Policy klokkenluiders Moore

CONTENTS

<u>Belang van deze policy :</u>

Deze policy is de weergave van het beleid van Moore Belgium, ingeschreven in het KBO onder het nummer 0406.878.277, met haar maatschappelijke zetel te 1020 Brussel, Esplanade 1, bus 96, en de met haar verbonden vennootschappen. Naar Moore groep wordt verder in deze policy verwezen als "Moore". Deze policy kan op eenzijdig initiatief van Moore en zonder dat dit onrechtmatig kan geacht worden, aangepast worden in functie van wijzigende regelgeving of wijzigend beleid van Moore. De medewerkers zullen tijdig geïnformeerd worden over dergelijke aanpassingen.

1. Inleiding

a. Deze policy is opgesteld om te voldoen aan de toepasselijke wet- en regelgeving met betrekking tot de bescherming van klokkenluiders, nl.

- Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden;
- Wet van 28 november 2022 betreffende de bescherming van melders van inbreuken op het Unie- of nationale recht vastgesteld binnen een juridische entiteit in de private sector (hierna: Klokkenluiderswet).

b. Met deze policy wil Moore **transparantie** bieden aan haar medewerkers en derden over de bestaande kanalen om (vermeende) onregelmatigheden binnen Moore te melden. Op deze manier hoopt Moore de drempel om wanpraktijken te melden, te verlagen. Daarnaast biedt men aan de hand van deze policy **bescherming** voor de klokkenluider of melder. Moore garandeert haar medewerkers een onafhankelijk en een vertrouwelijk onderzoek ingevolge een eventuele melding.

c. Deze policy legt op zich **geen meldingsplicht** op aan haar medewerkers en/of derde partijen; er is de mogelijkheid voorzien om te melden, niet enige verplichting.

2. Definities

Inbreuken: handelingen of nalatigheden die onrechtmatig zijn, betrekking hebben op bepaalde domeinen en ingaan tegen het doel of de toepassing van de regels in deze domeinen;

Informatie over inbreuken: informatie, waaronder redelijke vermoedens, over feitelijke of mogelijke inbreuken, die hebben plaatsgevonden of zeer waarschijnlijk zullen plaatsvinden, alsmede over pogingen tot verhulling van dergelijke inbreuken;

Melding of melden: het mondeling of schriftelijk meedelen van informatie over inbreuken;

Interne melding: het binnen een juridische entiteit in de private sector mondeling of schriftelijk meedelen van informatie over inbreuken;

Externe melding: het mondeling of schriftelijk aan de federale coördinator of aan de bevoegde autoriteiten meedelen van informatie over inbreuken;

Openbaarmaking of openbaar maken: het publiek toegankelijk maken van informatie over inbreuken;

Melder: een persoon die informatie over inbreuken meldt of openbaar maakt;

Werkgerelateerde context: huidige of vroegere beroepsactiviteiten in de private sector waardoor, ongeacht de aard van die activiteiten, personen informatie kunnen verkrijgen over inbreuken en waarbij die personen te maken kunnen krijgen met represailles indien zij dergelijke informatie zouden melden;

Facilitator: een natuurlijke persoon die een melder bijstaat in het meldingsproces en wiens bijstand vertrouwelijk moet zijn;

Betrokkene: een natuurlijke of rechtspersoon die in de melding of bij de openbaarmaking wordt genoemd als persoon aan wie de inbreuk wordt toegeschreven of met wie die persoon in verband wordt gebracht;

Represaille: elke directe of indirecte handeling of nalatigheid naar aanleiding van een interne of externe melding of openbaarmaking, die tot ongerechtvaardigde benadeling van de melder leidt of kan leiden;

Anonieme melding: melding waarvan niemand, zelfs niet de ontvanger, de identiteit van de auteur kent;

Meldingsbeheerder: de onpartijdige persoon of dienst die bevoegd is om de meldingen op te volgen, de communicatie met de melder te onderhouden, hem indien nodig om bijkomende informatie te verzoeken, hem feedback te verstrekken en, indien van toepassing, meldingen te ontvangen.

3. Toepassingsgebied

3.1. Waarover kan er gemeld worden ?

a. Via het meldingskanaal dat Moore op haar intranet (Touch) ter beschikking stelt kunnen inbreuken of informatie over inbreuken worden gemeld die betrekking hebben op de **volgende gebieden** :

- overheidsopdrachten;
- financiële diensten, producten en markten, voorkoming van witwassen van geld en terrorismefinanciering;
- productveiligheid en -conformiteit;
- veiligheid van het vervoer;
- bescherming van het milieu;
- stralingsbescherming en nucleaire veiligheid;
- veiligheid van levensmiddelen en diervoeders, diergezondheid en dierenwelzijn;
- volksgezondheid;
- consumentenbescherming;
- bescherming van de persoonlijke levenssfeer en persoonsgegevens, en beveiliging van netwerk- en informatiesystemen;
- de financiële belangen van de EU komen in het gedrang of de interne markt wordt verstoord;
- bestrijding van belastingfraude;
- bestrijden sociale fraude.

b. Vallen **niet onder het toepassingsgebied** van de klokkenluiderspolicy:

- klachten in verband met geweld, pesten en ongewenst seksueel gedrag ;
- meldingen op basis van informatie gedekt door het medisch beroepsgeheim;
- klachten in verband met de dienstverlening van Moore (bijvoorbeeld klachten over facturen);
- klachten met betrekking tot een tewerkstellingssituatie (onbetaald loon, loon dat niet conform is, verplichting tot overwerken, verboden werken op zon- en feestdagen, werken in onveilige of ongezonde omstandigheden, enz.) en die geen sociale fraude inhouden.

Voor voorgaande meldingen kan men zich wenden tot de bestaande kanalen zoals, afhankelijk van de melding, de vertrouwenspersoon vermeld in het arbeidsreglement, de HR dienst, of de dossierbeheerder van de klant.

3.2. Wie kan een melding doen?

Alle werknemers, contractanten en derden die verbonden zijn aan Moore en die informatie over inbreuken hebben verkregen in een **werkgerelateerde context** kunnen een melding doen. Het gaat onder meer over **volgende personen**:

- werknemers;
- werknemers van een onderaannemer;
- zelfstandigen;
- aandeelhouders of bestuurders;
- stagiairs;
- vrijwilligers die in een werkgerelateerde context informatie over inbreuken heeft verkregen;
- voormalige werknemers;
- sollicitanten.

4. Rapporteringsmogelijkheden

Als melder kan je **op 3 manieren** een melding doen. Hoewel niet verplicht, acht Moore het wenselijk dat er eerst gebruik wordt gemaakt van de interne meldingskanalen.

4.1. Interne melding

Het **intern meldingskanaal** is een meldingsplatform **Whistleblower Software** dat door een externe firma ter beschikking wordt gesteld als webbased applicatie waar **u als melder schriftelijk of mondeling** een melding kan doen. Moore en de met haar verbonden vennootschapen werken samen om een gedane melding te beheren en deze melding te onderzoeken of op te volgen. Bij het doen van een melding wordt gevraagd om aan te geven vanuit welke Business Unit de melding afkomstig is of op welke Business Unit deze melding betrekking heeft. De term Business Unit is geen wettelijke notie maar een binnen Moore gekend begrip om de afdeling aan te duiden waarbinnen de activiteit wordt verricht.

De **functie van meldingsbeheerder** wordt intern ingevuld door Irene Timmermans van Accountancy. Betreft het een melding tot voorkoming van witwassen van geld en terrorismefinanciering, dan heeft de meldingsbeheerder het recht om de melding te delen met de AMLCO (interne coördinator anti-witwasregelgeving) van Moore en/of de verantwoordelijke persoon op het hoogste niveau in toepassing de anti-witwasregelgeving. Voor andere meldingen zal de meldingsbeheerder in het kader van het onderzoek samenwerken met aangewezen personen uit de betrokken Business Unit.

Indien er onduidelijkheden of bijkomende vragen zijn bij de melding kan de meldingsbeheerder bijkomende informatie vragen aan de melder. De melder heeft ook steeds de mogelijkheid de meldingsbeheerder te contacteren teneinde een overleg te vragen over de melding.

Te allen tijde wordt de vertrouwelijkheid van de melder en van de melding gewaarborgd.

4.2. Externe melding

Naast het intern meldingskanaal kan een melder zich wenden tot een extern meldingskanaal. Dit kan hij doen nadat hij eerst een melding heeft gedaan via het intern meldingskanaal, maar dit is niet vereist, doch wel wenselijk. Een melder kan zich dus ook rechtstreeks wenden tot één van de aangewezen autoriteiten. Deze instanties kunnen meldingen ontvangen, feedback geven en zullen de melding opvolgen.

Deze autoriteiten staan op verzoek van de melder de betrokkenen bij ten aanzien van elke administratieve of gerechtelijke autoriteit die betrokken is bij hun bescherming tegen represailles en kunnen naar aanleiding daarvan in het bijzonder bevestigen dat die persoon een melding heeft gedaan overeenkomstig deze wet.

De lijst van bevoegde overheidsinstanties is de volgende:

Overheidsopdrachten	Dienst Overheidsopdrachten van de FOD Kanselarij van de Eerste minister
Financiële diensten, producten en markten, voorkoming van witwassen van geld en terrorismefinanciering	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
Productveiligheid en productconformiteit	FOD Economie, FOD Volksgezondheid, FAGG, BIPT, FOD Mobiliteit

Veiligheid van het vervoer	FOD Mobiliteit, Nationale Autoriteit voor Maritieme Beveiliging.
Bescherming van het milieu	FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu, Leefmilieu Brussel, CREG, Algemene Directie Energie, ACER.
Stralingsbescherming en nucleaire veiligheid	Federaal Agentschap voor Nucleaire Controle.
Veiligheid van levensmiddelen en diervoeders, diergezondheid en dierenwelzijn	FAVV, FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu.
Volksgezondheid	Sciensano, FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu, FAGG, Federale commissie “Rechten van de patiënt”
Consumentenbescherming	FOD Economie
Bescherming van de persoonlijke levenssfeer en persoonsgegevens, en beveiliging van netwerk- en informatiesystemen	Gegevensbeschermingsautoriteit, CCB, EDPS

Bij gebrek aan een aangewezen autoriteit is de bevoegde autoriteit de federale Ombudsman. U kan deze als volgt contacteren:

- Via meldingsformulier: https://www.federaalombudsman.be/nl/meldingsformulier
- Via email: integriteit@federaalombudsman.be
- Op afspraak: Stuur een e-mail naar integriteit@federaalombudsman.be of bel het nummer 0800 999 61 om een afspraak te maken met één van de medewerkers van het Centrum Integriteit.

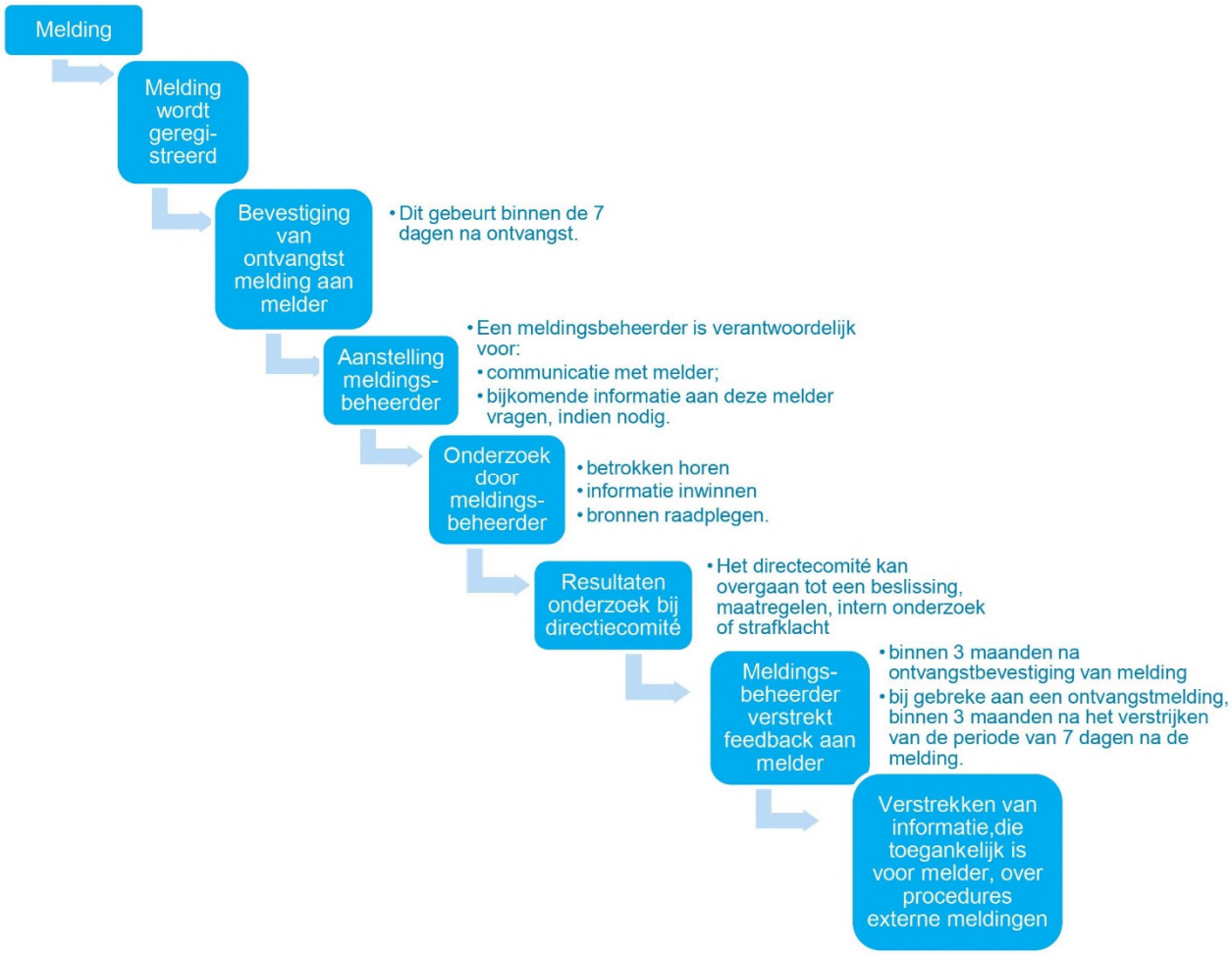
4.3. Openbaarmaking

Een melder die een openbaarmaking doet, komt slechts in bepaalde gevallen in aanmerking voor bescherming. Ten eerste moet de melder eerst een interne en externe melding, of meteen een externe melding hebben gedaan waarna er geen passende maatregelen zijn genomen binnen de genoemde termijnen. Daarnaast moet de melder gegronde redenen hebben om aan te nemen dat:

- de inbreuk een dreigend of reëel gevaar kan zijn voor het algemeen belang of;
- er een risico op represailles bestaat bij een externe melding of;
- de kans klein is dat de inbreuk doeltreffend wordt verholpen, wegens de bijzondere omstandigheden van de zaak (bv. bewijsmateriaal kan worden achtergehouden of vernietigd,…).

5. Onderzoeksverloop na een interne melding

De procedure die wordt gestart na de melding kan als volgt worden weergegeven :



1. De melder doet een **melding** via het daaraan toegewezen kanaal.
2. De **melding** wordt geregistreerd door het platform, samen met de datum waarop de melding gebeurde.
3. Binnen de zeven dagen na ontvangst krijgt de melder een **bevestiging van ontvangst** van de melding.
4. Na ontvangst van de melding wordt de **meldingsbeheerder aangesteld.** Deze is verantwoordelijk voor de communicatie met de melder en zal het onderzoek voeren.

5. Deze meldingsbeheerder zal tijdens het **onderzoek** de juistheid van de gedane beweringen in de melding nagaan, de melding opvolgen en de gemelde inbreuken indien nodig aanpakken.

   De meldingsbeheerder is in deze hoedanigheid gemachtigd om op onafhankelijke wijze een onderzoek op te starten. Hij kan

   - de betrokken personen horen
   - informatie inwinnen
   - bronnen raadplegen.

   Aan de hand van deze onderzoeksdaden moet de meldingsbeheerder de juistheid van de gedane beweringen in de melding nagaan. Bij deze informatie-inwinning wordt de vertrouwelijkheid van de betrokken personen beschermd.

6. De **meldingsbeheerder rapporteert zijn bevindingen schriftelijk aan het directiecomité**. Enkel indien de melding een lid van het directiecomité betreft, wordt het rapport gericht aan de voorzitter van het directiecomité. Het directiecomité neemt een beslissing en treft eventuele maatregelen op basis van het rapport van de melder. Afhankelijk van wat er werd bevonden door de meldingsbeheerder kan er een intern onderzoek worden opgestart of kan Moore een strafklacht indienen.

7. Na het finaliseren van het onderzoek verstrekt de meldingsbeheerder aan de melder **feedback** over de geplande opvolging en de redenen hiervoor, over de maatregelen om juistheid van de beweringen na te gaan en over maatregelen om inbreuk aan te pakken. Zowel de melder als de betrokken personen worden geïnformeerd over het afsluiten van het onderzoek. De melder zal een bericht ontvangen dat de feedback klaar is en dat hij of zij deze kan lezen op het platform. Dit gebeurt ten laatste drie maanden na de ontvangstbevestiging of binnen de drie maanden na het verstrijken van de periode van zeven dagen na de melding.

6. Vertrouwelijkheid en bescherming persoonsgegevens

De melding en behandeling van een melding verloopt steeds met respect voor de **geheimhouding en vertrouwelijkheid**.

De **gegevens van de melder worden vertrouwelijk gehouden.** De melder wordt ook de mogelijkheid geboden om anoniem te melden. Verder hebben **niet-gemachtigde personeelsleden** geen toegang tot het intern meldingskanaal.

Daarnaast wordt de **identiteit van de melder en de betrokken derden** (facilitator, derden verbonden met melder en die het slachtoffer kunnen worden van represailles in een werkgerelateerde context) met vertrouwelijkheid behandeld. Dit geldt ook voor alle andere informatie waaruit de identiteit van de melder direct of indirect kan worden afgeleid. De identiteit van de melder en de betrokken derden is enkel gekend door de meldingsbeheerder, tenzij de melder hem daar schriftelijk van ontheft. De geheimhoudingsplicht over de betrokken derden eindigt wanneer de onderzoeksprocedure wordt beëindigd.

In ruil voor deze geheimhouding en vertrouwelijkheid wordt van de melder gevraagd om **vertrouwelijk om te gaan met zijn melding** en deze noch rechtstreeks, noch via derden, openbaar te maken totdat de meldingsbeheerder de beëindiging van het onderzoek heeft meegedeeld.

Elke **verwerking van persoonsgegevens** in het kader van een interne melding gebeurt overeenkomstig de Europese Verordening 2016/679 ofwel de Algemene Verordening Gegevensbescherming (AVG) en overeenkomstig het privacybeleid van Moore dat u hier kunt raadplegen. Voor de verwerking van persoonsgegevens in het kader van de klokkenluidersprocedure wordt Moore als verwerkingsverantwoordelijke beschouwd. Iedere melding wordt geregistreerd in een daartoe voorzien register. Moore werkt voor het organiseren van haar intern meldingskanaal samen met een externe dienstverlener (Whistleblower Software Aps) die fungeert als haar externe verwerker. Zowel Moore als haar externe verwerker bieden de nodige waarborgen inzake vertrouwelijkheid en veiligheid. De persoonsgegevens worden enkel binnen de Europese Unie verwerkt.

7. Bescherming

7.1. Voorwaarden om bescherming te genieten

Een melder kan zich beroepen op beschermingsmaatregelen als hij **gegronde redenen** had om aan te nemen dat de **informatie over inbreuken op het moment van de melding correct was** en **binnen het toepassingsgebied van deze policy viel**, op

voorwaarde dat de **correcte procedures** werden gevolgd van de interne of externe melding of openbaarmaking.

Facilitatoren en derden die verbonden zijn met de melders komen eveneens in aanmerking voor de hierna bepaalde beschermingsmaatregelen, indien ze gegronde redenen hadden om aan te nemen dat de melder binnen het toepassingsgebied voor bescherming van deze policy viel.

Indien blijkt dat de **melding onjuist of ongegrond is,** dan geniet de melder nog steeds de bescherming als deze **melding te goeder trouw werd gedaan**. De onderneming kan dus geen schade verhalen op de melder. De melder wordt vrijgesteld van burgerrechtelijke, strafrechtelijke of tuchtrechtelijk aansprakelijkheid.

Daarnaast kunnen melders niet aansprakelijk worden gesteld voor de verwerving van of de toegang tot de **informatie die wordt gemeld of openbaar wordt gemaakt**, tenzij die verwerving of toegang op zichzelf een strafbaar feit uitmaakt.

Voor elke andere mogelijke aansprakelijkheid van melders die voortvloeit uit handelingen of nalatigheden die **geen verband houden met de melding of openbaarmaking of die niet noodzakelijk zijn voor het onthullen van een inbreuk**, blijft het toepasselijk recht gelden.

Een melder die **opzettelijk een manifest ongegronde melding** heeft gedaan, en aldus op onrechtmatige wijze gebruik heeft gemaakt van de meldingsprocedure van deze policy kan hiervoor gesanctioneerd worden.

7.2. Bescherming in de vorm van het verbod op represailles

Indien de melder, de facilitator of derde die verbonden is met de melder aan bovenvermelde voorwaarden voldoet, geniet hij **bescherming tegen elke vorm van onbillijke behandeling, nadelige beslissingen of represailles**

7.3. Indien de melder toch slachtoffer wordt van represailles

7.3.1. Intern melden

Indien de melder van mening is dat hij of zij het slachtoffer is geworden van represailles, dan kan deze dit altijd **melden aan HR**. Op die manier kan er binnen Moore aan een oplossing worden gewerkt.

7.3.2. Juridische procedures

Daarnaast staan er steeds juridische procedures open voor de melder indien er represailles werden genomen.

8. Ondersteuningsmaatregelen

Iedereen die een melding wil doen, heeft recht op

- informatie en adviezen over procedures en remedies die bescherming bieden tegen represailles alsmede over de rechten van de betrokkene;
- technische, psychologische, en sociale ondersteuning.

Het **Federaal Instituut voor de bescherming en de bevordering van de rechten van de mens** speelt een belangrijke rol in het voorzien en ondersteunen van zulke maatregelen. Men kan zich derhalve tot deze instantie wenden.