), zoals die jaarlijks door de bestuursondersteuning aan het Dagelijks bestuur worden aangeboden, wordt inzicht gegeven in het aantal Incidenten dat zich in de betreffende periode heeft voorgedaan en de aard daarvan. Tevens bevat de rapportage informatie over de voortgang van de afhandeling van Incidenten ter behandeling zijn voorgelegd, en de naar aanleiding van deze Incidenten genomen maatregelen.
- De voorzitter van het Dagelijks bestuur is bij Incidenten met een risicoclassificatie 'hoog' verantwoordelijk voor het toezien op de opvolging van de genomen acties door agendering van de voortgang van de afhandeling van het Incident in de vergadering van het Dagelijks bestuur. Bij Incidenten met een risicoclassificatie 'laag' of 'medium' is de bestuursondersteuning verantwoordelijk voor het toezien op de opvolging van de genomen acties.

### **Onvoorziene omstandigheden**

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

### **Wijzigingen in deze regeling**

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