Klokkenluiders Policy

1 Doel

Vlaams Instelling voor Technologisch Onderzoek, VITO, met maatschappelijke zetel te Boeretang 200, 2400 Mol en met ondernemingsnummer 0244.195.916 (hierna genaamd de Organisatie) wil in haar activiteiten integer en ethisch handelen en wil er daarom voor zorgen dat haar medewerkers de mogelijkheid hebben, conform de hierna vastgestelde modaliteiten en voorwaarden, om in de Organisatie vastgestelde of vermoede inbreuken op de in punt 2.2 van deze policy bedoelde wettelijke en regelgevende normen, op de meest serene en vertrouwelijke manier te kunnen melden.

Het zijn vaak de eigen medewerkers die als eerste op de hoogte zijn van bedreigingen of inbreuken die zich binnen een organisatie voordoen. Zij zouden echter tegengehouden kunnen worden om hun bezorgdheid of vermoedens te uiten uit angst voor reacties of represailles.

Deze mogelijke vrees zou er echter uiteindelijk toe kunnen leiden dat de Organisatie in het ongewisse blijft over mogelijke inbreuken en niet de nodige stappen kan ondernemen om deze inbreuken aan te pakken. Dit zou dan ook de belangen van de Organisatie, die hoogstaande normen van goed bestuur en beroepsethiek nastreeft, kunnen inperken.

Het doel van deze policy is om dergelijke situaties te voorkomen door alle medewerkers en andere personen die een contractuele relatie met de Organisatie hebben, sterk aan te moedigen om elke inbreuk, illegale, onethische of frauduleuze activiteit met betrekking tot de activiteiten van de Organisatie te melden zonder angst voor sancties of andere maatregelen.

Deze policy is opgesteld overeenkomstig het Bestuursdecreet van 7 december 2018 betreffende de bescherming van melders van inbreuken op het Unie- of het nationale recht vastgesteld binnen de Vlaamse overheid en Vlaamse instellingen, in overeenstemming met de Europese 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.

Deze policy heeft tot doel:

- de vertrouwelijke, al dan niet anonieme melding van informatie over mogelijke of daadwerkelijke inbreuken mogelijk te maken;
- een bescherming te bieden aan personen die een inbreuk melden of de melder bijstaan;
- de procedure vast te leggen die de melder van een inbreuk daartoe moet volgen.

Deze policy is beschikbaar op de website van VITO (onder het luik ‘over VITO’ - Corporate governance) en op het VITO intranet Channel V (onder het luik Personeel & Organisatie - Regels en voorschriften) en kan geactualiseerd/gewijzigd worden. Bij wijziging gebeurt er telkens een melding.

Deze policy sluit uiteraard op geen enkele wijze de directe dialoog en communicatie van informatie, buiten de meldingsprocedure om, uit. De Organisatie wil benadrukken dat medewerkers met bezorgdheden of vermoedens zich ten allen tijde kunnen richten tot hun leidinggevenden, de afdeling Personeel en Organisatie of de vertrouwenspersonen.

2 Toepassingsgebied

2.1 Wie valt onder dit policy?

Deze policy is van toepassing op de volgende personen:

- huidige en vroegere werknemers, die verbonden zijn of waren in het kader van een arbeidsovereenkomst met de Organisatie;
- huidige en vroegere medewerkers, die niet verbonden zijn met een arbeidsovereenkomst met de Organisatie;
- kandidaten die betrokken zijn of waren in een rekruteringsprocedure in de Organisatie;
- personen die op zelfstandige basis samenwerken of hebben samengewerkt met de Organisatie en de kandidaten voor een zelfstandige samenwerking in het kader van precontractuele onderhandelingen;
- vrijwilligers en stagiairs (bezoldigd of onbezoldigd);
- aandeelhouders en leden van het bestuurs-, leidinggevend of toezichthoudend orgaan van de Organisatie (met inbegrip van niet-uitvoerende leden);
- elke persoon die werkt of gewerkt heeft onder toezicht en leiding van aannemers, onderaannemers en/of leveranciers van de Organisatie;
- eenieder die informatie heeft over inbreuken in de Organisatie op het gebied van financiële diensten, producten en markten zelfs buiten een werk gerelateerde context.

2.2 Welke inbreuken kunnen gemeld worden?

Alle inbreuken op wetgeving en regelgeving die in Vlaanderen van toepassing zijn, kunnen het voorwerp uitmaken van een klokkenluidersmelding. Het gaat dan om een handeling of nalatigheid die onrechtmatig is, of het doel of de toepassing van regelgeving ondermijnt.

3 De melding

3.1 Doel van de melding

Elke inbreuk met betrekking tot de in punt 2.2 bedoelde gebieden alsook elke informatie over dergelijke inbreuken, met inbegrip van elk redelijk vermoeden van daadwerkelijke of potentiële inbreuken die hebben plaatsgevonden of zeer waarschijnlijk zullen plaatsvinden binnen de Organisatie, en pogingen om dergelijke inbreuken binnen de Organisatie te verbergen, kunnen schriftelijk of mondeling worden aangemeld via een van de in punt 4 bedoelde kanalen.

3.2 De voorwaarden voor een melding en bescherming

Om bescherming te genieten, hanteert de richtlijn het criterium dat de melder ten tijde van de melding redelijke gronden moet hebben om aan te nemen dat de door hem gemelde zaken op waarheid berusten en binnen het toepassingsgebied van de richtlijn vallen.

VITO baseert zich op het algemene wettelijke kader op het vlak van bescherming en sanctionering, doch neemt aan dat een werknemer niet altijd kan weten of het punt dat zij/hij wenst aan te kaarten onder de toepassing van het Unieriecht valt, waardoor vergissingen kunnen voorvallen.

4 Meldingskanalen

Elke persoon die onder deze policy valt en die informatie heeft over reële of vermoede inbreuken bedoeld in punt 2.2 wordt aangemoedigd om dit zo spoedig mogelijk te goeder trouw en overeenkomstig de principes zoals opgenomen in punt 3.2 aan de Organisatie te melden.

4.1 Interne meldingskanalen

4.1.1 Wie kan gebruik maken van het intern meldingskanaal?

De interne meldingskanalen die door de Organisatie zijn opgezet en die in punt 4.1.2 van deze policy worden beschreven, staan uitsluitend open voor medewerkers van de Organisatie.

4.1.2 Welke kanalen staan ter beschikking?

Een melding van een inbreuk kan plaatsvinden via één van de volgende kanalen:

- Online via de klokkenluidertool van VITO: vito.sdwhistle.com
- Per post
    - Verantwoordelijke Human Capital, Boeretang 200, 2400 Mol
    - Diversity & Inclusion Officer, Boeretang 200, 2400 Mol
- Per telefoon
    - Verantwoordelijke Human Capital: +32 14 33 55 76
    - Diversity & Inclusion Officer: +32 14 33 55 72
- Via een fysieke ontmoeting

De melding vindt bij voorkeur plaats in het Nederlands of het Engels. Elke melding die in een andere taal gebeurt, zal eerst moeten worden vertaald aangezien dit de nauwkeurigheid van de inhoud van de melding kan aantasten.

Het is ook mogelijk om te verzoeken om een persoonlijke ontmoeting met de meldingsbeheerder zoals hieronder vermeld in punt **4.1.4** van deze policy.

Elk van de bovengenoemde kanalen wordt op een vertrouwelijke en beveiligde manier beheerd, zodat de vertrouwelijkheid van de identiteit van de melder en eventuele in de melding genoemde derden gewaarborgd is. De toegang tot de kanalen is strikt beperkt tot medewerkers die er toegang toe hebben op basis van verantwoordelijkheden en/of bevoegdheden.

4.1.3 Hoe verloopt de melding?

Een melding omvat een korte omschrijving van de redelijke vermoedens over een gepleegde of mogelijke inbreuk op één van de in artikel 2.2. vermelde domeinen die heeft plaatsgevonden of die zeer waarschijnlijk zal plaatsvinden alsmede over de eventuele pogingen tot het verhullen of verbergen van dergelijke inbreuken.

De melding kan ook anoniem geschieden op de volgende wijze:

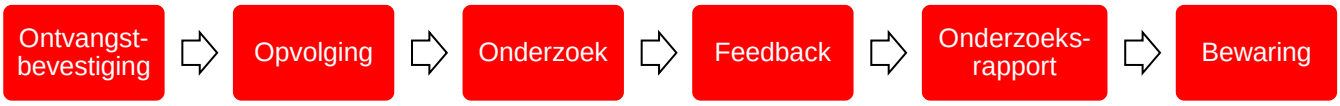
- Melding in de klokkenluidertool VITO door gebruik te maken van een anoniem emailadres: vito.sdwhistle.com
- het opstellen van niet-handgeschreven brief die wordt gepost op een wijze dat er geen enkele

link kan worden gelegd met de eventuele identiteit of woonplaats van de melder en met vermelding van een wijze waarop deze (anoniem) kan gecontacteerd worden in het kader van de opvolging van de melding.

De melding moet voldoende gedetailleerd en gedocumenteerd zijn en moet de volgende gegevens bevatten (wanneer de relevante informatie bekend is):

- een gedetailleerde beschrijving van de gebeurtenissen en hoe deze onder de aandacht van de melder zijn gekomen;
- de datum en plaats van de gebeurtenis;
- de namen en functies van de betrokken personen, of informatie die hun identificatie mogelijk maakt;
- de namen van andere personen, indien van toepassing, die de gemelde feiten kunnen bevestigen;
- bij het doen van een melding, de naam van de melder (deze informatie wordt niet gevraagd wanneer een anonieme melding wordt gedaan); en
- alle andere informatie of elementen die het onderzoeksteam kunnen helpen om de feiten te verifiëren.

4.1.4 Wat gebeurt er na de melding?



1-Ontvangstbevestiging
De opsteller van de melding zal binnen 7 dagen na melding een ontvangstbevestiging ontvangen. Tevens wordt een dossiernummer verstrekt met het oog op de opvolging van het dossier.

2-Opvolging
Opvolging verwijst naar elk optreden van de ontvanger van een melding om de juistheid van de in de melding gedane beweringen na te gaan en de gemelde inbreuk zo nodig aan te pakken, onder meer via maatregelen zoals een intern vooronderzoek, onderzoek, vervolging, een terugvordering van middelen of het beëindigen van de procedure.

De meldingsbeheerder volgt meldingen op, onderhoudt de communicatie met de melder, vraagt indien nodig bijkomende informatie op, koppelt terug naar de melder en neemt eventueel nieuwe meldingen in ontvangst.

3-Onderzoek

De melding zal snel en zorgvuldig worden onderzocht in overeenstemming met deze policy. Alle onderzoeken worden grondig uitgevoerd met inachtneming van de beginselen van vertrouwelijkheid, onpartijdigheid en eerlijkheid ten opzichte van alle betrokken personen. De meldingsbeheerder stelt, indien nodig, een onderzoeksteam samen. Het onderzoeksteam krijgt de bevoegdheid overeenkomstig de bestaande procedures en policies binnen de organisatie.

Personen die betrokken zijn bij de (mogelijke) inbreuken die door de melder worden gemeld, worden uitgesloten van het onderzoeksteam en mogen ook niet deelnemen aan de beoordeling van de melding of de vaststelling van de te ondernemen acties met betrekking tot de melding.

Belangenconflicten worden gerapporteerd aan de raad van bestuur indien de directie/het dagelijks bestuur wordt geviseerd in de melding. Indien de raad van bestuur betrokken lijkt, dan neemt de voorzitter van de Raad van Bestuur de nodige stappen en informeert indien nodig de voogdijminister of diens kabinet.

De meldingsbeheerder kan beslissen een melding wel of niet te onderzoeken na hierover te hebben overlegd met het management binnen de organisatie.

4-Feedback
De meldingsbeheerder zal de melder passende feedback geven binnen een redelijke termijn, en ten hoogste binnen drie maanden vanaf de datum van de ontvangstbevestiging van de melding. Deze feedback bevat informatie voor de melder over de geplande en/of ondernomen maatregelen en de redenen voor deze maatregelen. Hij/zij informeert de melder via het gekozen interne meldingskanaal.

5-Onderzoeksrapport
Na afloop van het onderzoek stelt het onderzoeksteam een overzichtsrapport op, waarin de uitgevoerde onderzoeksmaatregelen worden beschreven. Een geredigeerde, niet- vertrouwelijke en geanonimiseerde versie van dit overzichtsrapport kan, uitsluitend op 'need-to-know'-basis, buiten het onderzoeksteam worden gedeeld met het lokale of executive management om tot een definitieve beslissing te komen.

Een lid van het onderzoeksteam stelt een eindrapport op met een beschrijving van de feiten en de uiteindelijke beslissing:

i. In het geval dat de (mogelijke) inbreuk wordt aangetoond, worden relevante acties vastgesteld met het oog op het tegengaan van de (mogelijke) inbreuk en het beschermen van de Organisatie; of
ii. In het geval dat uit het onderzoek blijkt dat er onvoldoende of geen bewijs is van de (mogelijke) inbreuk, wordt er geen verdere actie ondernomen.

De melder wordt via het gekozen intern meldingskanaal geïnformeerd over de afsluiting van de melding en de genomen beslissing.

4.1.5 De meldingsbeheerder

De Organisatie heeft de opvolging van interne meldingen toevertrouwd aan de Verantwoordelijke Human Capital (als bevoegd persoon) en mede gedelegeerd aan de Diversity & Inclusion Officer.

4.1.6 Registratie van de meldingen

De Organisatie houdt een register bij van alle ontvangen meldingen, in overeenstemming met de vertrouwelijkheidsmaatregelen die in paragraaf 5.1 van deze policy worden uiteengezet.

Deze meldingen en de ermee verbonden informatie worden bewaard zolang de contractuele relatie tussen de melder en de Organisatie loopt.

Wanneer voor het melden, met de instemming van de melder, een telefoonlijn met gespreksopname wordt gebruikt, zal de Organisatie de mondelinge melding als volgt registreren:

- door een opname van het gesprek in een duurzame en opvraagbare vorm; of
- door een volledige en nauwkeurige schriftelijke weergave van het gesprek opgesteld door de meldingsbeheerder. De melder zal de mogelijkheid worden geboden deze schriftelijke weergave te controleren, corrigeren en voor akkoord te tekenen.

Indien voor de melding een telefoonlijn zonder gespreksopname wordt gebruikt, zal de Organisatie de mondelinge melding registreren in de vorm van een nauwkeurig verslag van het gesprek, opgesteld door het voor het behandelen van de melding verantwoordelijke personeelslid. De melder zal de mogelijkheid worden geboden dit verslag te controleren, corrigeren en voor akkoord te tekenen.

In geval een persoonlijke ontmoeting plaatsvindt met de meldingsbeheerder zal, mits de melder hiermee instemt, een volledig en nauwkeurig verslag van het onderhoud worden bijgehouden in een duurzame en opvraagbare vorm. De Organisatie heeft het recht om het onderhoud te registeren als volgt:

- door een gespreksopname in een duurzame en opvraagbare vorm;
- door een nauwkeurig verslag van het onderhoud. De melder zal de mogelijkheid worden geboden dit verslag te controleren, corrigeren en voor akkoord te tekenen.

4.2 Externe meldingskanaal

Melders kunnen gebruik maken van het extern meldingskanaal georganiseerd door de Vlaamse ombudsdienst indien zij dit geschikter achten.

De Vlaamse Ombudsdienst is verantwoordelijk voor het ontvangen van externe meldingen, het controleren van de ontvankelijkheid ervan en het doorsturen naar de bevoegde autoriteit voor onderzoek, die verschillend zal zijn naargelang het voorwerp van de melding.

Deze autoriteit kan bijvoorbeeld de FOD Policy & Ondersteuning zijn (op het gebied van overheidsopdrachten), de Autoriteit voor Financiële Diensten en Markten (FSMA), de Nationale Bank van België (NBB) of het College van Toezicht op de Bedrijfsrevisoren (op het gebied van financiële diensten, producten en markten), de FOD Economie (op het gebied van consumentenbescherming), de Gegevensbeschermingsautoriteit (op het gebied van de bescherming van de persoonlijke levenssfeer en persoonsgegevens), enz.

In uitzonderlijke gevallen kan de Vlaamse Ombudsdienst ook het onderzoek ten gronde voeren.
De contactgegevens van de Vlaamse Ombudsdienst zijn als volgt:

Adres: Vlaamse Ombudsdienst, Leuvenseweg 86, 1000 Brussel
E-mail: klokkenluiden@vlaamseombudsdienst.be
Telefoon: 02 552 48 48

5 Beschermingsmaatregelen

De Organisatie engageert zich ertoe om alles in het werk te stellen om de personen die onder deze policy vallen, een gepaste en effectieve bescherming te bieden voor zover de melding voldoet aan de voorwaarden van het decreet met name door de volgende maatregelen te nemen:

5.1 Waarborg van de vertrouwelijkheid

De Organisatie garandeert de nodige maatregelen te nemen opdat medewerkers en andere door deze policy beoogde personen in alle vertrouwen een melding kunnen neerleggen bij de Organisatie.

De Organisatie verbindt zich ertoe de nodige maatregelen te voorzien zodat de identiteit van de melder niet zonder zijn vrije en uitdrukkelijke toestemming kan worden bekend gemaakt aan andere personen dan de personeelsleden die bevoegd zijn om meldingen te ontvangen of op te volgen.

Dit geldt ook voor alle informatie waaruit de identiteit van de melder rechtstreeks of onrechtstreeks kan worden afgeleid.

In afwijking van het vorige lid kan de identiteit van de melder van de inbreuk worden bekendgemaakt wanneer dit krachtens bijzondere wetgeving in het kader van een onderzoek door de nationale autoriteiten of in het kader van een gerechtelijke procedure noodzakelijk en evenredig is, met name ter bescherming van de rechten van de verdediging van de betrokkene.

In het laatste geval wordt de melder geïnformeerd over de bekendmaking van zijn of haar identiteit voordat deze plaatsvindt, tenzij deze informatie lopende onderzoeken of gerechtelijke procedures in gevaar zou brengen. Dit is bijvoorbeeld het geval als de melder een belangrijke getuige in de rechtbank vertegenwoordigt of in geval van ongerechtvaardigde of onrechtmatige aangifte om de rechten van de verdediging van de betrokkene te beschermen.

5.2 Bescherming tegen represaillemaatregelen

Elke vorm van represailles tegen de in artikel 2.1 bedoelde personen die krachtens deze policy bescherming genieten, met inbegrip van het dreigen met represailles en pogingen tot represailles, is verboden.

6 Verwerking van persoonsgegevens

In het kader van de interne meldingsprocedure wordt de Organisatie beschouwd als de verantwoordelijke voor de verwerking van de persoonsgegevens.

Elke verwerking van persoonsgegevens in het kader van deze policy wordt uitgevoerd overeenkomstig de toepasselijke wetgeving inzake de bescherming van persoonsgegevens, met inbegrip van de Europese Algemene Verordening Gegevensbescherming (“AVG” of “GDPR”).

De volgende persoonsgegevens kunnen worden verwerkt in het kader van een melding: naam, functie, datum van indiensttreding, contactgegevens en e-mailadres van de melder en van personen, betrokken bij de inbreuk, alle geïdentificeerde of identificeerbare informatie die de melder levert en die wordt verzameld in het kader van het intern onderzoek. Deze verwerking van gegevens gebeurt in het kader van de naleving van een wettelijke verplichting en/of het gerechtvaardigd belang van de organisatie, in de mate het intern meldkanaal de wettelijke doelstellingen overstijgt, met name de detectie van inbreuken, het waarborgen van de veiligheid en het ethisch handelen van de Organisatie.

Persoonsgegevens die duidelijk niet relevant zijn voor de verwerking van een melding worden niet verzameld of, indien verzameld, zo spoedig mogelijk verwijderd. Deze gegevens worden bijgehouden

tot wanneer de inbreuk waarvan melding werd gedaan, is verjaard en in elk geval gedurende een termijn van vijf jaar na de melding.

De identiteit van de melder kan enkel bekend worden gemaakt met de toestemming van de melder. Andere gegevens blijven eveneens strikt confidentieel en worden enkel gedeeld op een strikte need-to-know basis.

Alle personen van wie persoonsgegevens worden verwerkt in het kader van meldingen van inbreuken hebben recht op inzage en kopie, recht op rectificatie, recht op gegevenswissing, recht van bezwaar en recht om een klacht in te dienen bij de toezichthoudende autoriteit overeenkomstig de toepasselijke wetgeving. Deze rechten kunnen evenwel beperkt worden door de rechten en vrijheden van anderen, in het bijzonder het recht van de melder op geheimhouding en het recht van de Organisatie op een correcte opvolging van de melding.

Voor meer informatie over de verwerking van persoonsgegevens verwijzen we naar de HR Privacy kennisgevingen voor medewerkers, sollicitanten, zelfstandige dienstverleners en uitzendkrachten en de HR Privacy Policy die beschikbaar is op het intranet (Channel V – P&O – Regels en Voorschriften) van de Organisatie.

7 Inwerkingtreding

Deze policy gaat in op 1 augustus 2023 voor onbepaalde tijd.

De Organisatie behoudt zich het recht voor om deze policy - na overleg met de vakorganisaties - ten allen tijde te wijzigen, onder meer maar niet uitsluitend naar aanleiding van wijzigingen in relevante regelgeving en/of operationele behoeften.