

Klokkenluidersprocedure voor Sofidel Benelux NV

0	02nd January 2024	<i>New emission</i>	Fabiana Da San Martino <i>Compliance Officer</i>	Elena Betti <i>Risk Management & Compliance Director</i>
Herz	Datum	Beschrijving	Bewerkt	Goedgekeurd

1. Doel

Het doel van deze procedure is het reglementeren van de principes en regels voor de behandeling van klokkenluiderszaken die Sofidel Benelux NV (hierna “**de Vennootschap**”) heeft besloten aan te nemen in overeenstemming met het Groepsbeleid en de Richtlijn (EU) 2019/1937 (hierna de “**Klokkenluidersrichtlijn**”) die in België in wet is omgezet door de federale overheid op 28 november 2022.

1.1. Verwijzingen naar normen

Deze procedure wordt vastgesteld in overeenstemming met de volgende wetgevingsbesluiten:

- Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 *betreffende de bescherming van natuurlijke personen die inbreuken op het recht van de Unie melden*;
- Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en houdende intrekking van Richtlijn 95/46/EG*;
- De Europese regelgeving werd door de federale overheid op 28 november 2022 in wet omgezet.

2. Procesfasen

2.1. Subjectief toepassingsgebied: de geadresseerden

De geadresseerden van deze procedure zijn potentiële klokkenluiders. In het bijzonder:

- Werknemers;
- Zelfstandigen;
- Leveranciers;
- Vrijwilligers en betaalde of onbetaalde stagiairs;
- Aandeelhouders en personen met een administratieve, leidinggevende, toezichthoudende of vertegenwoordigende functie, met inbegrip van niet bij het dagelijks bestuur betrokken leden van de raad van bestuur;
- Alle personen die werken onder toezicht en leiding van de natuurlijke of rechtspersoon met wie het contract is gesloten, diens onderaannemers en leveranciers;
- Klanten.

Het is niet noodzakelijk dat de melding of openbaarmaking plaatsvindt tijdens de arbeidsrelatie of een andere bestaande rechtsbetrekking. In feite kunnen ze ook gedaan worden:

- Voorafgaand aan de totstandkoming van het dienstverband of andere juridische relatie, indien de informatie over inbreuken werd verkregen tijdens het wervingsproces of in andere precontractuele stadia;
- Tijdens de proefperiode;

Na de beëindiging van het dienstverband of andere juridische relatie, indien de informatie over inbreuken werd verkregen vóór de beëindiging van deze relatie.

2.2. Het objectieve toepassingsgebied

2.2.1. Het object van de melding

Deze procedure betreft meldingen met betrekking tot:

- Inbreuken in de vorm van administratieve, boekhoudkundige, civiele of strafrechtelijke strafbare feiten;
- Schending van de Europese wetgeving, namelijk:
 - i. strafbare feiten die vallen binnen het toepassingsgebied van handelingen van de Europese Unie met betrekking tot de volgende gebieden, voor zover ze relevant zijn voor de Verenigde Staten: overheidsopdrachten, diensten, financiële producten en markten en preventie van witwassen en financiering van terrorisme, productveiligheid en -naleving, transportveiligheid, milieubescherming, volksgezondheid, consumentenbescherming, privacy en bescherming van persoonsgegevens, en netwerk- en informatiesysteembeveiliging;
 - ii. Handelingen of nalatigheden die de financiële belangen van de Europese Unie schaden

Hieronder volgt een illustratieve en niet-limitatieve lijst van inbreuken die de financiële belangen van de Europese Unie schaden, zoals uiteengezet in de desbetreffende Europese regelgeving:

Type inbreuk	Toelichting
Witwassen	De omzetting of overdracht van activa, uitgevoerd in de wetenschap dat deze afkomstig zijn van criminele activiteiten of van deelname aan dergelijke activiteiten, met als doel het verbergen of verhullen van de illegale oorsprong van dergelijke activa of om iemand die betrokken is bij een dergelijke activiteit te

Type inbreuk	Toelichting
	helpen de wettelijke gevolgen van hun daden te ontlopen.
Onrechtmatige toe-eigening van openbare middelen	<p>Het gebruiken of voorleggen van valse verklaringen of documenten om bijdragen of financieringen te verkrijgen die door de Europese instellingen worden toegekend of uitbetaald.</p> <p>Het weglaten van relevante informatie om bijdragen of financiering toegekend of uitbetaald te krijgen door de Europese instellingen.</p>
Actieve corruptie	<p>Het beloven of geven van geld aan ambtenaren, klanten of zakenpartners.</p> <p>Het beloven of geven van geschenken of giften aan ambtenaren, klanten of zakenpartners waarvan de totale waarde niet als gering kan worden gedefinieerd.</p>
Gedrag gericht op het ontduiken van belasting over de toegevoegde waarde	Facturen of andere documenten uitgeven voor transacties die zelfs gedeeltelijk niet bestaan om BTW te ontduiken.
Smokkelen	<p>Het onttrekken van goederen aan douanetoezicht.</p> <p>Het opgeven van valse of onjuiste gegevens om geen of minder douanerechten te betalen.</p>

- iii. Handelingen of nalatigheden met betrekking tot de interne markt, inclusief schendingen van de EU mededingings- en staatssteunregels, evenals schendingen met betrekking tot de interne markt die verband houden met handelingen die in strijd zijn met vennootschapsbelastingregels of mechanismen die tot doel hebben een belastingvoordeel te verkrijgen dat het doel of de strekking van de toepasselijke vennootschapsbelastingwetgeving tenietdoet.

Deze procedure voorziet in de mogelijkheid voor de melder om een anonieme melding te doen, op voorwaarde dat deze onderbouwd en voldoende gedocumenteerd is. Daarom zullen meldingen die algemeenheid, benaderingen of loutere klachten bevatten, niet worden behandeld.

De *Klokkenluiderswet* sluit van het toepassingsgebied van de procedure uit:

- a. Geschillen, vorderingen of verzoeken gerelateerd aan een persoonlijk belang van de melder of van de persoon die een klacht indient bij de gerechtelijke of boekhoudkundige autoriteiten die

- uitsluitend verband houden met zijn/haar individuele werk of openbare arbeidsrelatie, of inherent zijn aan zijn/haar werk of openbare arbeidsrelatie met hiërarchisch hogere personen;
- b. Inbreuken op de nationale veiligheid, evenals aanbestedingen met betrekking tot defensie of nationale veiligheidsaspecten, tenzij deze aspecten onder het afgeleide recht van de Europese Unie vallen;
- c. Communicaties van commerciële aard.

2.2.2. De inhoud van de melding

Meldingen moeten onderbouwd zijn, gebaseerd op nauwkeurige en overeenstemmende feiten, en zo compleet en uitgebreid mogelijk.

Waar mogelijk moet de melder het volgende verstrekken:

- Een duidelijke en volledige beschrijving van de feiten die het onderwerp zijn van de melding;
- Een indicatie van de omstandigheden van tijd en plaats waarin het feit dat onderwerp is van de melding zich heeft voorgedaan;
- De persoonlijke gegevens of andere elementen waarmee de betrokkene persoon of personen geïdentificeerd kunnen worden (bijv. de titel, de plaats van tewerkstelling waar de activiteit wordt uitgevoerd);
- Alle documentatie die de melding onderbouwt;
- Alle andere nuttige informatie om het bestaan van de gemelde feiten vast te stellen.

Het is niet relevant voor de verwerking van de melding en de bescherming tegen represailles om welke redenen de melder de melding of openbaarmaking heeft gedaan.

2.3. Meldingskanalen

2.3.1. Interne meldingskanalen

Meldingen kunnen zowel schriftelijk als mondeling worden gedaan via de hieronder vermelde kanalen:

- Een speciaal IT-platform dat toegankelijk is vanaf de website www.sofidel.com; <https://sofidelgroup.integrityline.com/> in de rubriek Sofidel Group/ Governance sectie, en dat voorziet in:
 - De mogelijkheid om een schriftelijke melding te doen door specifieke formulieren in te vullen;
 - De mogelijkheid om een mondelinge melding te doen met behulp van een gesproken berichtensysteem;

- Verzoek – via het speciale IT-platform – van de melder om een bijeenkomst met de meldingsbeheerder – die op verzoek van de melder ook bijgewoond mag worden door eventuele facilitators – die binnen tien werkdagen na de datum van ontvangst van het verzoek gehouden moet worden:
 - In bedrijfsgebouwen die de volledige geheimhouding van de melder garanderen;
 - Met toestemming van de melder, door middel van een videoconferentieverbinding die de uiterste geheimhouding van het gesprek garandeert en waaraan alleen de personen die daartoe gerechtigd zijn, mogen deelnemen.

Onder voorbehoud van toestemming van de melder wordt de melding die tijdens de bijeenkomst mondeling gedaan wordt, door de meldingsbeheerder vastgelegd middels een opname op een apparaat dat geschikt is om op te slaan en af te luisteren, of middels notulen die door de melder geverifieerd, gewijzigd en goedgekeurd kunnen worden middels zijn handtekening.

Als de interne melding wordt ingediend via een ander kanaal dan uitdrukkelijk vermeld, moet de ontvanger de melding onmiddellijk (en niet later dan zeven dagen na ontvangst) doorsturen naar de meldingsbeheerder en tegelijkertijd de melder op de hoogte stellen van de verzending. In dit geval kan anonimiteit niet altijd gegarandeerd worden.

2.3.2. Externe meldingskanalen

Onverminderd de voorkeur voor het interne meldingskanaal, mag de melder een externe melding doen, gericht aan de Federale Ombudsman, die een coördinerende rol heeft in de externe meldingskanalen, en deze alleen zal doorsturen naar de bevoegde autoriteit als aan een van de volgende voorwaarden is voldaan op het moment dat de externe melding wordt ingediend:

- a. Het interne meldingskanaal is niet voorzien binnen de werkcontext van de melder, oftewel dit kanaal is niet actief of, zelfs als het geactiveerd is, voldoet het niet aan de bepalingen van de *Klokkenluiderswet*;
- b. De melder heeft al een interne melding gedaan en daar is geen gevolg aan gegeven;
- c. De melder heeft gegronde redenen om aan te nemen dat, als hij of zij een interne melding zou doen, deze niet effectief zou worden opgevolgd, of dat dezelfde melding zou kunnen leiden tot het risico op represaille;
- d. De melder heeft redelijke gronden om aan te nemen dat de inbreuk een dreigend of duidelijk gevaar voor het openbaar belang kan vormen.

Daartoe heeft de Federale Ombudsman voorzien in de volgende kanalen:

- IT-platform voor het verzamelen en beheren van meldingen van onwettige handelingen en mededelingen over represaillemaatregelen, toegankelijk via de volgende link <https://www.meldpuntsocialefraude.belgie.be/nl/>

- Telefoonlijn of spraakberichtensysteem waarmee, na een ingesproken toelichting op de verwerking van persoonsgegevens en de informatie die nodig is om de volledige tekst van die toelichting te vinden, gesproken meldingen kunnen worden verkregen;
- Het Contactcenter is bereikbaar van **maandag tot vrijdag, van 7 uur tot 20 uur, op het nummer 02 511 51 51**. Buiten deze uren kunt u vragen om teruggebeld te worden. Een operator van het Contactcenter belt u dan de volgende werkdag op.

2.3.3. Openbaarmaking

Zonder afbreuk te doen aan de voorkeur voor het interne meldingskanaal en aan de mogelijkheid om, in de aanwezigheid van de hierboven vermelde voorwaarden, de externe meldingskanalen te gebruiken, kan de melder een openbare melding doen, gebruik makend van de bescherming voorzien door de *Klokkenluiderswet*, alleen als op het moment van de indiening ervan:

- de melder eerder een interne en externe melding heeft gedaan ofwel direct een externe melding heeft gedaan, bij aanwezigheid van de noodzakelijke voorwaarden, en binnen de in de *Klokkenluidersregeling* gestelde termijnen geen antwoord heeft ontvangen over de voorziene of genomen maatregelen naar aanleiding van de meldingen;
- de melder redelijke gronden heeft om aan te nemen dat de schending een acuut of duidelijk gevaar voor het openbaar belang kan vormen;
- de melder gegronde redenen heeft om aan te nemen dat de externe melding het risico van represaille met zich mee kan brengen of niet effectief kan worden opgevolgd vanwege de specifieke omstandigheden van het geval, zoals wanneer bewijsmateriaal verborgen of vernietigd kan worden, of wanneer er een gegronde angst is dat degene die de melding heeft ontvangen samenspannt met de overtreder of betrokken is bij de inbreuk.

2.4. Het beheer van de melding

De rol van de meldingsbeheerder die de melding ontvangt middels het meldingskanaal dat specifiek geïmplementeerd is door Sofidel Benelux NV is toegewezen aan de Human Resources Manager, die ontvangen interne meldingen vertrouwelijk behandelt, de melder en met hem/haar gelijkgestelde personen beschermt, evenals de eer en de identiteit van de melder.

Als de melding betrekking heeft op de meldingsbeheerder, kan de melder de melding doorsturen naar de *Klokkenluiderscommissie* die specifiek is opgericht binnen SO.FI.DEL. S.p.A. en die bestaat uit de *Human Resources Director*, de *Risk Management & Compliance Director*, de *Internal Audit Manager* voor de juiste evaluaties met betrekking tot de te nemen maatregelen.

Het beheerproces van de melding is onderverdeeld in de vijf stappen die hieronder worden beschreven, en elk van deze stappen moet adequaat worden gedocumenteerd:

- a. Voorafgaande beoordeling;
- b. Onderzoek;
- c. Besluit;
- d. Archivering van de documentatie;
- e. *Rapportage* en monitoring van corrigerende maatregelen.

De melder heeft de mogelijkheid om, via toegang tot het platform, op elk moment de voortgang van zijn melding te controleren, evenals het resultaat van de procedure (inclusief archivering).

a) Voorafgaande beoordeling

De meldingsbeheerder behandelt meldingen vertrouwelijk en past de gepaste procedures toe om zowel de melder als de identiteit en eer van de betrokkene en van alle andere betrokken personen te beschermen.

De meldingsbeheerder voert een voorafgaande beoordeling van de melding uit en zorgt ervoor dat deze op de juiste manier wordt behandeld, en in het bijzonder:

- Dat er binnen zeven dagen na de datum van ontvangst van de melding een ontvangstbevestiging van de melding aan de melder wordt gestuurd, via het daarvoor bestemde IT-platform;
- Controleert of de melding voldoende gedetailleerd is om beoordeeld te kunnen worden, neemt contact op met de melder als er aanvullingen nodig zijn, en stelt ook vast of de melding binnen het toepassingsgebied van de *Klokkenluidersregelgeving* valt;
- Archiveert de meldingen en stelt de melder op de hoogte en formaliseert schriftelijk de redenen voor de beslissing om de meldingen te archiveren:
 1. Die niet binnen het toepassingsgebied van deze procedure vallen, en stuurt deze, indien nodig, door naar andere bevoegde afdelingen/functionies van het bedrijf (bijv. in het geval van klachten);
 2. Indien de melder niet binnen de periode van 30 werkdagen na het verzoek de gevraagde aanvullende informatie verstrekt, of deze onvolledig en/of onvoldoende verstrekt voor een volledige beoordeling van de melding;
 3. Die duidelijk ongegrond of te kwader trouw zijn of waarvan de inhoud zo algemeen is dat er geen zorgvuldige follow-up mogelijk is.
- Als de melding voldoende gedetailleerd is, verder gaan met fase b).

b) Onderzoek

Als de meldingsbeheerder bij het resultaat van de voorlopige beoordeling van mening is dat de melding gegrond is omdat deze voldoende onderbouwd en met bewijsmateriaal gestaafd is, zal de meldingsbeheerder:

- De melding classificeren;
- Specifieke onderzoeksactiviteiten uitvoeren (bijv. documentanalyse, interviews, interne onderzoeken) tevens, waar dit het meest effectief wordt geacht en met voorafgaande toestemming van de Melder, gebruik te maken van de onderzoekscapaciteit van het bedrijf, zolang het aantal werknemers onder de 250 blijft, en/of met de hulp, indien nodig geacht, van zowel de bedrijfsfuncties die bevoegd zijn voor het onderwerp van de melding als de controleorganen of externe consultants/professionals voor specifieke en gespecialiseerde onderzoeksbehoeften. Als er gebruik wordt gemaakt van externe consultants/professionals, is het noodzakelijk om een vertrouwelijkheidsclausule voor gedeelde informatie op te nemen in het servicecontract dat met hen wordt afgesloten, waarin precies wordt aangegeven welke soorten informatie en/of documenten geheim moeten blijven (NDA);
- De omstandigheden onderzoeken door de beschikbare documenten en gegevens te analyseren en, waar dit nodig wordt geacht, de melder en andere personen die verband kunnen houden met de feiten die het onderwerp zijn van de melding, ondervragen. Deze activiteiten moeten worden gedocumenteerd door de bijeenkomst op te nemen of door notulen van de bijeenkomst te maken die door de melder of andere betrokken personen voor goedkeuring moeten worden ondertekend;
- Het onderzoek onderbreken als hij van mening is dat na grondig onderzoek, waarbij ook andere bedrijfsstructuren of externe consultants/professionals betrokken kunnen zijn, de melding ongegrond is, waarbij hij de redenen voor het archiveren van de melding formeel vastlegt;
- Voor zorgvuldige feedback aan de melder zorgen, mocht deze vragen om informatie over de voortgang van de zaak.

In de onderzoeksfase garandeert de meldingsbeheerder:

- De onpartijdigheid, eerlijkheid en nauwkeurigheid van de analyse en evaluatie van de interne melding;
- De vertrouwelijkheid van de verzamelde informatie en de vertrouwelijkheid van de identiteit van de melder, indien verstrekt;
- Het niet gebruiken van interne meldingen verder dan nodig is voor een adequate follow-up.

De meldingsbeheerder mag met de betrokken functies, controleorganen en professionals alleen de informatie delen die strikt noodzakelijk is voor de uitvoering van zijn activiteiten, en de identiteit van de melder, indien bekend, alleen vrijgeven met diens uitdrukkelijke toestemming. Zonder

toestemming mag de meldingsbeheerder geen informatie, feiten of bewijzen delen die de identificatie van de melder mogelijk maken.

Binnen drie maanden na de datum van ontvangstbevestiging, of bij het ontbreken daarvan, binnen drie maanden na het verstrijken van de periode van zeven dagen vanaf de indiening van de melding, geeft de meldingsbeheerder via het speciale IT-platform feedback aan de melder over het gevolg dat al aan de melding gegeven is of nog gegeven zal worden. De bevestiging kan definitief zijn als het onderzoek is afgerond, of tussentijds van aard zijn over de voortgang van het onderzoek als het nog niet is afgerond. In het laatste geval zal de meldingsbeheerder het eindresultaat van het onderzoek meedelen.

c) Besluit

Zodra de onderzoeksfase is afgerond, kan de meldingsbeheerder de volgende beslissingen nemen:

- Archivering zonder bevindingen;
- Aanbeveling van corrigerende maatregelen (bijv. trainingssessies, communicatie-initiatief, organisatorische wijzigingen, procedurele updates, *audits*), in coördinatie met andere bevoegde functies;
- Evaluatie van mogelijke disciplinaire maatregelen, in overeenstemming met de geldende wetgeving, individuele nationale collectieve arbeidsovereenkomsten en interne regelgeving, met inschakeling van de bevoegde functies;
- Tijdige informatie aan de wettelijke vertegenwoordiger en voor meldingen met betrekking tot corruptie aan het Focal Point van Sofidel Benelux NV , evenals aan de bevoegde functies/organen, rekening houdend met het onderwerp van de melding, indien vereist door het geval in kwestie voor de gepaste beoordeling van elke actie die moet worden ondernomen binnen het bereik van de bevoegdheid.

Nadat het besluit geformaliseerd is, consolideert de meldingsbeheerder een rapport over het onderzoek waarin wordt uitgelegd:

- De inhoud van de melding en eventuele ondersteunende documentatie;
- De uitgevoerde onderzoeksactiviteiten, met een uitgebreide chronologische reconstructie daarvan;
- De bevindingen en het bewijsmateriaal die al dan niet ter ondersteuning van de melding zijn verzameld, zodat de informatie die nodig is om de zaak te beoordelen duidelijk wordt geïllustreerd;
- De conclusies, waarin wordt aangegeven of het gemelde gedrag een inbreuk betreft, of dit nu bewezen is of niet (of dat het verzamelde bewijsmateriaal ontoereikend was) en, als het feit is vastgesteld, de te nemen maatregelen worden voorgesteld.

d) Archivering van de documentatie

Alle documentatie zal worden bewaard, onverminderd verdere wettelijke termijnen in de uitdrukkelijk voorziene gevallen, gedurende 5 jaar vanaf de datum van afsluiting van de onderzoeksactiviteiten. Een tijdslimiet die, in het geval van defensieve onderzoeken door het Bedrijf of onderzoeken en inspecties door de gerechtelijke autoriteiten of de gerechtelijke politie, evenals in het geval van rechtszaken of procedures, verlengd kan worden tot de beëindiging van dergelijke activiteiten of procedures.

De melding zelf wordt in een meldingsregister bewaard zolang de contractuele relatie tussen de melder en de werkgever voortduurt.

De naam, functie en contactgegevens van zowel de melder en elke persoon waarop de beschermings- en ondersteuningsmaatregelen van toepassing zijn, als van de betrokkene, met inbegrip van, indien van toepassing, het ondernemingsnummer, worden bijgehouden tot de verjaringstermijn voor de gemelde inbreuk is verstreken.

e) Rapportage en monitoring van corrigerende maatregelen

De meldingsbeheerder formaliseert schriftelijk, als onderdeel van het eindverslag, de beoordelingen en beslissingen die genomen zijn, de informatie die gegeven is indien vereist door de betreffende zaak en de aanbevelingen en voorstellen voor disciplinaire maatregelen (indien van toepassing), en archiveert deze ook op het platform, om de traceerbaarheid, vertrouwelijkheid, bewaring en terugvindbaarheid van de gegevens gedurende de hele procedure te garanderen.

Het is de plicht van de verantwoordelijken van de functies/processen waarop de melding betrekking heeft om de aanbevelingen van de meldingsbeheerder en de vastgestelde corrigerende maatregelen uit te voeren, ook met de ondersteuning van externe professionals.

De meldingsbeheerder houdt toezicht op de implementatie van de aanbevelingen en de implementatie van corrigerende maatregelen, en geeft regelmatig updates aan de wettelijke vertegenwoordiger en voor corruptie-gerelateerde meldingen aan het Focal Point van Sofidel Benelux NV, evenals aan de bevoegde functies/organen waar dit vereist is door de betreffende zaak.

2.5. Bescherming voor degenen die betrokken zijn bij het meldingsproces

2.5.1. De bescherming van de melder of met hem/haar gelijkgestelde personen

Het beschermingssysteem voor de melder is ook van toepassing op verschillende personen die aan represailles onderworpen zouden kunnen worden, zelfs indirect, vanwege hun rol in het meldingsproces, de openbaarmaking of aangifte, evenals vanwege hun specifieke relatie met de melder. In het bijzonder:

- De meldingsbeheerders;

- Derden die verbonden zijn met de melder en die het risico lopen op represaille in een professionele context;
- Rechtspersonen die gecontroleerd worden door of in een professionele context verbonden zijn met de melder.

Daarnaast bestaat het beschermingssysteem voor de melder (of met hem/haar gelijkgestelde personen) uit de volgende beschermingen:

i. De bescherming van geheimhouding en persoonlijke gegevens

In overeenstemming met de fundamentele principes van gegevensbescherming, zoals doelbinding en gegevensminimalisatie, mogen meldingen niet verder worden gebruikt dan nodig is voor een adequate vervolgactie.

Het personeel van Sofidel Benelux NV dat een melding ontvangt en/of in welke hoedanigheid dan ook betrokken is bij de behandeling van de melding, is verplicht tot geheimhouding van de identiteit van de personen (melders, of met hen gelijkgestelde personen en Gemelde Personen), van alle informatie waaruit deze identiteit direct of indirect kan worden afgeleid, en van de gemelde feiten, behalve in gevallen waarin:

- De melder instemt met de bekendmaking van dergelijke informatie aan andere dan bevoegde personen;
- In het kader van interne en externe meldingsprocedures de bekendmaking van de identiteit van de melder noodzakelijk is voor de verdediging van de betrokkene, met de uitdrukkelijke toestemming van de melder voor de bekendmaking van zijn of haar identiteit, en na schriftelijke kennisgeving van de redenen die tot de bekendmaking van zijn of haar identiteit hebben geleid.
- In het kader van de tegen de betrokkene ingeleide tuchtprocedure, indien de identiteit van de melder noodzakelijk is voor de verdediging van de betrokkene, met de uitdrukkelijke toestemming van de melder voor de bekendmaking van zijn of haar identiteit, en na schriftelijke kennisgeving van de redenen die tot de bekendmaking van zijn of haar identiteit hebben geleid;

Schending van de geheimhoudingsplicht leidt tot disciplinaire aansprakelijkheid, onverminderd enige andere aansprakelijkheid waarin de wet voorziet. Persoonsgegevens die duidelijk niet van nut zijn voor de verwerking van een specifieke melding worden niet verzameld of worden, als ze per ongeluk worden verzameld, onmiddellijk gewist.

De identiteit van de melder kan bekend worden gemaakt als dit noodzakelijk is in het kader van een onderzoek of gerechtelijke procedure, om de rechten van de verdediging te beschermen van de persoon op wie de melding betrekking heeft.

Het model voor het ontvangen en beheren van meldingen moet een DPIA (*Data Protection Impact Assessment*, ex art. 35 AVG) ondergaan om geschikte technische en organisatorische maatregelen te

identificeren en aan te nemen ter garantie van een beveiligingsniveau dat past bij de BIV-classificatie (Beschikbaarheid, Integriteit en Vertrouwelijkheid).

ii. *Bescherming tegen eventuele represaillemaatregelen, al was het maar een poging daartoe of een dreigement van het Bedrijf, naar aanleiding van de gedane melding, openbaarmaking of klacht*

Opdat de melder bescherming kan genieten, moet er een nauw verband bestaan tussen de melding, de openbaarmaking, de aangifte en het ongunstige gedrag/de handeling/het verzuim dat direct of indirect oneerlijke schade veroorzaakt, heeft veroorzaakt of kan veroorzaken.

De melder kan de Federale Ombudsman informeren over de represaille waarvan hij of zij denkt het slachtoffer te zijn geweest. De gerechtelijke autoriteit neemt ook de noodzakelijke maatregelen, met inbegrip van tijdelijke maatregelen, om de bescherming van de aangevoerde subjectieve rechtssituatie te waarborgen (bijv. schadevergoeding, herplaatsing op de werkplek, bevel om het represaillegedrag te staken en nietigverklaring van de bij wijze van represaille genomen maatregelen).

Bescherming is niet gegarandeerd als is vastgesteld, ook door een vonnis in eerste aanleg, dat de melder strafrechtelijk aansprakelijk is voor laster of smaad, of in ieder geval voor dezelfde inbreuken die zijn begaan bij de aanklacht bij de gerechtelijke of boekhoudkundige autoriteiten, of dat hij/zij civielrechtelijk aansprakelijk is in gevallen van opzettelijk wangedrag of grove nalatigheid. In dergelijke gevallen wordt een disciplinaire straf opgelegd aan de melder of de klokkenluider.

In de context van gerechtelijke of administratieve procedures of in elk geval van buitengerechtelijke geschillen met betrekking tot de vaststelling van verboden gedragingen, handelingen of nalatigheden tegen de melder (of met hem/haar gelijkgestelde personen), wordt verondersteld dat dergelijke gedragingen, handelingen of nalatigheden zijn gepleegd als gevolg van de melding, openbare bekendmaking of aanklacht bij de gerechtelijke of boekhoudkundige autoriteiten. De last om te bewijzen dat dergelijke gedragingen of handelingen gemotiveerd zijn door externe redenen ligt bij de persoon die ze heeft verricht.

iii. *Beperkingen van strafrechtelijke, civielrechtelijke en administratieve aansprakelijkheid*

Niet strafbaar is de persoon die door zijn of haar melding: (i) informatie openbaar maakt of verspreidt over inbreuken die onder de geheimhoudingsplicht vallen – met uitzondering van de verplichting met betrekking tot gerubriceerde informatie, het beroepsgeheim van forensische en medische deskundigen, het geheim van beraadslagingen van rechtbanken – of die verband houden met de bescherming van auteursrechten of de bescherming van persoonsgegevens; (ii) informatie openbaar maakt of verspreidt over inbreuken die de reputatie van de betrokkene schaden.

De melder kan alleen van deze beperking profiteren als hij/zij: a. redelijke gronden heeft om aan te nemen dat de openbaarmaking of verspreiding van de informatie noodzakelijk is om de inbreuk aan het licht te brengen; b. heeft gehandeld in overeenstemming met de voorwaarden die zijn vastgesteld voor het doen van de melding, hetzij intern of extern, of voor het doen van de openbaarmaking.

In elk geval wordt strafrechtelijke aansprakelijkheid en elke andere aansprakelijkheid, inclusief burgerlijke aansprakelijkheid, niet uitgesloten voor gedragingen, handelingen of nalatigheden die geen verband houden met de melding of die niet strikt noodzakelijk zijn om de inbreuk bekend te maken.

iv. Het voorzien in ondersteunende maatregelen door entiteiten uit de derde sector

De federal Ombudsman/ the Federal Institute for Human Rights (FIRM/IFDH) om gratis informatie, psychologische, sociale, technische en media-ondersteuning juridische bijstand in strafrechtelijke of civiele procedures en financiële ondersteuning bij gerechtelijke procedures.

2.5.2. Beschermingsmaatregelen voor de betrokkene en anderen die betrokken zijn in de melding

Aan de betrokkene moet de vertrouwelijkheid van zijn of haar identiteit worden gegarandeerd om nadelige gevolgen, waaronder gevolgen voor de reputatie, binnen de werkcontext te voorkomen.

Vertrouwelijkheid moet ook gegarandeerd worden ten aanzien van andere personen dan de betrokkene, maar die wel betrokken zijn in de melding daar zij daarin genoemd worden.

De melding is niet voldoende om een disciplinaire procedure tegen de betrokkene te starten.

Als, na concrete bevindingen over de melding, de meldingsbeheerder doorgaat met het onderzoek, kan er contact worden opgenomen met de betrokkene en kan deze de gelegenheid krijgen om de nodige opheldering te verschaffen.

De betrokkene heeft niet het recht om informatie te krijgen over de herkomst van de melding, noch heeft hij/zij het recht om informatie te krijgen over de persoonlijke gegevens van de melder.

De bescherming van de betrokkene is van toepassing behoudens de wettelijke bepalingen die de verplichting opleggen om de naam bekend te maken van de persoon van wie wordt vermoed dat hij of zij verantwoordelijk is voor de inbreuk (bijv. verzoeken van gerechtelijke autoriteiten).

Tevens zal het gedrag van een melder die ongegronde meldingen doet met kwade opzet of grove nalatigheid bestraft worden.

Elk misbruik van deze procedure, met inbegrip van interne meldingen die duidelijk opportunistisch zijn en/of uitsluitend zijn gedaan om de betrokkene of andere in de melding betrokken personenschade te berokkenen, zal leiden tot aansprakelijkheid in tuchtrechtelijke en andere bevoegde fora.

2.6. Implementatie van de procedure

De wettelijke vertegenwoordiger van Sofidel Benelux NV houdt toezicht op de effectieve implementatie van deze procedure en garandeert:

- de activering van het kanaal voor interne meldingen, waarbij de nodige middelen worden verstrekt voor de invoering en het onderhoud van het speciale IT-platform;
- het uitvoeren van geschikte specifieke opleidingsactiviteiten voor leden van de meldingsbeheerder en voor potentiële melders die een werkrelatie hebben met Sofidel Benelux NV.

2.7. Verspreiding van de procedure en *rapportage* over de werking van interne kanalen

Om het gebruik van het interne meldingssysteem aan te moedigen en de verspreiding van een cultuur van legaliteit te bevorderen, wordt de procedure in zijn geheel gepubliceerd op de website met procedures van het bedrijf.

De meldingsbeheerder rapporteert halfjaarlijks over de goede werking van de interne rapportagekanalen, met in een verslag geaggregeerde informatie over de resultaten van de rechtstreeks uitgevoerde activiteit en over de follow-up van de ontvangen meldingen. Deze rapportering gebeurt in overeenstemming met de regelgeving inzake gegevensbescherming. De meldingsbeheerder stuurt het bovengenoemde verslag naar de wettelijke vertegenwoordiger.

Daarnaast wordt er voorzien in een informatiestroom, indien nodig geautomatiseerd, naar de klokkenluiderscommissie van de moedermaatschappij met geaggregeerde informatie over de resultaten van de uitgevoerde activiteiten; een nuttig hulpmiddel voor alle monitoring- en verificatieactiviteiten.

3. Lijst met formulieren

Geen formulier bijgevoegd

4. Archivering

DOCUMENTEN	VERANTWOORDELIJKE	FORMAAT	BEWAARTERMIJN
Eindrapport en alle documenten met betrekking tot de melding	Meldingsbeheerder	Elektronisch	5 jaar

5. Definities

- **Werkcontext:** huidige of vroegere werk- of beroepsactiviteiten, uitgevoerd in de context van werkrelaties, waardoor een persoon, ongeacht de aard van dergelijke activiteiten, informatie verkrijgt over inbreuken en in de context waarvan hij/zij represailles zou kunnen riskeren in het geval van een melding of openbaarmaking aan de gerechtelijke of boekhoudkundige autoriteiten;
- **Openbaarmaking:** het openbaar maken van informatie over inbreuken via de pers of elektronische media of anderszins via verspreidingsmiddelen waarmee een groot aantal mensen kan worden bereikt;
- **Facilitator:** natuurlijke persoon die een melder in het meldingsproces bijstaat, binnen dezelfde werkcontext opereert en wiens hulp vertrouwelijk moet blijven;
- **Meldingsbeheerder:** natuurlijke persoon of een afdeling die meldingen ontvangt, deze onderzoekt en alle stappen onderneemt die nodig worden geacht om vast te stellen of ze gegrond zijn;
- **Informatie over inbreuken:** informatie, met inbegrip van gegronde vermoedens, over inbreuken die gepleegd zijn of die, op basis van concrete elementen, gepleegd zouden kunnen worden in de organisatie waarmee de melder of de persoon die de klacht indient bij de gerechtelijke of boekhoudkundige autoriteit een juridische band heeft, evenals elementen betreffende gedrag dat erop gericht is dergelijke inbreuken te verbergen;
- **Bevestiging:** mededeling aan de melder van informatie over de follow-up die aan de melding gegeven is of gepland is gegeven te worden;
- **Represaille:** elk gedrag, handelen of nalaten, zelfs als dit slechts een poging of een dreigement is, dat wordt gepleegd naar aanleiding van de melding, het rapport van de gerechtelijke of boekhoudkundige instantie of de openbare bekendmaking en dat de melder of de persoon die de melding doet, direct of indirect ongerechtvaardigde schade berokkent of kan berokkenen;
- **Melder:** de natuurlijke persoon die de melding doet, hetzij via interne meldingskanalen, hetzij via externe meldingskanalen, of die informatie over inbreuken openbaar maakt die hij of zij in het kader van zijn of haar werk heeft verkregen;
- **Betrokkene:** de natuurlijke of rechtspersoon die in de interne of externe melding of openbare bekendmaking wordt genoemd als de persoon aan wie de inbreuk wordt toegeschreven of als een persoon die anderszins betrokken is bij de betrokkene of bij de openbaar gemaakte inbreuk;
- **Melding:** schriftelijke of mondelinge communicatie van informatie over inbreuken;
- **Anonieme melding:** melding zonder de elementen die het mogelijk maken om de melder te identificeren;

- **Interne melding:** schriftelijke of mondelinge communicatie van informatie over inbreuken, ingediend via het interne meldingskanaal;
- **Externe melding:** schriftelijke of mondelinge communicatie van informatie over inbreuken, ingediend via het externe meldingskanaal dat door de nationale referentie-instantie is ingesteld;
- **Opvolging:** de actie die ondernomen is door de persoon aan wie het beheer van het meldingskanaal is toevertrouwd om het bestaan van gemelde feiten, het resultaat van het onderzoek en de eventueel genomen maatregelen te beoordelen;
- **Derden:** medewerkers, freelancers, consultants, leveranciers, klanten en meer in het algemeen iedereen die in een belangenrelatie staat met Sofidel Benelux NV, betaald of onbetaald;
- **Inbreuken:** gedrag, handelen of nalaten dat schadelijk is voor het openbaar belang of de integriteit van het openbaar bestuur of de particuliere entiteit.