

## KLOKKENLUIDERSPOLICY

De 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, is een omzetting van de Europese Klokkenluidersrichtlijn 2019/1937. De wet biedt bescherming aan iedere persoon die informatie over een ernstig probleem met betrekking tot mogelijke onregelmatigheden of wangedrag bij een private onderneming heeft verkregen in een werkgerelateerde context en hieromtrent een melding wil doen.

Deze klokkenluiderspolicy heeft als doel om aan medewerkers(\*) van Vasco Group NV/Vasco BVBA en derde partijen transparantie te bieden over de bestaande kanalen om dergelijke (vermeende) onregelmatigheden binnen Vasco Group NV/Vasco BVBA te melden zonder dat zij hierbij de normale hiërarchische weg hoeven te volgen.

(\*) Dient onder medewerker te worden verstaan: de Vasco Group NV/Vasco BVBA werknemer, medewerker en ingeschakelde zelfstandige dienstverlener.

Op deze manier wenst Vasco Group NV/Vasco BVBA op te treden tegen eventuele onwettelijke, bedrieglijke of andere niet toegelaten praktijken of handelingen die onder de controle van de onderneming vallen, een onafhankelijk en vertrouwelijk onderzoek te waarborgen en eventuele belangenconflicten te vermijden. Deze policy impliceert echter geen meldingsplicht, maar een mogelijkheid voor medewerkers van Vasco Group NV/Vasco BVBA en derden om met toepassing van bepaalde waarborgen melding te doen van onregelmatigheden binnen de onderneming.

Voor de toepassing van deze policy gelden de volgende definities:

**Inbreuk :** handelingen of nalatigheden die :

- onrechtmatig zijn en betrekking hebben op de domeinen opgesomd onder artikel 3 “Toepassingsgebied”, of
- die ingaan tegen het doel of de toepassing van de regelgeving die binnen de in artikel 3 opgesomde toepassingsgebieden vallen.

**Informatie over inbreuk:** 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.

**Melder :** een natuurlijke persoon die in de context van zijn werkgerelateerde activiteiten informatie over inbreuken mondeling of schriftelijk meldt of openbaar maakt. Een werkgerelateerde activiteit of context betreft de 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.

De melder kan een (toekomstige) werknemer, ex-werknemer, zelfstandige dienstverlener, vrijwilliger, (on)bezoldigde stagiair, (werknemer bij een) klant, leverancier of (onder-)aannemer, aandeelhouder of een persoon die behoort tot het bestuurlijk, leidinggevend of toezichthoudend orgaan van een onderneming zijn die in een professionele context informatie heeft bekomen over een mogelijke inbreuk die hij/zij wenst te melden.

**Facilitator :** een natuurlijk persoon die een melder bijstaat in het meldingsproces en wiens bijstand vertrouwelijk moet zijn.

**Betrokkene :** een natuurlijke persoon (vb. een collega) of rechtspersoon (vb. een firma) 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.

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

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

## **Toepassingsgebied**

In het kader van deze regeling wordt een onderscheid gemaakt tussen enerzijds sociale integriteit en anderzijds zakelijke integriteit.

Het vertrouwenswerk op het gebied van *sociale* integriteit heeft betrekking op ongewenste omgangsvormen zoals onder meer pesten, discriminatie op basis van geslacht, leeftijd, beperking, geaardheid, seksuele leven, raciale of etnische afkomst, godsdienstige of levensbeschouwelijke overtuiging, ongewenst seksueel gedrag, geweld, ... Dit vraagt een andere benadering. Ondanks dat Vasco Group NV/Vasco BVBA ongewenste omgangsvormen beschouwt als niet-integer gedrag, vallen zij echter niet onder het specifieke toepassingsgebied van de klokkenluiderswetgeving.

De schending van *zakelijke* integriteit, zoals hierna verder gepreciseerd, daarentegen betreft onder andere de manier van omgaan met vertrouwelijke informatie, met materieel en goederen, veiligheid en gezondheid en de invulling die wordt gegeven aan de contacten met (potentiële) klanten en leveranciers. Het betreft

eveneens integriteitschendingen met betrekking tot boekhoudkundige, financiële, bancaire, audit-, omkoop- en mededingings-aangelegenheden.

Het verschil tussen beiden is dat bij *sociale* ongewenste omgangsvormen er vaak sprake is van een direct aanwijsbare klager en beklagde, tussen wie de ongewenste omgangsvormen zich voordoen, terwijl *zakelijke* integriteitskwesaties kunnen worden gesignaleerd en besproken zonder dat de melder (bv. als slachtoffer) hierbij rechtstreeks betrokken hoeft te zijn. In de praktijk is de scheiding tussen sociale en zakelijke integriteit niet altijd duidelijk aan te geven. Als richtlijn kan gelden dat ongewenste omgangsvormen zich in eerste instantie richten tegen een individu en dat andere integriteitschendingen zich veeleer richten tegen (de belangen van) de eigen organisatie, externe organisaties of de samenleving als geheel.

De *zakelijke* integriteitschendingen betreffen de volgende domeinen van het Europees en Belgisch recht:

- 1) overheidsopdrachten
- 2) financiële diensten, producten en markten, en voorkoming van witwassen van geld en terrorismefinanciering
- 3) productveiligheid en productconformiteit
- 4) veiligheid van het vervoer
- 5) bescherming van het milieu
- 6) stralingsbescherming en nucleaire veiligheid
- 7) veiligheid van levensmiddelen en diervoeders, diergezondheid, dierenwelzijn
- 8) volksgezondheid
- 9) consumentenbescherming
- 10) bescherming van de persoonlijke levenssfeer en persoonsgegevens, en beveiliging van netwerk- en informatiesystemen
- 11) bestrijding van belastingfraude
- 12) sociale fraudebestrijding
- 13) de financiële belangen van de Europese Unie
- 14) de Europese interne markt.

Het wangedrag kan reeds hebben plaatsgevonden, vindt momenteel plaats, of zal zich in de toekomst zeer waarschijnlijk voordoen.

Het zijn deze meldingen die volgens de hieronder beschreven procedure dienen te gebeuren om van de wettelijke bescherming tegen represailles te genieten.

## **Indienen melding en vervolgstappen**

### ***Keuze van het meest geschikte meldingskanaal***

Een melder heeft verschillende methodes ter beschikking om een inbreuk te melden. Sociale en interpersoonlijke integriteitsschendingen kunnen best gemeld worden via de eerste drie opgesomde kanalen. Inbreuken die onder het toepassingsgebied van de klokkenluidersregeling vallen, kan de melder best melden via één van de onderstaande methodes. Methodes 4, 5, en 6 zijn specifiek voorzien voor zakelijke integriteitsschendingen in het kader van de klokkenluidersregeling en kunnen enkel in die context worden gebruikt.

1. Een melding van een (vermeende) inbreuk kan in eerste instantie best bij de leidinggevende worden gedaan.
2. Indien de omstandigheden dit niet mogelijk maken of indien de leidinggevende onvoldoende gehoor geeft aan de melding, kan de melder een (vermeende) inbreuk melden aan de lokale vertrouwenspersoon.
3. De melder heeft ook steeds het recht om zijn werknemersvertegenwoordigers of vakbonden te raadplegen en zij zullen beschermd blijven tegen ongerechtvaardigde benadelende maatregelen als gevolg van deze raadplegingen.
4. Indien de melder van oordeel is dat hij/zij zich om de één of andere reden toch niet kan wenden tot deze personen, kan hij/zij een interne melding doen. Een interne melding is een melding van een inbreuk binnen Vasco Group NV/Vasco BVBA door mondeling of schriftelijk informatie over inbreuken te verstrekken via het intern meldingskanaal waarvan de procedure onder titel "*b. indienen van een melding via het intern meldingskanaal*" nader is omschreven.
5. Nadat de melder gebruik heeft gemaakt van het intern meldingskanaal of in het uitzonderlijke geval dat de melder van mening zou zijn dat hij/zij geen beroep kan doen op het intern meldingskanaal ondanks de garanties voorgeschreven in dit beleid (zoals vertrouwelijkheid, bescherming tegen represailles, en dergelijke meer) kan hij/zij een externe melding doen, hetzij mondelinge, hetzij schriftelijke via het extern meldpunt georganiseerd door de Overheid zoals verder toegelicht onder titel "*c. Indienen van een melding via het extern meldingskanaal van de overheid*".
6. Een publieke melding of openbaarmaking van informatie over inbreuken is mogelijk indien aan de strikte voorwaarden is voldaan zoals opgenomen onder titel "*d. Openbaarmaking van een inbreuk in uitzonderlijke omstandigheden*".

### ***Indienen van een melding via het intern meldingskanaal***

De melder heeft de mogelijkheid om een anonieme melding in te dienen. Een anonieme melding kan wel enkele nadelen met zich meebrengen :

- de opvolging van de melding is minder evident omdat bijkomende communicatie moeilijker is met anonieme melders;
- het is voor de onderneming moeilijker om een anonieme melder te beschermen tegen mogelijke of eerder subtiele represailles.

Het indienen van een melding gebeurt via:

[app.iflag.be/vasco](http://app.iflag.be/vasco)

Een melding bevat ten minste:

- De naam, de functie en contactgegevens van de melder indien hij geen anonieme melding wenst te doen;
- De datum van de melding;
- Een gedetailleerde omschrijving van de (vermeende) inbreuk, zoals
  - een beschrijving van de (vermeende) inbreuk;
  - eventueel met bijlagen (documentatie of bewijsstukken);
  - de identificatie van de mogelijke betrokkene(n) of departementen van de onderneming;
  - waar de inbreuk zich heeft voorgedaan;
  - wanneer de inbreuk zich heeft afgespeeld;
  - hoe en wanneer de melder de inbreuk hebt opgemerkt of op de hoogte werd gesteld;
  - wat uw relatie is met de onderneming (werknemer, freelancer, leverancier, aandeelhouder, ...) voor zover de melder geen anonieme melding doet;
  - de impact van het incident (voor de onderneming, voor het algemeen belang, ...)
  - en alle andere relevante informatie aangaande de (vermeende) inbreuk

Vasco Group NV/Vasco BVBA heeft een meldingsbeheerder aangewezen die de meest geschikte persoon of departement is binnen de organisatie om op vertrouwelijke en onafhankelijke wijze de meldingen te beheren zonder gevaar voor belangenconflicten. De meldingsbeheerder is:

Chantal Belien, HR Manager

## **Ontvankelijkheid en vooronderzoek**

- a) De meldingsbeheerder bevestigt aan de melder in alle gevallen de ontvangst van de schriftelijk ingediende melding binnen de zeven (7) dagen.
  - De meldingsbeheerder zal in eerste instantie nagaan of de melding ontvankelijk is en zal daarbij een eerste beoordeling maken. Deze beoordeling heeft in eerste instantie tot doel een inschatting te maken van de aard, de betrouwbaarheid en de accuraatheid van de aangeleverde informatie.
  - In functie van deze beoordeling kan de meldingsbeheerder beslissen of de melding onontvankelijk is en dan dient hij de melder schriftelijk op de hoogte te stellen van de reden van afwijzing, of dat hij een verder vooronderzoek zal voeren.
- b) Indien een vooronderzoek wordt opgestart en de meldingsbeheerder van oordeel is dat verder onderzoek zich opdringt, zal na afloop en met akkoord van de melder een geanonimiseerd advies worden overgemaakt aan Peter Ketelslegers, Bestuurder.

In dit advies worden de redenen voor verder onderzoek uiteengezet en wordt een aanzet tot plan van aanpak opgenomen.
- c) Indien uit het vooronderzoek blijkt dat er sprake is van een opzettelijk valse melding, zal het dossier voor verder gevolg worden overgemaakt aan de personeelsdienst van Vasco Group NV/Vasco BVBA.

## **Onderzoek**

- a) De Meldingsbeheerder zal op basis van voormeld advies beslissen of en met welke onderzoekscommissie het onderzoek dient te worden uitgevoerd: de meldingsbeheerder, aangevuld met interne, dan wel externe experts, ofwel een externe partij desgevallend aangevuld met interne (staf)medewerker(s).
- b) De melder zal eveneens schriftelijk op de hoogte worden gebracht van het feit dat een grondig onderzoek wordt opgestart.
- c) De onderzoekscommissie zal het onderzoek uitvoeren binnen een redelijke termijn. Als algemene regel geldt een termijn van hoogstens drie maanden na de ontvangstbevestiging te hebben verstuurd naar de melder. Binnen deze termijn zal de melder ook feedback krijgen over de opvolging, de geplande of genomen maatregelen en over de redenen voor die opvolging.
- d) De melder ontvangt gedurende het onderzoek en dus ook na de eerste termijn van drie maanden algemene informatie over de voortgang van het onderzoek en de uitkomst, tenzij de melder dit niet wenst of dit nadelig is voor de melder of voor het onderzoek, of tenzij er andere gegronde redenen zijn om de melder niet te informeren.

## **Eindrapportering**

De eindrapportering omvat de volgende stappen :

- a) De meldingsbeheerder of onderzoekscommissie rapporteert haar bevindingen schriftelijk aan Peter Ketelslegers, Bestuurder en deze beslist welk gevolg er dient aan te worden gegeven.

- b) De meldingsbeheerder stelt de melder op de hoogte dat de bevindingen van de onderzoekscommissie aan Peter Ketelslegers, Bestuurder heeft gestuurd.
- c) In het eindrapport wordt de identiteit van de melder afgeschermd, tenzij deze zijn schriftelijke toestemming heeft gegeven om zijn identiteit vrij te geven. De identiteit van de betrokkene(n) wordt enkel opgenomen indien het onderzoek van de melding geleid heeft tot aantoonbare feiten.
- d) Indien Peter Ketelslegers, Bestuurder van oordeel is dat er sanctionerend dient te worden opgetreden, zal hij de bevoegde persoon van het management een kopij bezorgen van het eindrapport.

### **Indienen van een melding via het extern meldingskanaal van de overheid**

Na eerst een melding te hebben gedaan via een intern meldingskanaal, kan de (anonieme) melder een inbreuk melden via een extern meldingskanaal van de overheid indien er geen gepaste maatregelen zijn genomen via de interne procedure. De melder kan ook meteen een melding via het externe meldingskanaal van de overheid doen.

Het externe meldingskanaal biedt de mogelijkheid om schriftelijk en mondelinge meldingen te doen bij de Federale Ombudsman. Een mondelinge melding is mogelijk via de telefoon of via andere spraakberichtsysteem en, op verzoek van de melder, door middel van een fysieke ontmoeting binnen een redelijke termijn. De volgende webpagina van de Federale ombudsman bevat meer informatie over de meldingen bij dit extern meldkanaal : <https://www.federaalombudsman.be/nl/centrum-integriteit/welke-meldingen>. Het extern meldingskanaal van de overheid is bereikbaar via de federale ombudsman per:

- e-mail (ook om een afspraak te maken) : [integriteit@federaalombudsman.be](mailto:integriteit@federaalombudsman.be)
- telefoon (ook om een afspraak te maken) : 02/289.27.04
- online meldingsformulier : <https://www.federaalombudsman.be/nl/meldingsformulier>

Het onafhankelijk extern meldingskanaal van de Federale Ombudsman zal binnen de zeven (7) dagen een ontvangstbevestiging versturen, tenzij :

- De melder uitdrukkelijk aangeeft dit niet te willen
- De ontvangstbevestiging een gevaar kan zijn voor de bescherming van de identiteit van de melder.

Het extern meldingskanaal zal binnen de drie maanden of, in bijzondere gevallen, zes maanden feedback geven aan de melder over de geplande opvolging of genomen maatregelen en over de redenen voor die opvolging, tenzij een wettelijke bepaling dit verhindert. Het extern meldingskanaal zal de melder in kennis stellen van het eindresultaat van de onderzoeken.

De bevoegde autoriteiten kunnen besluiten dat een gemelde inbreuk duidelijk van geringe betekenis is of reeds het voorwerp was van eerdere meldingen over dezelfde feiten zonder bijkomende nieuwe elementen met als gevolg dat zij de procedure afronden. De bevoegde autoriteiten informeren de melder van hun beslissing en van de motivering daarvan.

## **Openbaarmaking van een inbreuk in uitzonderlijke omstandigheden**

Een (anonieme) melder die een inbreuk openbaar maakt door informatie over inbreuken publiek toegankelijk te maken (vb. via de media), komt in aanmerking voor bescherming indien aan de volgende voorwaarden is voldaan :

7. De melder heeft eerst een interne of externe melding gedaan zoals voorgeschreven onder titels b) of c) maar er zijn geen passende maatregelen genomen; of,
8. De melder heeft gegronde redenen om aan te nemen dat:
  - de inbreuk een dreigend of reëel gevaar kan zijn voor het algemeen belang; of
  - in geval van 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.

## **Waarborgen voor de positie van de melder**

### ***Beschermingsvoorwaarden***

Melders krijgen bescherming indien :

- Zij gegronde redenen hebben om aan te nemen dat de gemelde informatie over inbreuken op het moment van de melding juist was en dat die informatie binnen het toepassingsgebied van dit beleid valt. De melder verliest het voordeel van de bescherming niet op de enkele grond dat de te goeder trouw gedane melding onjuist of ongegrond is bevonden; en
- Zij de informatie melden via het intern of extern meldingskanaal. De melder krijgt ook bescherming indien hij de inbreuk openbaar maakt voor zover hij eerst een interne of externe melding heeft gedaan.

Anonieme melders die informatie over inbreuken hebben gemeld of openbaar gemaakt, maar later zijn geïdentificeerd en onderhevig zijn aan represailles, komen in aanmerking voor bescherming indien ze beantwoorden aan deze beschermingsvoorwaarden.

De volgende personen en juridische entiteiten krijgen bescherming indien ze gegronde redenen hebben om aan te nemen dat de melder onder de beschermingsvoorwaarde valt:

- Facilitators;
- Derden die verbonden zijn met de melders en die het slachtoffer kunnen worden van represailles in een werkgerelateerde context, zoals collega's of familieleden van de melders;
- Juridische entiteiten die eigendom zijn van de melders, waarvoor de melders werken of waarmee de melders anderszins in een werkgerelateerde context verbonden zijn.



## **Geheimhouding**

De meldingsbeheerder, hieronder begrepen de gemachtigde personeelsleden die bevoegd zijn voor de ontvangst en opvolging van de meldingen, houdt de identiteit van de melder geheim. De meldingenbeheerder is tevens aangeduid omwille van de kwaliteiten van de vertrouwelijke behandeling van de zaak en van de identiteit van de melder, en dienst onafhankelijkheid om belangenconflicten te vermijden. Meer in het bijzonder geldt tijdens de behandeling een verbod tot mededeling van de identiteit – of elementen die het mogelijk maken de identiteit te achterhalen – van de melder. De verplichting tot geheimhouding geldt ook indien een anonieme melder door andere informatie alsnog direct of indirect identificeerbaar is.

De meldingenbeheerder kan identiteit van de melder enkel bekend maken:

- indien de melder daar de vrije en uitdrukkelijke (schriftelijke) toestemming voor geeft; of
- indien de melder zelf de geheimhouding opzettelijk verbreekt.

De geheimhouding van de identiteit zal niet gelden indien dwingende wetgeving tot bekendmaking verplicht is in het kader van onderzoek door nationale autoriteiten of gerechtelijke procedures. De bevoegde autoriteit zal de melders voorafgaandelijk informeren over de redenen van de bekendmaking tenzij dit de onderzoeken of gerechtelijke procedures in gevaar zou brengen.

Iedereen die rechtstreeks of onrechtstreeks betrokken is bij de behandeling van een melding van een (vermoedelijke) inbreuk is verplicht tot geheimhouding over alles wat hem/haar in verband daarmee (zoals de melding, het vooronderzoek en het onderzoek zelf) is toevertrouwd of bekend geworden tegenover iedereen die niet bevoegd is tot kennisname en voor zover die verplichtingen uit de aard van de zaak volgt.

Het intern meldingskanaal voor de ontvangst van meldingen is zodanig opgesteld door ontwerp, opzet en beheer om op beveiligde wijze de vertrouwelijkheid van de identiteit van de melder en van eventuele in de melding genoemde derden te beschermen en waartoe niet-gemachtigde personeelsleden geen toegang hebben.

## **Voorkomen van represailles, zoals sancties of oneerlijke behandeling**

Een represaille is een directe of indirecte handeling of nalatigheid die in een werkgerelateerde context plaatsvindt ten nadele van een melder naar aanleiding van een interne of externe melding of openbaarmaking, en die tot ongerechtvaardigde benadeling van de melder leidt of kan leiden. Elke vorm van represailles waaronder dreigingen met en pogingen tot represailles, is verboden en betreffen met name :

1. schorsing, tijdelijke buitendienststelling, ontslag of soortgelijke maatregelen;
2. degradatie of weigering van bevordering;
3. overdracht van taken, verandering van locatie van de arbeidsplaats, loonsverlaging, verandering van de werktijden;
4. het onthouden van opleiding;
5. negatieve prestatiebeoordeling of arbeidsreferentie;

6. het opleggen of toepassen van een disciplinaire maatregel, berisping of andere sanctie, zoals een financiële sanctie;
7. dwang, intimidatie, pesterijen of uitsluiting;
8. discriminatie, nadelige of ongelijke behandeling;
9. niet-omzetting van een tijdelijke arbeidsovereenkomst in een arbeidsovereenkomst voor onbepaalde tijd, in het geval de werknemer de gerechtvaardigde verwachting had dat hem een dienstverband voor onbepaalde tijd zou worden aangeboden;
10. niet-verlenging of vervroegde beëindiging van een tijdelijke arbeidsovereenkomst;
11. schade, met inbegrip van reputatieschade, met name op sociale media, of financieel nadeel, met inbegrip van omzetsderving en inkomstderving;
12. opname op een zwarte lijst op basis van een informele of formele overeenkomst voor een hele sector of bedrijfstak, waardoor de persoon geen baan meer kan vinden in de sector of de bedrijfstak;
13. vroegtijdige beëindiging of opzegging van een contract voor de levering van goederen of diensten;
14. intrekking van een licentie of vergunning;
15. psychiatrische of medische verwijzingen.

Melders die handelen overeenkomstig deze regeling kunnen hun melding doen zonder daarmee hun arbeidsrechtelijke positie in gevaar te brengen of enige andere nadelige gevolgen te moeten vrezen. Dit impliceert dat hij/zij op geen enkele wijze in zijn/haar positie wordt benadeeld als gevolg van deze vraag of melding, voor zover hij/zij te goeder trouw handelt.

Represailles tegen melders als gevolg van een oprechte melding worden beschouwd als een ernstige schending van deze meldingsregeling, in welk geval Vasco Group NV/Vasco BVBA passende acties zal ondernemen om de melder te beschermen en om diegenen die verantwoordelijk zijn voor de represailles te sanctioneren.

Medewerkers die menen naar aanleiding van een melding nadelige gevolgen te hebben ondervonden, moeten dit zo snel als mogelijk kenbaar maken aan de meldingsbehandelaar. Het slachtoffer van represailles kan ook een gemotiveerde klacht indienen bij de federale coördinator, die een buitengerechtelijke beschermingsprocedure zal opstarten indien hij een redelijk vermoeden van een represaille heeft vastgesteld. De federale coördinator die deze klacht zal opnemen, is de Federale Ombudsman van wie de contactgegevens onder artikel 4, 'c. *Indienen van een melding via het extern meldingskanaal van de overheid*' zijn opgenomen.

De federale coördinator verifieert bij Vasco Group NV/Vasco BVBA het bestaan van een redelijk vermoeden van een represaille. Vasco Group NV/Vasco BVBA reageert binnen de 20 dagen op het verzoek van de federale coördinator.

## **Misbruik van de meldingsregeling**

Vasco Group NV/Vasco BVBA gaat ervan uit dat melders hun melding van een inbreuk te goeder trouw zullen uiten. Als de meldingenbeheerder bij nader onderzoek geen bevestiging kan vinden voor bepaalde meldingen of indien deze niet gegrond blijken te zijn, zullen er geen maatregelen worden genomen tegen melders die te goeder trouw hun bekommernis hebben kenbaar gemaakt.

Vasco Group NV/Vasco BVBA kan evenwel niet toestaan dat melders opzettelijk meldingen indienen waarvan zij weten of geacht worden te weten dat deze onjuist zijn. Vasco Group NV/Vasco BVBA zal opzettelijk valse meldingen op gepaste wijze sanctioneren volgens de sancties voorgeschreven in het arbeidsreglement. De melder die te kwader trouw is kan aansprakelijk worden gesteld voor de schade die iemand lijdt ten gevolge van valse meldingen.

Melders die opzettelijk valse informatie hebben gemeld of openbaar hebben gemaakt, kunnen strafrechtelijk worden vervolgd wegens de aanranding van de eer of de goede naam van personen.

## **Verwerking persoonsgegevens en uw rechten**

Vasco Group NV/Vasco BVBA is de verwerkingsverantwoordelijke van de persoonsgegevens in uitvoering van deze meldingsregeling. Dit impliceert dat zowel de melder als de betrokkene bij Vasco Group NV/Vasco BVBA terecht kunnen om hun recht van informatie, inzage, verbetering, portabiliteit en verwijdering van gegevens uit te oefenen, rekening houdende met de volgende beperkingen:

- De betrokkene (voorwerp van de gemelde inbreuk) heeft geen recht op toegang tot de identiteit van de melder of die van derden (of van elementen die hun identificatie zouden kunnen mogelijk maken), tenzij met hun akkoord of in geval van een valse melding of lasterlijke aantijging door de melder of een valse getuigenis van een derde;
- De melder heeft evenmin recht op toegang tot de persoonsgegevens van de beklagde, noch tot deze van een derde, tenzij na onderzoek blijkt dat de beklagde onterecht de melder heeft verdacht (bv. stellen dat de melder zelf betrokken was bij wanpraktijken die hij heeft gemeld) of wanneer derden te kwader trouw handelen (vb. valse getuigenis).
- De persoonsgegevens van de betrokken partijen worden niet verwijderd zolang het intern en/of extern (politieel/gerechtelijk/administratief) onderzoek loopt.

Vasco Group NV/Vasco BVBA doet beroep op een derde partij, nl. iFlag gevestigd in Lasne, om de meldingsregeling te implementeren om zo de vertrouwelijkheid van de meldingen te garanderen en een efficiënte administratieve verwerking te verzekeren.

Uw persoonsgegevens zullen niet naar derde landen worden verstuurd die niet voorzien in een passend beschermingsniveau van uw persoonsgegevens.

Tijdens de meldingsprocedure zullen naast de feiten, ook de naam, de functie en contactgegevens van de melder en van de beklaagde worden verwerkt. Het verwerken van deze persoonsgegevens is noodzakelijk in het kader van de 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 (art. 6, §1, c) AVG). De doorgifte van een melding aan een verwerker (een dienstverlener zoals een cloudopslagprovider of tool om de meldingen te beheren) kan gebeuren op basis van de gerechtvaardigde belangen van Vasco Group NV/Vasco BVBA om deze gegevens efficiënt te verwerken met het oog op het beheer van de meldingen, de anonimiteit te waarborgen, het toegangsmanagement, enz. (art. 6, §1, f) AVG). Indien u een melding doet door middel van een stemopname, zal dit gebeuren op basis van uw toestemming (art. 6, §1, a) AVG).

U kan steeds terecht op het e-mailadres [whistleblowing@vasco.eu](mailto:whistleblowing@vasco.eu) wanneer u verdere vragen hebt betreffende de genomen waarborgen om uw persoonsgegevens te beschermen en betreffende de verwerking van uw persoonsgegevens in het kader van de meldingsregeling of om uw recht van toegang tot, de verbetering of overdraagbaarheid van gegevens of verwijdering van uw persoonsgegevens te vragen voor zover de uitoefening van de rechten valt binnen de wettelijke voorwaarden.

Indien u, na contact te hebben opgenomen met Vasco Group NV/Vasco BVBA, alsnog een klacht wil indienen met betrekking tot de verwerking van uw persoonsgegevens, kan u terecht bij de bevoegde toezichthoudende autoriteit, met name de Gegevensbeschermingsautoriteit.

De overheid die instaat voor het extern meldingskanaal handelt als verwerkingsverantwoordelijke. Dit betekent dat u bij externe meldingen, terecht kan bij de overheid voor de uitoefening van uw rechten.

De bevoegde autoriteiten en het Federaal Instituut voor de bescherming en de bevordering van de rechten van de mens (bereikbaar via deze [link](https://federaalinstituutmensenrechten.be/nl/contact) : <https://federaalinstituutmensenrechten.be/nl/contact> of via [info\[at\]firm-ifdh.be](mailto:info@firm-ifdh.be)) zullen u informeren en adviseren over ondersteuningsmaatregelen, zoals :

- informatie en adviezen over de beschikbare remedies en procedures die bescherming bieden tegen represailles, alsmede over de rechten van de betrokkene;
- technisch advies ten aanzien van autoriteiten die betrokken zijn bij de bescherming van de melder;
- rechtsbijstand en financiële bijstand in het kader van gerechtelijke procedures;
- technische, psychologische, mediagerelateerde en sociale ondersteuning

### **Bewaartermijn**

De persoonsgegevens verwerkt in het kader van de meldingsregeling worden niet langer dan noodzakelijk voor het intern en/of extern (politieel/gerechtelijk/administratief) onderzoek bewaard. In geval van politieele, administratieve, gerechtelijke of tuchtrechtelijke procedures, worden de gegevens na het verstrijken van de toepasselijke verjaringstermijn of beroepstermijn gearchiveerd of tot maximaal twee maanden erna bewaard.

## **Sancties**

De inbreuken zoals onder andere opgesomd in "*3. Toepassingsgebied*" van deze policy betreffende de meldingsregeling en vastgesteld in het eindresultaat volgend uit het onderzoek naar een klacht via deze meldingsregeling kunnen aanleiding geven tot sancties (o.a. waarschuwing, ontslag om dringende reden) zoals onder meer omschreven in het arbeidsreglement of de arbeidsovereenkomst.

Naast deze arbeidsrechtelijke sancties, kan de betrokkene of de melder te kwader trouw, afhankelijk van de aard van de inbreuk en de toepasselijke wetgeving, bijkomende sancties oplopen, zoals strafsancties en schadevergoedingen.

## **Medewerking management**

Ten behoeve van een goede inbedding van deze meldingsregeling zal het management de volgende activiteit ontplooiën:

- Ervoor zorgen dat deze regeling voorhanden is en bekend is bij alle medewerkers;
- Alle zaken rondom meldingen van integriteitschendingen zeer ernstig nemen, tijdig actie ondernemen en vertrouwelijkheid en zorgvuldigheid garanderen.

## **Overige bepalingen**

Deze regeling wordt binnen de twee jaar na inwerkingtreding geëvalueerd.

In de gevallen waarin de regeling niet voorziet, beslist Peter Ketelslegers, Bestuurder.