Procedure klokkenluidersregeling

Datum van uitwerking: februari 2023

De nieuwe wetgeving van 8 december 2022 voert de verplichting tot het opzetten van meldingskanalen in zodat inbreuken op bepaalde wetgeving binnen private organisaties in een vroeg stadium kunnen worden opgespoord en behandeld, en dat tegelijkertijd een doeltreffende bescherming biedt aan de klokkenluiders.

Inbreuken in welke beleidsterreinen?

- *Financiële diensten, producten en markten, voorkomen van witwassen van geld en financiering van terrorisme*
- *Productveiligheid en productconformiteit*
- *Veiligheid van het vervoer*
- *Milieubescherming*
- *Overheidsopdrachten*
- *Stralingsbescherming en nucleaire veiligheid*
- *Veiligheid van levensmiddelen, dierenvoeding, dierengezondheid en dierenwelzijn*
- *Volksgezondheid*
- *Consumentenbescherming*
- *Bescherming van persoonlijke levenssfeer en persoonsgegevens, beveiliging van netwerk en informatiesystemen*
- *Bestrijding van belastingfraude*
- *Sociale fraudebestrijding*
- *Financiële belangen EU of verstoring interne markt*

1. Klokkenluider

Wanneer iemand mistoestanden in zijn (voormalige) organisatie aan het licht brengt, dan spreken we van een klokkenluider.

De klokkenluider kan een (ex-)werknemer, sollicitant, vrijwilliger, stagiair of zelfstandige werkzaam in de onderneming, aandeelhouders, bestuurder zijn, maar ook iemand die werkt onder toezicht en leiding van (onder-)aannemers en leveranciers, enz. Kortom, eenieder in een werkgerelateerde context.

ZORGGROEP arum

Als klokkenluider moet je redelijke gronden hebben om aan te nemen dat wat je meldt juist is, gezien de omstandigheden en de informatie waarover je op het moment van de melding beschikt. Wie opzettelijk of bewust onjuiste of misleidende informatie meldt, geniet geen bescherming tegen represailles.

Inbreuk

Het begrip 'inbreuk' wordt heel ruim bekeken:

- Handelingen of nalatigheden:
  - In overtreding van de geldende regels in de opgesomde beleidsterreinen;
  - Die ingaan tegen het doel of de toepassing van deze regels
- Poging tot inbreuk, voltooide inbreuk, lopende inbreuk, poging tot verberging inbreuk
- Bewezen inbreuk OF inbreuk waarvan klokkenluider op het moment van de melding gegronde reden had om aan te nemen dat de info over de inbreuk juist was.

Garanties en bescherming

De procedures en systemen die gebruikt worden om meldingen te ontvangen en op te volgen, moeten de nodige garanties bieden inzake de vertrouwelijkheid, anonimiteit en kwaliteit van de behandeling. De nieuwe regeling stelt een verbod op represailles vast ter vergelding voor een melding of openbaarmaking. De definitie van represailles is ruim omschreven. Denk bijvoorbeeld aan represailles in het kader van negatieve beoordelingen of ontslag, maar ook bij verandering van taken, financiële sancties of reputatieschade.

Bij een melding via de interne en externe meldkanalen, heb je de keuze om je naam bekend te maken als melder, of anoniem te blijven voor de meldingsbeheerder. Niet-anonieme meldingen hebben de voorkeur, om de verdere opvolging en behandeling van je klacht te vereenvoudigen. De meldingskanalen zorgen voor systemen die de vertrouwelijkheid beschermen van:

- jouw identiteit
- de identiteit van de anderen die in de melding genoemd zijn
- de informatie waaruit jouw identiteit of deze van de anderen kunnen blijken

Dit door andere de toegang tot deze informatie te beperken.

Meldkanalen

Er zijn drie mogelijke kanalen om een melding te doen. Er wordt niet gewerkt met een getrapt systeem, de melder kiest zelf een meldkanaal. Er wordt aangemoedigd om zoveel als mogelijk de interne kanalen voorrang te geven. We willen daarbij nog benadrukken dat we binnen onze organisatie werken met vertrouwenspersonen die een eerste aanspreekpunt zijn in functie van het welzijn voor al onze medewerkers. Indien dit niet voldoende veilig voelt, kan er geschakeld worden naar onderstaande meldkanalen.

i) Intern meldkanaal

Als melder meld je de informatie over een inbreuk bij voorkeur intern als de inbreuk op een doeltreffende manier intern kan behandeld worden en er geen risico op represailles bestaat. Aangezien Zorggroep Arum meer dan 250 medewerkers heeft, is het bij wet verplicht om anonimiteit bij de melding mogelijk te maken. Er kan dus anoniemen een melding gemaakt worden, we zijn hier echter geen voorstander van, omdat men dan moeilijk (of niet) kan communiceren over de opvolging.

Meldingsbeheerder

De meldingsbeheerder garandeert de vertrouwelijkheid van de melding en zal de meldingen op een objectieve en integere manier inschatten en opvolgen. Voor Zorggroep Arum is de interne preventieadviseur de meldingsbeheerder.

Hoe melden?

Iedere stakeholder (medewerker of externe) kan op verschillende manieren contact opnemen:

- (Anonieme) brief naar: vzw Zorggroep Arum - t.a.v. meldingsbeheerder, Stokkemerbaan 147, 3650 Dilsen-Stokkem
- (Anoniem) formulier: https://forms.office.com/e/MTM4QFMfk6
- E-mail naar: de meldingsbeheerder via ipa@arum.be
- Via telefoon naar Zorggroep Arum, men kan dan vragen naar de meldingsbeheerder: 089/79 84 20

Melders kunnen ook verzoeken om binnen een redelijke termijn een inbreuk te melden via een fysieke ontmoeting. Een dergelijke fysieke melding kan ook op afspraak bij de interne preventieadviseur.

Behandeling meldingen

- Alle meldingen komen aan bij de meldingsbeheerder (brief, mail, formulier, telefoon).
- De meldingsbeheerder filtert de meldingen, beoordeelt de waarachtigheid en zorgt voor een ontvangstmelding binnen de 7 dagen (dit kan niet bij een anonieme melding).
- De meldingsbeheerder geeft de informatie door aan de algemeen directeur zonder vermelding van de bron - zo wordt vermeden dat de melder negatieve gevolgen ondervindt. De algemeen directeur informeert op dezelfde wijze het bestuursorgaan. Ook indien de meldingsbeheerder de melding effectief filtert, en er dus geen verdere stappen dienen ondernomen te worden, informeert de meldingsbeheerder de algemeen directeur en de algemeen directeur het bestuursorgaan hierover. Zodoende wordt er steeds gewaakt over een vier-ogen principe tot op het niveau van het bestuursorgaan.
- De algemeen directeur beoordeelt de melding en kijkt of en welke actie er nodig is. De algemeen directeur brieft de meldingsbeheerder hierover.
- De meldingsbeheerder registreert welke actie werd ondernomen naar aanleiding van de melding en koppelt binnen de 3 maanden terug naar de melder (niet mogelijk bij anonieme melding).
- Jaarlijks wordt in een terugkoppeling voorzien van de ontvangen meldingen en behandeling ervan ten aanzien van de ondernemingsraad zonder vermelding van de bron - zo wordt vermeden dat de melder negatieve gevolgen ondervindt.

Registratie

De meldingsbeheerder verzamelt alle meldingen en houdt bij welke gevolgen hieraan werden gegeven.

Archivering

De gegevens worden enkel door de meldingsbeheerder gearchiveerd. Hierdoor is het niet mogelijk dat derden (intern of extern) toegang krijgen tot de meldingen en de melder hierdoor nadeel ondervindt.

ii) Extern meldkanaal

Daarnaast heeft de wetgever recent ook autoriteiten aangeduid die onafhankelijke en autonome externe meldingskanalen moeten opzetten voor het ontvangen en in behandeling nemen van informatie over inbreuken. De instanties die optreden als bevoegde autoriteit voor het ontvangen van externe meldingen over specifieke inbreuken in het kader van de 'Klokkenluiderswet' voor de private sector, zijn voornamelijk diverse federale overheidsdiensten en andere overheidsinstantie (zie bijlage 1 voor de verschillende contactgegevens). Ze zullen instaan voor het onderzoek en de controle van meldingen en kunnen eventuele sancties opleggen. De Federale Ombudsman zal belast zijn met de coördinatie van externe meldingen in de private sector en zal optreden als 'default' autoriteit.

iii) Openbaarmaking

In zeer uitzonderlijke omstandigheden kan er geschakeld worden naar een openbaarmaking van een melding van een inbreuk. In geval van openbaarmaking moet aan één van de volgende voorwaarden voldaan zijn opdat je als melder bescherming geniet:

- Je hebt eerst intern of extern gemeld, of hebt meteen extern gemeld omdat je meende dat de inbreuk niet doeltreffend behandeld kon worden of dat er een risico op represaille bestond. Vervolgens zijn er geen passende maatregelen genomen binnen de drie maanden nadat het betreffende meldingskanaal de melding heeft ontvangen. (= indirecte openbaarmaking)
- Je meent dat een van de volgende situaties zich voordoet (= directe openbaarmaking):
    - De inbreuk kan een dreigend of reëel gevaar vormen voor het algemeen belang.
    - Er bestaat naar aanleiding van een externe melding een risico op represailles of het is niet waarschijnlijk dat de inbreuk doeltreffend wordt behandeld door de bijzondere omstandigheden van de zaak.

Dit is niet van toepassing op gevallen waarin een persoon rechtstreeks informatie aan de pers verstrekt op grond van specifieke bepalingen die een stelsel voor de bescherming van de vrijheid van meningsuiting en informatie instellen.

Bijlage 1: lijst federale autoriteiten

1. **Financiële diensten, producten en markten, voorkomen van witwassen van geld en financiering van terrorisme**: FSMA voor de regels bedoeld in artikel 45 van de wet van 2 augustus 2002, NBB voor de regels bedoeld in de artikelen 12bis en 36/2 van de wet van 22 februari 1998, College van toezicht op de bedrijfsrevisoren voor de regels bedoeld in artikel 32 van de wet van 7 december 2016;
2. **Productveiligheid en productconformiteit**: FOD Economie, FOD Volksgezondheid, FAGG, BIPT, FOD Mobiliteit;
3. **Veiligheid van het vervoer**: FOD Mobiliteit, Nationale Autoriteit voor Maritieme Beveiliging;
4. **Milieubescherming**: FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu, Leefmilieu Brussel, CREG, Algemene Directie Energie, ACER;
5. **Overheidsopdrachten**: de dienst Overheidsopdrachten van de FOD Kanselarij van de Eerste minister;
6. **Stralingsbescherming en nucleaire veiligheid**: Federaal Agentschap voor Nucleaire Controle;
7. **Veiligheid van levensmiddelen, dierenvoeding, dierengezondheid en dierenwelzijn**: FAVV, FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu;
8. **Volksgezondheid**: Sciensano, FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu, FAGG, Federale commissie “Rechten van de patiënt”;
9. **Consumentenbescherming**: FOD Economie;
10. **Bescherming van persoonlijke levenssfeer en persoonsgegevens, beveiliging van netwerk en informatiesystemen**: Gegevensbeschermingsautoriteit, CCB, EDPS.