

INTERNE MELDPROCEDURE KLOKKENLUIDERSRICHTLIJN

Bijlage 14 van het arbeidsreglement van Curando

1. Wetgeving en doelstelling

De klokkenluiderswet is een nieuwe Belgische omzettingswet die werd goedgekeurd op 24/11/2022. De wet heeft als doel om zowel interne medewerkers als derde partijen die – in een werk gerelateerde context – kennis nemen van inbreuken begaan door Curando op het Europese Unierecht of inbreuken die de Belgische wetgever aan het toepassingsgebied van de Belgische klokkenluiderswet heeft toegevoegd, de mogelijkheid biedt om hiervan melding te maken zonder angst te moeten hebben voor vergeldingsmaatregelen. Curando zet hiervoor een intern meldingskanaal op. Iedereen die een melding wenst te maken binnen het toepassingsgebied van de klokkenluiderswet, zal hiervoor in eerste instantie het intern meldingskanaal gebruiken.

2. Definities:

Inbreuk	Handelingen of nalatigheden die: <ul style="list-style-type: none"> • onrechtmatig zijn en betrekking hebben op Uniehandelingen en beleidsterreinen die binnen het in artikel 3 bedoelde materiële toepassingsgebied vallen, of • het doel of de toepassing ondermijnen van de regels in de Uniehandeling en beleidsterreinen die binnen het in artikel 3 bedoelde materiële toepassingsgebied vallen.
Informatie over inbreuken	Informatie, waaronder redelijke vermoedens, over feitelijke of mogelijke inbreuken, die hebben plaatsgevonden of zeer waarschijnlijk zullen plaatsvinden binnen de organisatie waar de melder werkt of heeft gewerkt of waarmee de melder uit hoofde van zijn werk in contact is geweest, en ook over pogingen tot verhulling van dergelijke inbreuken.
Melding	Het mondeling en/of schriftelijk verstrekken van informatie over inbreuken. <ul style="list-style-type: none"> • Interne melding: het binnen de organisatie mondeling/schriftelijk meedelen van informatie over inbreuken. • Externe melding: het mondeling of schriftelijk meedelen van informatie over inbreuken aan de bevoegde autoriteiten.
Openbaarmaking	Het mondeling of schriftelijk publiek meedelen van informatie over inbreuken.
Melder	Een natuurlijke persoon die in de context van zijn werkgerelateerde activiteiten verkregen informatie over inbreuken (intern, extern of openbaar) meldt.
Betrokkene	Een natuurlijke of rechtspersoon die in de (interne, externe of openbare) melding of bij de openbaarmaking wordt genoemd als persoon aan wie de inbreuken worden toegeschreven of met wie die persoon in verband wordt gebracht.
Facilitator	Een natuurlijke persoon die een melder bijstaat in het meldingsproces in een werk gerelateerde context en wiens bijstand vertrouwelijk moet zijn.
Represaille	Een (in)directe handeling of nalatigheid die in een werkgerelateerde context plaatsvindt n.a.v. een interne of externe melding of openbaarmaking, en die tot ongerechtvaardigde benadeling van de melder (of van de facilitators of derden die verbonden zijn met de melder) leidt of kan leiden.
Opvolging	Optreden van de ontvanger van een melding of een bevoegde autoriteit om de juistheid van de in de melding gedane beweringen na te gaan en de gemelde inbreuk zo nodig aan te pakken.
Feedback	Het aan de melder verstrekken van informatie over de als opvolging geplande of genomen maatregelen en over de redenen voor die opvolging.
Bevoegde autoriteit	De Belgische autoriteit die is aangewezen om meldingen overeenkomstig artikel 5 van dit beleid te ontvangen en de melders feedback te geven en opvolging te verzekeren.

Werk gerelateerde context	De huidige of vroegere arbeidsactiviteiten 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 als zij dergelijke informatie zouden melden.
Federale coördinator	De autoriteit die belast is met de coördinatie van de externe meldingen voor de privésector overeenkomstig afdeling 4 hoofdstuk 4 van de klokkenluiderswet.
Meldingsbeheerder	De onpartijdige persoon of dienst die bevoegd is om de meldingen op te volgen, de communicatie met de melder te onderhouden, hem indien nodig om bijkomende informatie kan verzoeken, hem feedback te verstekken en indien van toepassing meldingen te ontvangen.

3. Melder en meldingen

Een “melder” is elkeen die bij Curando werkzaam is of is geweest of werkzaamheden heeft verricht in welke hoedanigheid dan ook: werknemer, zelfstandige, interim of consultant, bestuurder, leidinggevende, maar ook vrijwilligers en (on)bezoldigde stagiairs en eenieder die werkt onder toezicht en leiding van aannemers, onderaannemers en leveranciers van Curando.

De melder kan alle informatie melden over feitelijke of mogelijke inbreuken die hebben plaatsgevonden of zeer waarschijnlijk zullen plaatsvinden binnen de organisatie waarvan de melder kennis heeft binnen de werkgerelateerde context en die hij wil onthullen. Tot die informatie horen ook redelijke vermoedens. Het gaat om inbreuken op volgende gebieden:

- Overheidsopdrachten
- Financiële diensten
- Productveiligheid
- Veiligheid van het vervoer
- Bescherming van het milieu en stralingsbescherming
- Veiligheid van levensmiddelen en diervoeder, diergezondheid en dierenwelzijn
- Volksgezondheid
- Consumentenbescherming
- Bescherming van de persoonlijke levenssfeer en persoonsgegevens en beveiliging van netwerk en informaticasystemen
- Bestrijding van belastingfraude en sociale fraude

Deze meldprocedure beschrijft de werkwijze voor het melden en de behandeling van inbreuken die NIET kunnen gemeld worden via de reeds bestaande meldkanalen en/of contactpersonen.

Curando zet reeds sterk in op een veilige meldcultuur van incidenten of bijna-incidenten binnen en buiten de zorg. De reeds bestaande meldkanalen voor bewoners en niet-bewonersgerelateerde incidenten of bijna-incidenten blijven van toepassing volgens de procedure veiligheidsincidenten. Voor meldingen of klachten rond psychosociale thema’s zoals grensoverschrijdend gedrag kan men steeds terecht bij de direct leidinggevenden of de vertrouwenspersonen.

4. Interne meldingen

6.1 Intern meldingskanaal

Een melding kan (niet) anoniem en gebeurt schriftelijk, via een mail naar het departementshoofd HRM (heleen.debaeke@curando.be), in alle vertrouwen en zonder sancties voor de melder.

Elke melding wordt met de nodige ernst opgevolgd. Een vertrouwelijke behandeling wordt gewaarborgd. Er worden geen stappen ondernomen om de identiteit van de anonieme melder te achterhalen.

6.2 Behandeling van interne meldingen

Binnen vzw Curando worden de interne meldingskanalen intern beheerd. Binnen Curando is het departement HRM verantwoordelijk als onpartijdige persoon voor de opvolging van de melding en de communicatie. Uiterlijke binnen de 7 dagen na ontvangst van de melding krijgt de melder een ontvangstbevestiging toegestuurd.

6.3 Bekendmaking aan overheidsinstanties

Als een melding informatie bevat die van rechtswege moet doorgegeven worden aan een overheidsinstantie die verantwoordelijk is voor de opvolging van misdrijven binnen de gebieden vermeld in artikel 3, zal het departement HRM de informatie doorsturen naar de betrokken overheidsinstantie.

6.4 Feedback

De melder krijgt binnen een redelijk termijn, en dit ten laatste 3 maanden na het verstrijken van de ontvangstbevestiging of indien er geen ontvangstbevestiging is verstuurd aan de melder, drie maanden na het verstrijken van de periode van zeven dagen na de melding, feedback over de afhandeling van de melding. Dat betekent dat hij informatie krijgt over de al dan niet genomen corrigerende 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 is, zal het departement HRM waken over de vertrouwelijkheid van de onderzoeksdaten en over de naleving van de rechten van derden.

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

5. Externe meldingen

7.1. Externe meldingskanalen

De melder die geen interne melding wil doen, kan ook beroep doen op een extern meldingskanaal. De externe meldingen gebeuren bij de federale coördinator van de bevoegde autoriteit (zie bijlage 1). De melder kan dit doen volgens de methoden die beschikbaar gesteld worden door de bevoegde autoriteit.

7.2 Behandeling van externe meldingen

Uiterlijk binnen de zeven dagen na ontvangst van de melding krijgt de melder een ontvangstbevestiging toegestuurd van de bevoegde federale dienst.

Binnen een redelijke termijn, en ten laatste drie maanden na het versturen van de ontvangstbevestiging, of indien er geen ontvangstbevestiging is verstuurd aan de melder, drie maanden na het verstrijken van de periode van zeven dagen na de melding, krijgt de melder informatie van de bevoegde federale dienst over de als opvolging geplande of genomen maatregelen en over de redenen van die opvolging.

In uitzonderlijke gemotiveerde gevallen kan deze termijn zes maanden bedragen.

De bevoegde autoriteiten en de federale coördinator duiden de personeelsleden aan die

verantwoordelijk zijn voor de behandeling van de meldingen. Deze personeelsleden zijn gehouden tot geheimhoudingsplicht en krijgen een opleiding voor het behandelen van meldingen.

6. Openbaarmaking

Een persoon die een openbaarmaking doet, komt in aanmerking voor bescherming uit hoofde van de klokkenluiderswet, als de volgende voorwaarden vervuld zijn:

- Indirecte openbaarmaking: persoon deed eerst een interne en/of externe melding, maar er zijn n.a. v. die melding geen passende maatregelen genomen binnen de gestelde termijn; of
- Directe openbaarmaking: persoon heeft gegronde redenen om aan te nemen dat de inbreuk een dreigend of reëel gevaar kan zijn voor het algemeen belang; of er bij een 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.

Dit is niet van toepassing op gevallen waarin een persoon rechtstreeks informatie aan de pers verstrekt op grond van specifieke bepalingen die een stelsel voor de bescherming van de vrijheid van meningsuiting en informatie instellen.

7. Vertrouwelijkheid en geheimhouding

Het departement HRM zorgt ervoor dat de informatie over de melding zodanig wordt bewaard dat deze fysiek en digitaal alleen toegankelijk is voor diegenen die als bevoegde personen werden aangeduid. Alle meldingen en daaropvolgende onderzoeksrapporten en/of vaststellingsrapporten, beslissingen,... worden met de grootst mogelijke vertrouwelijkheid behandeld.

Het departement HRM hanteert een strikte 'need to know'-basis voor het bekendmaken van informatie aan werknemers of derden. Alle werknemers die betrokken zijn bij de ontvangstmelding, of opvolging van meldingen, zullen een strikte geheimhouding handhaven over de inhoud van meldingen, rapporten, beslissingen ... en dit voor zover de toepasselijke wetgeving dat toelaat.

8. Bescherming

10.1 Bescherming tegen represailles

Curando garandeert dat de melder beschermd wordt tegen represailles, inclusief dreigingen en pogingen tot represailles, als de melder te goeder trouw handelt en de juiste weg volgt bij het maken van een melding.

De "juiste weg" betekent dat de melder in eerste instantie zoveel mogelijk gebruikmaakt van de voorziene interne meldingskanalen. Pas als er geen intern kanaal is, of als een externe melding zonder gevolg blijft, kan een melding openbaar gemaakt worden.

Onder "represailles" verstaan we onder meer:

- Schorsing, tijdelijke buitendienststelling, ontslag of soortgelijke maatregelen;
- Degradatie of weigering van bevordering;
- Overdracht van taken, wijziging arbeidsplaats, loonsverlaging, verandering van de werktijden;
- Het onthouden van opleiding;
- Een negatieve evaluatie of arbeidsreferentie;
- Het opleggen van een disciplinaire maatregel, berisping of andere sanctie;
- Dwang, intimidatie, pesterijen of uitsluiting;

- Discriminatie, nadelige of ongelijke behandeling;
- 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;
- Niet-verlenging of vervroegde beëindiging van een tijdelijke arbeidsovereenkomst;
- Schade, met inbegrip van reputatieschade, met name op sociale media, of financieel;
- Nadeel, met inbegrip van omzetzendering en inkomstendering;
- Opname op een zwarte lijst op basis van een informele of formele overeenkomst voor een hele sector of bedrijfstak, waardoor de melder geen baan meer kan vinden in de sector of de bedrijfstak;
- Vroegtijdige beëindiging of opzegging van een contract voor de levering van goederen of diensten;
- Intrekking van een licentie of vergunning;
- Psychiatrische of medische verwijzingen.

Naast de melder zelf worden ook de facilitators en derden die verbonden zijn met de melder en die ook het slachtoffer kunnen worden van represailles in een werk gerelateerde context, en de eventueel beschuldigde individuele personen beschermd.

Curando garandeert hen het recht op een eerlijk proces en het vermoeden van onschuld. Hun identiteit wordt strikt geheimgehouden zolang de onderzoeken naar aanleiding van de melding lopen.

10.2 Klachtenprocedure

Elke melder die meent slachtoffer te zijn van of bedreigd te worden met een represaille, kan een met redenen omklede klacht indienen bij de federale coördinator van de bevoegde autoriteit, die een buitengerechtelijke beschermingsprocedure opstart. De federale coördinator van de bevoegde autoriteit verifieert het bestaan van een redelijk vermoeden van een represaille.

De bewijslast dat het geen represaille is, valt ten laste van Curando. Als Curando een maatregel neemt tegen een melder die binnen het wettelijk kader valt, en kan aantonen dat de redenen voor die maatregel vreemd zijn aan de melding, dan is die maatregel geen represaille.

9. Misbruik van meldingskanalen/inbreuken op dit beleid

Curando zal enkel die meldingen behandelen die te goeder trouw werden gedaan en die binnen het toepassingsgebied van de klokkenluiderswet vallen. Werknemers die te kwader trouw een melding maken, met het oogmerk om te schaden, genieten geen bescherming.

Bij het te kwader trouw maken van een melding, stelt de betrokken werknemer zich in het bijzonder bloot aan de sancties die deel uitmaken van het arbeidsreglement, met inbegrip van de ultieme maatregel van ontslag.

10. Bewaring van documenten/register van meldingen

Het departement HRM houdt een register bij van alle meldingen, waarin zowel de ontvangst van de melding, het onderzoek ernaar en de oplossing ervan worden opgevolgd. De meldingen worden in dit register bewaard zolang de contractuele relatie tussen de melder en de werkgever loopt. Onderzoeksrapporten en ondersteunende informatie worden minimaal tot vijf jaar na het einde van het onderzoek bewaard.

11. Verwerking van persoonsgegevens

Alle persoonsgegevens worden verwerkt in overeenstemming met de toepasselijke wetgeving over gegevensbescherming, waaronder de Algemene Verordening Gegevensbescherming (“GDPR”). De omgang met persoonsgegevens wordt omschreven in art.6 van het arbeidsreglement.

12. Ondersteuningsmaatregelen

Het Federaal Instituut voor de bescherming en de bevordering van de rechten van de mens wordt belast met het toepassen van of toezien op de ondersteuningsmaatregelen, zowel in geval van een interne melding, een externe melding als een openbaarmaking.

De melder heeft, naargelang het geval, toegang tot de volgende ondersteuningsmaatregelen:

- Volledige en onafhankelijke informatie en adviezen, die gemakkelijk en kosteloos toegankelijk zijn over de beschikbare remedies en procedures die bescherming bieden tegen represailles, en ook over de rechten van de betrokkene, met inbegrip van zijn rechten op het vlak van bescherming van persoonsgegevens; de melder moet bovendien worden geïnformeerd dat hij in aanmerking komt voor de beschermingsmaatregelen waarin deze wet voorziet;
- Technisch advies ten aanzien van elke autoriteit die betrokken is bij de bescherming van de melder;
- Rechtsbijstand in grensoverschrijdende strafrechtelijke en burgerlijke procedures overeenkomstig Richtlijn (EU) 2016/1919 en Richtlijn 2008/52/EG van het Europees Parlement en de Raad en rechtsbijstand in andere procedures alsook juridisch advies of andere juridische bijstand, overeenkomstig de bepalingen over de juridische tweedelijnsbijstand en de rechtsbijstand;
- Ondersteunende maatregelen, waaronder technische, psychologische, media gerelateerde en sociale ondersteuning, voor de melder;
- Financiële bijstand aan de melder in het kader van gerechtelijke procedures.

Bijlage 1 : Lijst federale autoriteiten

1. Overheidsopdrachten: de dienst Overheidsopdrachten van de FOD Kanselarij van de Eerste minister;
2. 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;
3. Productveiligheid en productconformiteit: FOD Economie, FOD Volksgezondheid, FAGG, BIPT, FOD Mobiliteit;
4. Veiligheid van het vervoer: FOD Mobiliteit, Nationale Autoriteit voor Maritieme Beveiliging;
5. Bescherming van het milieu: FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu, Leefmilieu Brussel, CREG, Algemene Directie Energie, ACER;
6. Stralingsbescherming en nucleaire veiligheid: Federaal Agentschap voor Nucleaire Controle;
7. Veiligheid van levensmiddelen en diervoeders, diergezondheid en dierenwelzijn: FAVV, FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu;
8. Volksgezondheid: Sciensano, FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu, FAGG, Federale commissie “Rechten van de patiënt”;
9. Consumentenbescherming: FOD Economie;
10. Bescherming van de persoonlijke levenssfeer en persoonsgegevens, en beveiliging van netwerk- en informatiesystemen: Gegevensbeschermingsautoriteit, CCB, EDPS