Bijlage 14: Policy klokkenluiders-procedure

Inhoudsopgave

1 ALGEMEEN

1.1 Doelstelling

Dit document omschrijft het beleid en de procedure voor de melding van integriteitsinbreuken binnen VOT en is een onderdeel van het integriteitsbeleid waarmee VOT een open en integere bedrijfscultuur nastreeft.

Op grond van het decreet 18 november 2022 tot wijziging van Provinciedecreet, decreet Lokaal Bestuur en Bestuursdecreet, wat betreft klokkenluiders (BS 01.12.2022, inwerking: 11.12.2022), hetgeen de omzetting van de Europese Klokkenluidersrichtlijn 2019/1937 is, moet iedere persoon die informatie over een ernstige probleem met betrekking tot mogelijke onregelmatigheden of wangedrag bij een openbaar bestuur heeft verkregen in een werkgerelateerde context, de mogelijkheid krijgen om melding te maken van deze onregelmatigheden of inbreuken.

De Belgische wetgeving voorziet dat onder meer moet worden voorzien in een intern meldingskanaal voor de zogenaamde "klokkenluiders" en ervoor moet zorgen dat deze, op straffe van sancties, worden beschermd tegen represailles. Hiervoor zet VOT een intern meldkanaal op, dat belast is met het verkrijgen en behandelen van de meldingen. Er wordt ook een procedure opgesteld voor de interne melding en opvolging ervan, hierna uiteengezet. Naast deze interne meldingskanaal, kan de melder ook een externe melding bij de bevoegde autoriteiten of een openbaarmaking doen. Deze twee kanalen worden tevens hieronder uitgelegd.

1.2 Begrippen

Voor de toepassing van deze policy gelden de volgende begrippen:

- Een klokkenluider is een persoon die inbreuken of vermoedens van inbreuken meldt aan personen of organen die hiertoe actie kunnen ondernemen. Door (vermoedens van) inbreuken te melden, kan een klokkenluider bijdragen aan het
    - identificeren van zwakke plekken van VOT;
    - voorkomen van misbruik, onregelmatigheden, fraude en wanpraktijken op de werkvloer;
    - voorkomen en onthullen van inbreuken op belangrijke wet- en regelgeving
    - en schade ten gevolge daarvan vermijden of beperken.

  Een melding door een klokkenluider kan ook leiden
    - tot het onderzoeken van wanpraktijken en inbreuken die anders verborgen blijven en schade ten gevolge daarvan vermijden of beperken;
    - bijdragen aan het behoorlijk bestuur van VOT.

1.3 Toepassingsgebied

Deze policy is van toepassing op iedereen die werkzaam is bij VOT of is geweest of werkzaamheden heeft verricht voor VOT in welke hoedanigheid ook: werknemers, ex-werknemers, statutair personeel, zelfstandigen, leveranciers, consultants, aannemers, onderaannemers, sollicitanten, vrijwilligers, bezoldigde en niet-bezoldigde stagiairs, managers, leidinggevenden, bestuurders, …

2 WAT KAN JE MELDEN?

Elke bezorgdheid over (mogelijke) inbreuken op het Europees Unierecht of nationaal recht, die gebaseerd is op informatie die je uit je werkomgeving verkreeg, op volgende gebieden:

- overheidsopdrachten;
- financiële diensten, producten en markten, voorkoming van witwassen van geld en terrorismefinanciering;
- productveiligheid en -conformiteit;
- veiligheid van 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;
- bestrijding van belastingfraude;
- sociale fraudebestrijding.

Vallen evenwel niet onder de toepassing van deze klokkenluiderspolicy:

- meldingen i.v.m. de veiligheid van het land;
- meldingen met betrekking tot geclassificeerde gegevens;
- meldingen op basis van informatie gedekt door de bescherming van het beroepsgeheim van advocaten en van het medisch beroepsgeheim;
- meldingen op basis van informatie gedekt door de geheimhouding van gerechtelijke beraadslagingen en het strafprocesrecht.
- Meldingen i.v.m. discriminatie pesterijen, geweld op het werk en ongewenst seksueel gedrag op het werk, cf. wetgeving welzijn op het werk waar andere procedures voor gelden zoals opgenomen in het arbeidsreglement.

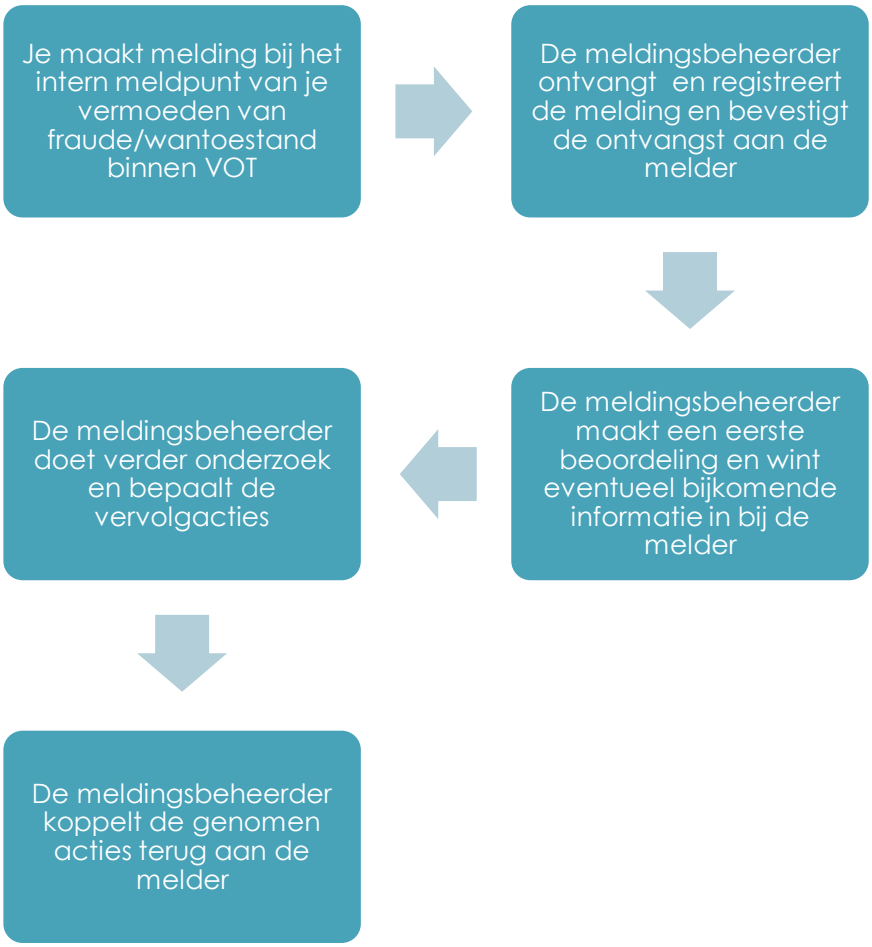
3 HOE KAN JE MELDEN?

Als je een (mogelijke) inbreuk die plaatsvond in je werkomgeving of een inbreuk, die zeer waarschijnlijk zal plaatsvinden, wil melden, dan raden wij je ten sterkste aan om dit onmiddellijk en eerst te melden aan je directe leidinggevende. Als dit niet kan, om welke reden ook, of als je melding aan je directe leidinggevende niet tot een bevredigende oplossing leidt, kan je je bezorgdheid melden via drie kanalen. Het intern kanaal is bij voorkeur de logische stap die eerst gebruikt wordt.

3.1 Intern kanaal

3.1.1 Procedure

Melders dienen zoveel mogelijk de hiertoe voorziene interne meldingskanalen te gebruiken. Deze interne kanalen hebben als doel inbreuken op de hierboven geschetste gebieden binnen de organisatie op te sporen en te verhelpen. Binnen VOT is de verantwoordelijke personeel meldingsbeheerder. De meldingsprocedure loopt als volgt:



1. ***Je maakt melding bij het intern meldpunt***

   - Je kan de keuze maken uit één van volgende interne meldingskanalen:
     - Telefonische melding bij Evy Huys op 057 22 62 90.
     - Melding per e-mail naar: meldpunt@votjeugdhulp.be
     - Schriftelijk aan: Meldpunt VOT, Poperingseweg 30, 8900 Ieper.
     - Melders kunnen ook verzoeken om binnen een redelijke termijn een inbreuk te melden via een fysieke ontmoeting. Een dergelijke fysieke melding kan op afspraak geregeld worden bij de personen hierboven vermeld onder 'telefonische melding'.

- Hierbij gelden volgende principes:
  - Vertrouwelijkheid: De werknemer die via het intern meldingskanaal een melding doet, kan dit eveneens op een anonieme wijze doen zodat zelfs de ontvanger van de melding je identiteit niet zal kennen. We raden je nochtans aan om je identiteit wel kenbaar te maken als je een melding doet. Enkel dan kan bijkomende informatie bij je opgevraagd worden om je melding te onderzoeken en er de gepaste opvolging aan te geven. Als je een anonieme melding doet, vermeld dan zoveel mogelijk details om de meldingsbeheerder toe te laten je melding ten gronde te onderzoeken.
  - Het bestaan van het intern meldingskanaal doet geen afbreuk aan het recht van de werknemer om, indien hij het nuttig acht, de personeelsdienst en/of vakbond met betrekking tot zijn rechten en verplichtingen te raadplegen vooraleer een melding te doen.

- Om de melding van een (mogelijke) inbreuk grondig te kunnen onderzoeken, is een goede omschrijving van de inbreuk belangrijk. Volgende vragen kunnen je hierbij helpen:
  - Wat is er gebeurd? Wat gaat er mogelijk gebeuren?
  - Wanneer is het gebeurd?
  - Waar is het gebeurd? Binnen welke dienst/afdeling/team?
  - Wie was of is erbij betrokken?
  - Is de situatie nog steeds aan de gang?
  - Namen van andere personen of getuigen die de gemelde feiten kunnen bevestigen?
  - Andere gegevens of elementen die kunnen helpen om de melding te onderzoeken? Je kan eventueel een bijlage (document, foto, filmpje, …) toevoegen van de (mogelijke) inbreuk.
  - Heb je de kwestie al besproken of kenbaar gemaakt via andere kanalen? Met wie/welke kanalen?
  - Als je je kenbaar maakt: wat zijn jouw contactgegevens?

2. De meldingsbeheerder ontvangt en registreert de melding en bevestigt de ontvangst aan de melder

- De meldingsbeheerder die een melding ontvangt, stuurt aan de melder een bevestiging van ontvangst van de melding binnen de 7 werkdagen na ontvangst. Ontvangstbevestiging is vanzelfsprekend niet mogelijk bij een anonieme melding.

- De meldingsbeheerder registreert de melding met de datum waarop deze ontvangen is en kent als enige de identiteit van de melder.

- De vertrouwelijkheid van de identiteit van de melder en van eventuele in de melding genoemde derden wordt steeds gewaarborgd.

- Niet-gemachtigde personeelsleden hebben geen toegang tot het register in het meldingskanaal.

3. *De meldingsbeheerder maakt een eerste beoordeling en wint eventueel bijkomende informatie in bij de melder*

- De meldingsbeheerder staat in voor een zorgvuldige opvolging van elke melding. In eerste instantie wordt de betrouwbaarheid en de bevoegdheid nagegaan.

- Het is mogelijk dat uit het voorafgaand onderzoek blijkt dat je melding geen (mogelijke) inbreuk op het Europees Unierecht of nationaal recht is, maar een bezorgdheid of incident waarvoor andere kanalen bestaan binnen VOT. De meldingsbeheerder kan je dan voorstellen om het juiste traject en kanaal te gebruiken. Je bent niet verplicht dit voorstel te aanvaarden.

- Indien er onduidelijkheden zijn in de initiële melding vraagt de meldingsbeheerder toelichting.

- Indien de meldingsbeheerder meent dat er grondige redenen zijn om aan te nemen dat het niet mogelijk is om de melding op een onafhankelijke wijze te kunnen behandelen, brengt hij/zij de melder (indien mogelijk) hiervan op de hoogte zodanig dat de melding naar keuze van de melder kan doorgestuurd worden naar een externe behandelaar.

4. *De meldingsbeheerder doet verder onderzoek en bepaalt de vervolgacties*

- De meldingsbeheerder doet verder onderzoek naar de vermeende onregelmatigheden. De meldingsbeheerder is in die hoedanigheid gemachtigd om op onafhankelijke wijze een onderzoek binnen VOT te voeren. De meldingsbeheerder hoort de persoon of personen over wie gemeld werd dat zij betrokken zijn bij de gemelde onregelmatigheden. De meldingsbeheerder wint informatie in en raadpleegt bronnen die nodig zijn in het kader van dat onderzoek. De meldingsbeheerder probeert op deze wijze de vermeende onregelmatigheden die door de melder werden gesignaleerd, te verifiëren.

- Bij het informeren en rapporteren maakt de meldingsbeheerder noch de identiteit van de melder, noch de identiteit van eventuele in de melding genoemde derden kenbaar.

- De meldingsbeheerder kan beroep doen op Audit Vlaanderen bij vragen over de (verdere) aanpak van een onderzoek naar aanleiding van een melding via audit@vlaanderen.be of op het telefoonnummer 02/553.45.55.

5. *De meldingsbeheerder koppelt de genomen acties terug aan de melder*

- Zo spoedig mogelijk, en uiterlijk 3 maanden na de ontvangstbevestiging van de melding, verstrekt de meldingsbeheerder feedback aan de melder. Deze termijn kan 1 maal verlengd worden met maximaal 3 maanden.
  Feedback is vanzelfsprekend niet mogelijk bij een anonieme melding.

- De feedback houdt in dat de melder informatie krijgt over de al dan niet genomen maatregelen, procesverbeteringen of –wijzigingen en/of andere verdere stappen. Deze feedback bevat geen details over specifieke personen en kan dan ook eerder van algemene aard zijn.

- Indien bijkomend onderzoek nodig of aangewezen, zal VOT waken over de vertrouwelijkheid van de onderzoeksdaden en over de naleving van de rechten van derden.

- Indien het niet mogelijk is om de melder enige feedback te geven, dan krijgt de melder daar bericht van, evenals van de reden waarom er nog geen informatie voorhanden is.

3.1.2 Waarborgen

1. *Geheimhouding en vertrouwelijkheid*

- De melding en behandeling van een melding verloopt met naleving van geheimhouding en vertrouwelijkheid.

- De identiteit van de melder wordt in geen geval zonder diens vrije en uitdrukkelijke toestemming bekendgemaakt aan anderen dan de gemachtigde personeelsleden die bevoegd zijn voor de ontvangst of de opvolging van meldingen. Dit geldt ook voor alle andere informatie waaruit de identiteit van de melder direct of indirect kan worden afgeleid. Van dit principe kan enkel afgeweken worden indien het gaat om een noodzakelijke en evenredige verplichting krachtens bijzondere wetgeving in het kader van onderzoek door nationale autoriteiten of gerechtelijke procedures, mede ter waarborging van de rechten van verdediging van de betrokkene. In dit geval worden de melders, voordat hun identiteit wordt bekendgemaakt, daarvan in kennis gesteld, tenzij die informatie de gerelateerde onderzoeken of gerechtelijke procedures in gevaar zou brengen.

- Aan de melder wordt het engagement gevraagd om vertrouwelijk om te gaan met zijn melding en deze noch rechtstreeks, noch via derden, openbaar te maken totdat VOT de beëindiging van het onderzoek heeft meegedeeld.

2. *Registratie*

- De meldingsbeheerder houdt een register bij van elke ontvangen melding, in overeenstemming met de bedoelde geheimhoudingsvereisten.

- Meldingen worden bijgehouden gedurende 2 jaar.

- Indien een persoon verzoekt om een onderhoud met de meldingsbeheerder om een interne melding te doen, zorgt VOT ervoor, mits de melder hiermee instemt, dat er een volledig en nauwkeurig verslag van het onderhoud wordt bijgehouden in een duurzame en opvraagbare vorm. VOT behoudt tevens zich het recht om de mondelinge melding te registreren door het maken van een opname van het gesprek in een duurzame en opvraagbare vorm, mits akkoord van de melder om de melding op deze wijze te registreren.

3. *Recht op bescherming van de persoonlijke levenssfeer*

- Elke verwerking van persoonsgegevens in het kader van een melding, met inbegrip van de uitwisseling of doorgifte van persoonsgegevens door de bevoegde autoriteiten, gebeurt overeenkomstig de Algemene Verordening Gegevensbescherming (GDPR) (Verordening (EU) 2016/679) en de wettelijke bepalingen inzake de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens. Persoonsgegevens die duidelijk niet relevant zijn voor de behandeling van een specifieke melding, worden niet verzameld, of worden, indien onbedoeld verzameld, onmiddellijk gewist.

- De naam, de functie en de contactgegevens zowel van de melder en elke persoon tot wie de beschermingsmaatregelen zich uitstrekken, als van de betrokkene, worden bijgehouden tot wanneer de gemelde inbreuk is verjaard.

- Deze betrokken personen kunnen zich elk beroepen op het recht van inzage en verbetering van de op zijn persoon betrekking hebben de verwerkte gegevens overeenkomstig de Algemene Verordening Gegevensbescherming (GDPR). Zij kunnen zich daarvoor ook richten tot de Gegevensbeschermingsautoriteit.

3.2 Extern kanaal

Melders kunnen ook gebruikmaken van een extern kanaal dat door de overheid wordt opgezet. Een klacht indienen kan dan bij de Federale Ombudsman en de sectorale instanties, waaronder deze federale autoriteiten (niet-limitatieve lijst):

- Overheidsopdrachten: de 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.

3.3 Pers of andere vormen van openbaarmaking

Naast de mogelijkheid om een melding te maken via het interne meldingskanaal of het externe meldingskanaal, heeft ieder persoon de mogelijkheid om de informatie met betrekking tot een inbreuk openbaar te maken.

Een melder die een openbaarmaking doet, komt in aanmerking voor de vermelde bescherming krachtens deze policy indien:

- de melder eerst een interne en/ of externe melding, maar er (naar aanleiding van die melding) geen passende maatregelen genomen zijn binnen een redelijke termijn;
  of
- de medewerker heeft gegronde redenen om aan te nemen dat:
  - de inbreuk een dreigend of reëel gevaar kan zijn voor het algemeen belang;
    of
  - er in geval van interne/ externe melding een risico op represailles bestaat, of het niet waarschijnlijk is dat de inbreuk doeltreffend wordt verholpen, wegens de bijzondere omstandigheden van de zaak, omdat bijvoorbeeld bewijsmateriaal kan worden achtergehouden of vernietigd, of een autoriteit kan samenspannen met de pleger van de inbreuk of bij de inbreuk betrokken is.

4 BESCHERMING VAN DE MELDER

4.1 Voorwaarden

Elke melder geniet de bescherming tegen repressailles indien

- zij intern of extern informatie meldden, of informatie openbaar maakten overeenkomstig de procedure in deze policy;
- de melder een gegronde reden had om aan te nemen dat de gemelde informatie over inbreuken op het moment van de melding juist was.

De melder geniet enkel bescherming indien de melding te goeder trouw is gedaan en de meldingsprocedure gevolgd werd. Er is geen bescherming bij opzettelijk of bewust onjuiste of misleidende meldingen.

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. Anonieme melders die later toch geïdentificeerd zouden worden genieten dezelfde bescherming.

4.2 Beschermingsmaatregelen tegen represailles

Indien de melder, facilitator of derde die verbonden is met de melder aan bovenvermelde voorwaarden voldoet, geniet hij bescherming tegen elke vorm van represailles, waaronder dreigingen met en pogingen tot represailles.

Onder represailles worden volgende maatregelen begrepen:

- schorsing, ontslag of soortgelijke maatregelen;
- degradatie of het onthouden van bevordering;
- overdracht van taken, verandering van locatie van de arbeidsplaats of verandering van de werktijden;
- het onthouden van opleiding;
- een negatieve evaluatie of arbeidsreferentie;
- het opleggen of toepassen van een disciplinaire maatregel, berisping of een andere sanctie, zoals een financiële sanctie;
- dwang, intimidatie, pesterijen en uitsluiting;
- niet-omzetting van een tijdelijk contract in een contract voor onbepaalde duur, als het personeelslid de gerechtvaardigde verwachting had dat hem een contract van onbepaalde duur zou worden aangeboden;
- niet-verlenging of vroegtijdige beëindiging van een tijdelijke arbeidsovereenkomst;
- schade, met inbegrip van reputatieschade op sociale media of financieel nadeel, met inbegrip van omzetderving en inkomstenderving;
- opname op een zwarte lijst op basis van een informele of formele overeenkomst voor de hele overheidsinstantie, waardoor de melder geen baan meer kan vinden bij die overheidsinstantie;
- vroegtijdige beëindiging of opzegging van een contract voor de levering van goederen of diensten;
- intrekking van een licentie of vergunning, afgeleverd door een overheidsinstantie;
- psychiatrische of medische verwijzingen;
- elke andere directe of indirecte handeling of nalatigheid dan de handelingen, vermeld in bovenstaande punten, die tot een ongerechtvaardigde benadeling van de melder leidt of kan leiden.

Tegen personen die informatie over inbreuken melden of een openbaarmaking doen overeenkomstig deze policy kunnen geen burgerrechtelijke, strafrechtelijke of tuchtrechtelijke vorderingen worden ingesteld, noch professionele sancties worden uitgesproken omwille van deze melding of openbaarmaking.

Melders kunnen 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 die toegang op zichzelf een strafbaar feit vormde.

Elke beschermde persoon die meent slachtoffer te zijn van of bedreigd te worden met een represaille, kan een gerechtelijke of administratiefrechtelijke procedure opstarten. Hierbij dient de melder aan te tonen dat er een melding of openbaarmaking werd gemaakt in overeenstemming met deze policy alsook dat zij geconfronteerd zijn met met een benadeling. VOT dient aan te tonen dat de genomen maatregel op andere motieven beslist werd dan de melding van de integriteitsschending.

5 SANCTIES

- Elke werknemer die de regels van deze policy overtreedt, kan gesanctioneerd worden met een van de sancties bepaald door het arbeidsreglement.

- De werknemer die opzettelijk een manifeste ongegronde melding heeft gedaan, en aldus op onrechtmatige wijze gebruik heeft gemaakt van de meldingsprocedure van deze klokkenluiderregeling, kan eveneens gesanctioneerd worden met een van de sancties bepaald door het arbeidsreglement.

- Personen die met VOT verbonden zijn en niet de hoedanigheid van werknemer van VOT hebben, en die de verplichtingen opgenomen in deze klokkenluiderregeling overtreden, kunnen door VOT gesanctioneerd worden met een disciplinaire sanctie.

- Daarnaast kunnen melders gestraft worden overeenkomstig de artikelen 443 tot 450 van het Strafwetboek wanneer wordt vastgesteld dat zij opzettelijk valse informatie hebben gemeld of openbaar hebben gemaakt. Personen die schade lijden als gevolg van dergelijke meldingen of openbaarmakingen hebben recht op schadevergoedingsmaatregelen overeenkomstig de contractuele of buitencontractuele aansprakelijkheid.