PENSIOENFONDS
NOTARIAAT

Incidentenregeling

Pensioenfonds Notariaat

25 mei 2023

PENSIOENFONDS
NOTARIAAT

Inhoudsopgave

PENSIOENFONDS
NOTARIAAT

Artikel 1 Definities

a.	bestuur:	het bestuur van het fonds;
b.	compliance officer:	de functionaris die door het bestuur van het fonds als compliance officer is benoemd;
c.	cyberincident:	een informatiebeveiligingsincident waarbij kwaadwillenden misbruik maken van het feit dat SPN en haar uitbestedingspartijen (via internet) verbonden zijn met de buitenwereld . Voorbeelden zijn bijvoorbeeld een hack, malware, phishing, ddos-aanval. Zwakheden in de processen, systemen en gedrag van mensen, waardoor de kwetsbaarheid toeneemt en herstel na het incident moeilijker is, worden ook als incidenten beschouwd. Cyberincidenten zijn een aparte categorie doordat snelle herkenning de reactietijd verkort en toenemend inzicht (door meldingen ook bij toezichthouder) helpt om weerbaarder te worden;
d.	datalek:	een ongeoorloofde of onbedoelde toegang tot persoonsgegevens, alsmede het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens. Een datalek is altijd een integriteitsincident (inbreuk op privacywetgeving en fondsbeleid) en veelal ook een informatiebeveiligingsincident. Vanwege de mogelijke impact van een datalek voor betrokkenen en het vereiste om tijdige melding bij de Autoriteit Persoonsgegevens worden datalekken als een aparte categorie incidenten gedefinieerd;
e.	directeur:	de directeur van het fonds;
f.	fonds:	Stichting Pensioenfonds Notariaat (hierna ook te noemen ‘SPN’);
g.	incident:	een gebeurtenis of situatie die inbreuk maakt op de beheerste en integere bedrijfsvoering van het fonds. Een incident kan leiden tot financiële schade, reputatieschade van het fonds en/of de sector, of de realisatie van de doelstellingen van het fonds op andere wijze nadelig beïnvloeden. Een incident kan dus ook een situatie zijn die nog geen impact heeft gehad maar deze wel kan krijgen, bijvoorbeeld een kwetsbaarheid in een systeem waardoor de beveiliging van informatie onvoldoende is. Het fonds onderscheidt de volgende categorieën incidenten:

		(1) integriteitsincidenten (2) datalekken (3) informatiebeveiligingsincidenten (4) cyberincidenten (5) operationele incidenten (6) overige incidenten;
h.	incidentenregister:	in dit register worden alle incidenten vastgelegd. Voor integriteitsincidenten en misstanden is er wegens de behoefte aan geheimhouding een separaat register dat onderhouden wordt door de compliance officer;
i.	IB-incident	of voluit een informatiebeveiligingsincident: een situatie of gebeurtenis die een inbreuk is op de beschikbaarheid, integriteit of vertrouwelijkheid van informatie.
j.	integriteitsincident:	een gedraging of gebeurtenis die een inbreuk is op regelgeving en compliance, zoals een overtreding van wet- en regelgeving (waarbij inbegrepen het niet voldoen aan de vereisten van toezichthouders) of een schending van intern beleid, regels en procedures.
k.	operationeel incident:	een incident dat plaats heeft gevonden in de dagelijkse uitvoering van de werkzaamheden door het fonds en waarbij er een inbreuk is gemaakt op de beheerste bedrijfsvoering;
l.	overig incident:	een incident, dat niet is onder te brengen bij een van de onder artikel 1 lid g genoemde andere incidentcategorieën.
m.	verbonden personen:	(1) leden van het bestuur; (2) leden van de raad van toezicht en het verantwoordingsorgaan; (3) externe leden van commissie; (4) medewerkers van het fonds, waaronder personen die tijdelijk (op inhuurbasis werkzaamheden voor het fonds verrichten (5) personen die door het bestuur als verbonden personen zijn aangewezen. Medewerkers van uitbestedingspartijen zijn geen verbonden personen, tenzij deze op basis van onderdeel (5)van dit lid wel als zodanig door het bestuur zijn aangewezen.
n.	toezichthouder:	De Nederlandsche Bank (DNB), de Autoriteit Financiële Markten (AFM), de Autoriteit Persoonsgegevens (AP), de Autoriteit Consument en Markt (ACM), de Belastingdienst en overige publieke toezichtorganen met jurisdictie ten aanzien van (de werkzaamheden van) het fonds.

Artikel 2 Reikwijdte incidentenregeling en samenhang met ander fondsbeleid

1. Een incident is niet altijd eenduidig toe te wijzen aan een categorie. Een inbreuk op het fondsbeleid is een integriteitsincident maar kan bijvoorbeeld tegelijkertijd een cyberincident en datalek zijn. Bij de kwalificatie van het incident wordt een keuze gemaakt op basis van waar het zwaartepunt van het incident ligt.
2. In het Privacybeleid van het fonds is de procedure opgenomen voor de melding van datalekken die naast deze incidentenregeling van toepassing is indien een incident als datalek wordt gekwalificeerd.
3. In de Klokkenluidersregeling van het fonds staan misstanden centraal. Misstanden zijn in de regel integriteitsincidenten. De focus in de klokkenluidersregeling ligt op de bescherming van de melder tegen benadeling. De klokkenluidersregeling staat naast de incidentenregeling. Het is aan de melder om te bepalen of de gebeurtenis als incident conform deze regeling of als vermoede misstand conform de klokkenluidersregeling wordt gemeld.
4. Een calamiteit wordt beschouwd als een incident en wordt als zodanig ook opgenomen in het incidentenregister. Voor informatie over hoe te handelen bij een calamiteit (de zogenaamde noodprocedure) wordt verwezen naar het calamiteitenplan (bijlage bij ABTN van het fonds) en het Beleid Business Continuity Management.
5. Een financiële crisissituatie zoals beschreven in het financieel crisisplan (bijlage bij ABTN van het fonds) valt buiten de reikwijdte van deze incidentenregeling.

Artikel 3 Melden van incidenten

1. Iedere verbonden persoon die een mogelijk incident constateert is gehouden dit te melden aan de directeur. Een melding kan zowel schriftelijk, elektronisch als mondeling worden gedaan. Meldingen kunnen ook anoniem worden gedaan.
2. Ook uitbestedingspartijen zijn gehouden incidenten te melden aan het fonds. In artikel 8 wordt ingegaan op de wijze waarop dit moet plaatsvinden.

Artikel 4 Initiële beoordeling en classificatie van incidenten

1. De directeur beoordeelt de melding en bepaalt of er sprake is van een incident, tot welke categorie het incident behoort en of er sprake is van een ernstig incident. Indien benodigd doet de directeur een beroep op externe expertise (bijvoorbeeld op gebied van IT of privacy).
2. Indien een melding geclassificeerd wordt als een integriteitsincident wordt de melding onverwijld doorgestuurd naar de compliance officer.
3. Een incident is in ieder geval een ernstig incident als minimaal een van de volgende situaties zich voordoet:
   a. Er is aangifte gedaan bij justitiële autoriteiten of er zal waarschijnlijk aangifte gedaan worden.
   b. De continuïteit van essentiële bedrijfsactiviteiten kan na het zich voordoen van het incident niet direct hersteld worden.
   c. De negatieve financiële impact van het incident is groter dan € 50.000.

d. Er is kans op ernstige reputatieschade of op een groot verlies van vertrouwen in het fonds.
e. Er is sprake van een ernstige tekortkoming in de opzet en/of werking van de maatregelen om een beheerste en integere bedrijfsvoering te borgen.
f. De Toezichthouder behoort redelijkerwijs in verband met haar toezichtstaak of op basis van een wettelijke verplichting te worden geïnformeerd over het incident.
g. Er is sprake van een datalek welke conform de wet en/of het Privacybeleid van het fonds gemeld dient te worden aan de Autoriteit Persoonsgegevens (AP).

Dit is geen limitatieve opsomming. Per voorgedane situatie en afhankelijk van de omstandigheden van het geval zal worden beoordeeld of er sprake is van de kwalificatie ernstig incident.

4. De directeur brengt de melder als bedoeld in artikel 3 lid 1 van zijn beoordeling op de hoogte. Dit kan zowel schriftelijk als elektronisch worden gedaan.

Artikel 5 Vastleggen van incidenten

1. De incidenten worden vastgelegd in het incidentenregister.
2. Van elk incident wordt ten minste de volgende informatie vastgelegd in de incidentenregisters: (a) wie de melder is (b) de datum van de melding van het incident (c) de kwalificatie van het incident en tot welke categorie het incident behoort (d) of er sprake is van een ernstig incident en zo ja, de onderbouwing waarom tot de kwalificatie ernstig incident is gekomen € een korte omschrijving van het incident (f) of een melding aan de Toezichthouder aan de orde is en zo ja, welke Toezichthouder een melding ontvangt (g) de eigenaar bij SPN voor de afhandeling/monitoring van het incident (h) de status in de afhandeling van het incident.
3. Integriteitsincidenten worden wegens de behoefte aan geheimhouding, samen met gemelde misstanden op basis van de Klokkenluidersregeling van het fonds, vastgelegd in een separaat register voor integriteitsincidenten, dat wordt onderhouden door de compliance officer.

Artikel 6 Behandeling van incidenten

1. De directeur wijst een niet-ernstig incident toe aan een eigenaar die het incident gaat behandelen.
2. Het behandelen van een incident omvat in ieder geval (a) actie ondernemen om te voorkomen dat de impact van het incident groter wordt (2) onderzoeken wat de oorzaak is van het incident en het doen van voorstellen om herhaling van het incident te voorkomen (3) het aanleggen van een dossier over het incident (4) bijwerken van de status in het incidentenregister (5) interne communicatie ter vergroting van de awareness.
3. Indien de directeur de melding als een ernstig incident heeft beoordeeld, treedt de directeur in overleg met de sleutelfunctiehouder risicobeheer om de aanpak af te stemmen. Indien de sleutelfunctiehouder geen bestuurslid is, richt de directeur zich tot het dagelijks bestuur van het fonds voor overleg over de aanpak.
4. Bij ernstige incidenten is de directeur de eigenaar van het incident tenzij de sleutelfunctiehouder risicobeheer of het bestuur deze rol aan een ander toewijzen. De directeur houdt de

sleutelfunctiehouder risicobeheer en het bestuur steeds op de hoogte van de voortgang en de belangrijke ontwikkelingen tijdens de behandeling van het incident.

5. Bij ernstige incidenten kunnen externe specialisten worden betrokken en/of een onderzoekscommissie worden ingesteld. De sleutelfunctiehouder risicobeheer en/of het bestuur besluit hiertoe. Als een onderzoek wordt verricht door een andere persoon dan de directeur of wordt verricht door een onderzoekscommissie is/zijn de onderzoeker(s) gehouden de directeur op de hoogte te brengen en te houden van alle ontwikkelingen in het onderzoek.
6. Ofschoon de eigenaar een belangrijke rol in de behandeling van incidenten inneemt, is het bestuur eindverantwoordelijk voor de afronding van het incident en de eventueel getroffen maatregelen.

Artikel 7 Integriteitsincidenten

1. Indien een melding beoordeeld wordt door de directeur als een integriteitsincident wordt de melding onverwijld doorgestuurd naar de compliance officer.
2. Indien het integriteitsincident betrekking heeft op de directeur wordt de melding rechtstreeks aan de compliance officer gedaan.
3. De compliance officer legt het incident vast in het register met integriteitsincidenten/ misstanden en onderhoudt dit register.
4. De compliance officer beoordeelt het incident en indien vervolgacties noodzakelijk zijn, worden deze in overleg met de directeur bepaald en toegewezen aan een eigenaar, tenzij er sprake is van een integriteitsincident als bedoeld in lid 2 van dit artikel. De compliance officer monitort de behandeling van het incident totdat het incident is afgehandeld.
5. Het bestuur kan de compliance officer om advies vragen en de compliance officer kan het bestuur ook ongevraagd adviseren.
6. Indien het een ernstig integriteitsincident betreft (conform de criteria genoemd in artikel 4 lid 3) treedt de compliance officer in overleg met de directeur en de sleutelfunctiehouder risicobeheer (of het dagelijks bestuur van het fonds indien de sleutelfunctiehouder geen bestuurder is) om eventuele vervolgacties af te stemmen.
7. De compliance office rapporteert elk kwartaal aan het bestuur de nog openstaande integriteitsincidenten en misstanden, en de in het desbetreffende kwartaal gemelde en reeds afgehandelde incidenten.

Artikel 8 Incidenten bij uitbestedingspartijen

1. Als zich bij een partij waaraan het fonds werkzaamheden heeft uitbesteed een incident voordoet dat zich op basis van artikel 4 lid 3 kwalificeert als ernstig, dan meldt deze uitbestedingspartij dit onverwijld aan de directeur.
2. De directeur betrekt de sleutelfunctiehouder risicobeheer (of het dagelijks bestuur van het fonds indien de sleutelfunctiehouder geen bestuurder is) bij het overleg met de uitbestedingspartij over de vervolgstappen.

3. Een ernstig incident bij een uitbestedingspartij wordt opgenomen in het incidentenregister van het fonds. De niet-ernstige incidenten worden alleen opgenomen in het incidentenregister van de uitbestedingspartij en periodiek gerapporteerd aan het fonds. De rapportage wordt behandeld door de eerstelijns bestuurscommissie die toeziet op de uitbestedingspartij.
4. De directeur monitort als eigenaar de behandeling van het ernstige-incident totdat het incident is afgehandeld.
5. De uitbestedingspartij rapporteert periodiek conform de contractuele afspraken aan het fonds de nog openstaande incidenten, en de in de desbetreffende periode gemelde en reeds afgehandelde incidenten.
6. Het fonds draagt er zorg voor dat de uitbestedingspartij bekend is met deze incidentenregeling en zich er contractueel aan committeert, of dat er andere contractuele afspraken worden gemaakt die leiden tot minimaal hetzelfde niveau van risicobeheersing als met deze incidentenregeling wordt geborgd.

Artikel 9 Melden toezichthouder en overige communicatie

1. Door of namens het bestuur wordt onverwijld de relevante toezichthouder geïnformeerd indien sprake is van een incident waarbij sprake is van een ernstig gevaar voor de beheerste en integere bedrijfsvoering
2. De Toezichthouder wordt op de hoogte gebracht van alle feiten, omstandigheden en achtergronden van het incident, alsmede de maatregelen die naar aanleiding van het incident zijn genomen.
3. Het bestuur beslist over de communicatie, zowel intern als extern, met betrekking tot incidenten. Het bestuur besluit tevens of en wanneer andere organen van het fonds, stakeholders en overige belanghebbenden op de hoogte worden gebracht van een incident.
4. Het bestuur kan de compliance officer om advies vragen inzake het melden van een incident aan de Toezichthouder en/of over de communicatie inzake het incident.

Artikel 10 Persoonsgericht onderzoek

1. Als er een redelijk vermoeden bestaat dat een verbonden persoon verantwoordelijk is voor of zich schuldig heeft gemaakt aan een incident, kan op verzoek van het bestuur een persoonsgericht onderzoek worden ingesteld. De persoon naar wie het persoonsgericht onderzoek zich richt, wordt onmiddellijk op de hoogte gebracht van het persoonsgericht onderzoek.
2. Een persoonsgericht onderzoek wordt ingesteld binnen een redelijke termijn, nadat vast is komen te staan dat sprake is van een redelijk vermoeden dat de verbonden persoon verantwoordelijk is voor of zich schuldig heeft gemaakt aan een incident.
3. De verbonden persoon naar wie het persoonsgericht onderzoek wordt verricht, wordt in de gelegenheid gesteld zijn/haar zienswijze kenbaar te maken. Zijn/haar zienswijze wordt schriftelijk vastgelegd.
4. Door het bestuur worden een of meerdere personen of organisaties aangewezen die het

persoonsgericht onderzoek verrichten.

5. Indien het onderzoek en/of het belang van het fonds dit vereist, kan in overleg met het 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 bestuur vereist.
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. Na de uitvoering van een persoonsgericht onderzoek, worden de resultaten gerapporteerd aan het bestuur. Het bestuur kan de compliance officer vragen om advies over de wijze waarop opvolging kan worden gegeven aan de resultaten van het onderzoek. Het bestuur besluit vervolgens op welke wijze opvolging wordt gegeven aan het incident.
8. Alle relevante documenten, daaronder begrepen de zienswijze van de verschillende betrokkenen, rapportages en het op schrift gestelde advies worden opgenomen in een dossier.

Artikel 11 Meldingen en geheimhouding

1. Melding van een incident kan anoniem gedaan worden. Indien aanvullende informatie benodigd is in het belang van het onderzoek, kan de verbonden persoon worden verzocht zijn medewerking hieraan te verlenen. De verbonden persoon is hiertoe niet verplicht.
2. De melding en de daarbij beschikbaar gestelde gegevens worden door alle betrokken partijen strikt vertrouwelijk behandeld. De identiteit van de melder wordt niet opgenomen in de communicatie naar derden tenzij daar een wettelijke verplichting toe bestaat of dit noodzakelijk is voor het uitvoeren van deze regeling, in het bijzonder voor het onderzoek als bedoeld in artikel 6 en artikel 10.
3. 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. 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.
4. Incidentendossiers worden in een passende beveiligde omgeving bewaard.

Artikel 12 Omgang met meldingen

1. Het fonds gaat er altijd van uit dat een melding van een incident te goeder trouw is gedaan, tot het moment dat zij overtuigd is geraakt van het tegendeel.
2. Het fonds draagt zorg dat een melder die te goeder trouw heeft gehandeld, op geen enkele wijze in zijn of haar positie wordt benadeeld. Ongeacht de wijze waarop de melder melding heeft gemaakt van het incident.
3. Het fonds 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.

4. In geval van intrekking van een melding zal het fonds, 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.
5. Een verbonden persoon die willens en wetens heeft deelgenomen aan of veroorzaker is van een incident, kan bij melding van dit incident geen recht ontlenen aan de beschermingsmaatregelen zoals die gelden voor een te goeder trouw handelende verbonden persoon.

Artikel 13 Inwerkingtreding

Deze incidentenregeling is vastgesteld op 25 mei 2023 door het bestuur van het fonds. De incidentenregeling vervangt alle voorgaande incidentenregelingen en treedt per deze datum in werking.