

Klokkenluiderspolicy

Preamble

Carat NV, Ambachtenstraat 7, 2260 Westerlo, ingeschreven in de Kruispuntbank van Ondernemingen onder het nummer 0445.993.726 hierna "de Onderneming" genoemd, streeft ernaar haar activiteiten op een integere en ethische manier uit te oefenen. Daarom biedt zij de mogelijkheid om elke inbreuk op de wettelijke en reglementaire bepalingen vermeld in artikel 1 van deze klokkenluiderspolicy (hierna "de Policy" genoemd) te melden, zodra een dergelijke inbreuk binnen de Onderneming wordt vastgesteld, en dit overeenkomstig de hierna bepaalde voorwaarden.

De Onderneming stelt hiertoe meldingskanaal ter beschikking. Koki Groep is zich bewust van haar maatschappelijke verantwoordelijkheid in al haar activiteiten en baseert deze op algemeen geldende ethische waarden en principes. Duurzaam management vormt eveneens een essentieel onderdeel van de bedrijfscultuur. Koki Groep leeft deze principes na en ziet toe op de naleving ervan.

Het binnen de Groep opgezette meldingskanaal wordt beheerst door:

- De "*Rules of procedure for the whistleblowing procedure at Metabowerke GmbH*" (hierna "het Reglement" genoemd), van tijd tot tijd updatet, beschikbaar via de volgende link:
 - https://www.metabo.com/t3/fileadmin/metabo/com_en/030_company/Rules_of_Procedure.pdf
- De pagina <https://www.carat-tools.com/be-nl> en <https://www.carat-tools.com/be-fr>, die een overzicht biedt van het beschikbare meldingskanaal.
- De pagina <https://koki-group-eu.integrityline.app/>, via welke een online melding kan worden ingediend.
- Elke ander Policy/Bepaling met betrekking tot de klokkenluiders, die ter beschikking zal worden gesteld.

Voor zover deze Policy van toepassing is op de Onderneming, primeert de huidige Policy boven de regels in het Reglement.

Het doel van deze Policy is om alle medewerkers en iedereen met een contractuele relatie met de Onderneming aan te moedigen om, onder de in deze Policy beschreven voorwaarden, elke onaanvaardbare, illegale, onethische of frauduleuze handeling met betrekking tot de activiteiten van de Onderneming te melden, zonder vrees voor represailles. In deze Policy beschrijft de Onderneming de aanbevolen procedure bij elk vermoeden van een inbreuk, en licht zij de bescherming toe die klokkenluiders genieten.

In dit kader verbindt de Onderneming zich ertoe te voldoen aan zowel Richtlijn (EU) 2019/1937 van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden, als de Belgische wet die deze omzet (hierna de "Belgische Klokkenluiderswet"¹ genoemd), en om:

- het vertrouwelijk melden, al dan niet anoniem, van enige informatie met betrekking tot een mogelijke of daadwerkelijke onaanvaardbare handeling mogelijk te maken;
- een hoog niveau van effectieve bescherming te bieden aan de persoon die de melding doet;
- de procedure vast te stellen die door de melder (hierna "de klokkenluider" genoemd) moet worden gevolgd;

¹ 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.

- vervolgmaatregelen te nemen tegen ongepast gedrag binnen de Onderneming.

Deze Policy is beschikbaar op de website van de Onderneming <https://www.carat-tools.com/be-nl> en <https://www.carat-tools.com/be-fr>.

Artikel 1. Materieel toepassingsgebied - welke inbreuken kunnen worden gemeld?

1.1.

Het meldingskanaal maakt het mogelijk om vermoedelijke inbreuken te melden die betrekking hebben op de volgende gebieden, zoals bepaald door de Belgische Klokkenluiderswet:

- Overheidsopdrachten;
- Financiële diensten, producten en markten, voorkoming van witwassen van geld en terrorismefinanciering;
- Productveiligheid en productconformiteit;
- Veiligheid van het 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.

Daarnaast kunnen ook de volgende inbreuken worden gemeld:

- Inbreuken waardoor de financiële belangen worden geschaad;
- Inbreuken in verband met de Europese interne markt, met inbegrip van inbreuken op de Unieregels inzake mededinging en staatssteun.

Een inbreuk wordt gedefinieerd als de handelingen of nalatigheden die onrechtmatig zijn en betrekking hebben op, of ingaan tegen het doel of de toepassing van de regels in het bovengenoemde toepassingsgebied. Hiertoe inbegrepen is elke inbreuk tegen de toepasselijke wettelijke of reglementaire bepalingen of van de bepalingen die werden aangenomen in toepassing van de voornoemde bepalingen.

1.2.

Daarnaast, met het oog op het engagement van de Onderneming en Koki Groep om haar activiteiten op een integere en ethische wijze uit te oefenen en om op de hoogte te zijn van eventuele inbreuken binnen de Onderneming, wordt het toepassingsgebied van deze Policy aangevuld met volgende gebieden:

- Schending van wetten en reglementaire vereisten;
- Schending van policy's en richtlijnen;
- Schending van de gedragscodes;
- Indicaties van corruptie en omkoping;
- Schendingen op het gebied van gezondheid en veiligheid op het werk;
- Indicaties van pesten, discriminatie en grensoverschrijdend gedrag;
- Opmerkingen met betrekking tot boekhouding en administratie;
- Schending van het mededingings- en antitrustrecht;

- Schending van mensenrechten;
- Schending van internationale handelscontroles;
- Belangenconflicten;
- Diversen.

Het meldingskanaal is niet bedoeld voor het indienen van algemene klachten, klachten van klanten of vragen over garantie.

Artikel 2. Personeel toepassingsgebied - wie kan schendingen melden?

Het meldingskanaal dient ertoe meldingen te behandelen van de volgende personen (de "klokkenluiders") die in een werkgerelateerde context informatie over bepaalde inbreuken hebben verkregen:

- De personen met de hoedanigheid van werknemer;
- De personen met de hoedanigheid van zelfstandige;
- De aandeelhouders en de personen die behoren tot het bestuurlijk, leidinggevend of toezichhoudend orgaan van een Onderneming, met inbegrip van niet bij het dagelijks bestuur betrokken leden, vrijwilligers en bezoldigde of onbezoldigde stagiairs;
- Eenieder die werkt onder toezicht en leiding van aannemers, onderaannemers en leveranciers;
- Personen die informatie over inbreuken die is verkregen in een inmiddels beëindigde werkrelatie melden of openbaar maken;
- Personen wier werkrelatie nog moet aanvangen, ingeval informatie over inbreuken is verkregen tijdens de wervingsprocedure of andere precontractuele onderhandelingen;
- Elke persoon die in het bezit is van informatie verkregen buiten een werkgerelateerde context, aangaande inbreuken binnen de Onderneming op het gebied van financiële diensten, producten en markten.

Artikel 3. De melding

Elke in artikel 2 genoemde persoon kan, via het hieronder vermelde meldingskanaal, informatie melden, met inbegrip van redelijke vermoedens, over daadwerkelijke of potentiële inbreuken of daarmee verband houdende risico's die hebben plaatsgevonden of zeer waarschijnlijk zullen plaatsvinden, of over pogingen om dergelijke inbreuken te verbergen.

Onder inbreuken wordt verstaan elke handeling of nalatigheid die onrechtmatig is en betrekking heeft op de in artikel 1 genoemde gebieden, of ingaat tegen het doel of de toepassing van de regels binnen deze gebieden.

Artikel 4. Meldingskanaal

Elke in artikel 2 genoemde persoon die kennis heeft van een inbreuk binnen de Onderneming op de in artikel 1 genoemde gebieden, of daartoe een redelijk vermoeden heeft, wordt verzocht dit meteen te melden via het meldingskanaal.

4.1. Intern meldingskanaal

4.1.1. Beschikbaar intern meldingskanaal

Het volgende kanaal is ter beschikking van klokkenluiders voor meldingen:

| | |
|--------|---|
| Online | Koki-group-eu.integrityline.app/ |
|--------|---|

Klokkenluiders die anoniem een melding willen doen², wordt aanbevolen gebruik te maken van het online meldingssysteem³. Dit systeem maakt anonieme communicatie met de klokkenluider mogelijk. De Onderneming raadt klokkenluiders die het online meldingssysteem gebruiken daarom aan om regelmatig in te loggen en hun dossier te controleren op nieuwe berichten.

Meldingen via het online meldingssysteem zijn gratis.

Als een melding betrekking heeft op een specifieke vennootschap van Koki Groep, kan de klokkenluider deze vennootschap selecteren in het online meldingssysteem, zodat de melding door de deze vennootschap wordt verwerkt.

Het meldingssysteem is op een veilige manier ontworpen, geïmplementeerd en beheerd, zodat:

- de vertrouwelijkheid van de identiteit van de klokkenluider en eventuele derden die in de melding worden genoemd gewaarborgd blijft;
- niet-gemachtigde personeelsleden geen toegang hebben tot deze gegevens;
- de privacy en persoonsgegevens van de klokkenluider en derden die in de melding worden genoemd te allen tijde worden beschermd.

4.1.2. Verwerking van meldingen

A. Indiening

De klokkenluider navigeert naar de startpagina en klikt op de knop "Een rapport indienen".

Op de volgende pagina kan de klokkenluider de melding in eigen woorden formuleren en de vragen beantwoorden over hetgeen hij heeft vastgesteld (door een antwoord te selecteren of eigen tekst in te voeren). Daarnaast is het mogelijk een bestand toe te voegen ter ondersteuning van de melding of een geluidsfragment op te nemen. De klokkenluider dient zich ervan bewust te zijn dat bestanden informatie over de auteur kunnen bevatten (metadata).

De klokkenluider kan de melding anoniem, dan wel in eigen naam indienen. Vervolgens dient de klokkenluider een beveiligde mailbox⁴ in te stellen (zie "Beveiligde mailbox"). Deze mailbox maakt het mogelijk feedback te ontvangen en eventuele vragen te beantwoorden.

² De klokkenluider wordt evenwel aangemoedigd om zijn of haar naam in de melding op te geven.

³ Hoe wordt de anonimiteit van de klokkenluider beschermd?

Bij het indienen van een melding of vraag via de Integriteitslijn blijft de klokkenluider anoniem, tenzij deze besluit zijn of haar identiteit bekend te maken. Op voorwaarde dat de klokkenluider zelf geen gegevens invoert waaruit zijn of haar identiteit zou kunnen blijken, garandeert het systeem de anonimiteit met een gecertificeerde technische oplossing.

De melding wordt dankzij encryptie en andere beveiligingsoplossingen anoniem gehouden. Bovendien slaat het systeem geen IP-adressen noch computer-ID's op en gebruikt het geen cookies. Wanneer evenwel een melding wordt gemaakt vanaf een computer in het bedrijfsnetwerk, bestaat het risico dat de bezochte websites worden opgeslagen in de geschiedenis van de browser of de onderneming. Om dit risico uit te sluiten, kan de klokkenluider de melding indienen via een computer die geen deel van het bedrijfsnetwerk uitmaakt. Bij het opladen van documenten moet de klokkenluider zich er ook bewust van zijn dat de bestanden metadata kunnen bevatten die de identiteit van de melder kunnen onthullen. Daarom moet de klokkenluider ervoor zorgen dat alle metadata van de bestanden worden verwijderd voordat deze worden geüpload.

⁴ Via de beveiligde mailbox krijgt de klokkenluider toegang tot een technische omgeving, die uitsluitend toegankelijk is voor de klokkenluider en de onderneming. Hierdoor kan contact worden opgenomen met de klokkenluider. Dit is belangrijk, aangezien tijdens de verwerking van de melding vaak vragen ontstaan die alleen met de hulp van de klokkenluider kunnen worden opgehelderd en mogelijk doorslaggevend zijn voor het verdere verloop.

Tot slot wordt de klokkenluider gevraagd een veiligheidsvraag te beantwoorden ter bevestiging dat hij of zij geen "robot" is.

B. Inhoud van de melding

Meldingen dienen de volgende informatie te bevatten:

- Wat is je vermoeden? (Beschrijving van hetgeen werd vastgesteld: wat is er gebeurd, wanneer en waar vond het incident plaats, is het incident nog gaande, enz.)
- In welk bedrijf vond het incident plaats?
- Waar vond het incident plaats? (land, plaats, evenement, enz.)
- Is de klokkenluider een werknemer van het betreffende bedrijf, leverancier, klant, enz.?
- Wat is de naam van de betreffende afdeling?
- Wie is betrokken bij het incident (potentiële verdachte)?
- Heeft iemand het incident waargenomen (getuigen)?
- Is er bewijs dat het incident aantoont (bijv. documenten, enz.)?

C. Wat gebeurt er na de melding?

▪ Ontvanger van de melding

Alle meldingen worden via beveiligde servers van het online meldkanaal doorgestuurd naar de Chief Compliance Officer van Metabowerke GmbH en diens vertegenwoordigers en/of, indien beschikbaar, naar een lokale of regionale verantwoordelijke Compliance Officer en diens vertegenwoordigers. Zij handelen onafhankelijk, vertrouwelijk en zonder belangenvermenging of instructies.

Indien de Chief Compliance Officer van Metabowerke GmbH, diens vertegenwoordigers, de Compliance Officer verantwoordelijk op lokaal of regionaal niveau en zijn vertegenwoordigers of andere werknemers een belangenconflict hebben, of indien de overtreding door één van deze personen zelf is begaan, wordt deze persoon onmiddellijk uitgesloten van het onderzoek.

▪ Ontvangstbevestiging

De klokkenluider ontvangt binnen zeven dagen na ontvangst van de melding een bevestiging van ontvangst, op voorwaarde dat hij contactgegevens heeft opgegeven of een communicatiemogelijkheid heeft ingesteld.

▪ Opvolging van de melding

- Controle van de melding

De ontvanger van de melding zorgt voor de opvolging.

Opvolging betekent elk optreden van de ontvanger van een melding om de juistheid (of ontvankelijkheid) van de in de melding gedane beweringen na te gaan. Dit houdt in dat wordt nagegaan of de melding onder het bovengenoemde toepassingsgebied valt. Indien dit niet het geval is, ontvangt de klokkenluider

Bij het aanmaken van de beveiligde mailbox ontvangt de klokkenluider een Case ID en dient hij een wachtwoord te kiezen. Deze case ID en wachtwoord zijn vereist om toegang te krijgen tot de mailbox en om te controleren of er vragen zijn ontvangen. Via de beveiligde mailbox wordt ook feedback verstrekt over de voortgang van de melding. Indien gewenst, kan alle communicatie anoniem blijven.

hierover feedback. Indien van toepassing valt onder opvolging ook het aanpakken van de gemelde inbreuk, met inbegrip van het nemen van maatregelen, zoals:

- een (intern) vooronderzoek;
- vervolging;
- een terugvordering van middelen;
- of het beëindigen van de procedure (indien de ontvanger van de melding door het beoordelen van de juistheid (of ontvankelijkheid) van de melding tot de conclusie komt dat het incident niet via het klokkenluiderssysteem gemeld mag worden).

- **Verduidelijking van de feiten**

De ontvanger van de melding onderhoudt contact met de klokkenluider om feedback te geven, en indien nodig, om meer informatie te vragen, bijvoorbeeld wanneer de feiten moeten worden opgehelderd (in dat geval neemt de ontvanger van de melding contact op met de klokkenluider via de Integriteitslijn of via andere communicatiemiddelen, indien die door de klokkenluider ter beschikking zijn gesteld).

Het kan nodig zijn om andere gespecialiseerde afdelingen in te schakelen, zoals de HR-afdeling, Gegevensbescherming, Inkoop, of externe dienstverleners.

Indien nodig worden de bevoegde autoriteiten betrokken. Dit kan met name het geval zijn wanneer er een wettelijke verplichting bestaat om dit te doen, of als verdere opheldering van de feiten niet langer via interne maatregelen mogelijk is, doch noodzakelijk blijkt.

Bij concrete meldingen van verdachte activiteiten kunnen specialisten worden ingeschakeld en kan een onderzoek worden ingesteld.

▪ **Onderzoek**

Indien de melding wordt bevestigd, wordt onmiddellijk een grondig onderzoek opgestart in overeenstemming met deze Policy. Alle onderzoeken worden grondig uitgevoerd, met inachtneming van de principes van vertrouwelijkheid, gegevensbescherming, onpartijdigheid en billijkheid van alle betrokkenen.

▪ **Maatregelen**

Passende maatregelen zullen worden onderzocht en, indien nodig, worden geïmplementeerd en opgevolgd.

Dit kan sancties tegen werknemers omvatten, zoals een waarschuwing, berisping of ontslag, waarbij zorgvuldig rekening wordt gehouden met de aard en de ernst van de overtreding en de mate van aansprakelijkheid.

Indien noodzakelijk kan een strafrechtelijke aanklacht worden ingediend. Daarnaast kan het nodig zijn om schadeclaims in te dienen.

Corrigerende maatregelen zijn erop gericht de schending te voorkomen, te beëindigen, of – indien dat niet mogelijk is – minstens te beperken.

Daarnaast wordt onderzocht of preventieve maatregelen kunnen worden genomen, uitgebreid of indien nodig geïmplementeerd.

D. Feedback

Uiterlijk drie maanden na de ontvangstbevestiging - of, indien er geen ontvangstbevestiging naar de klokkenluider is verstuurd, uiterlijk drie maanden na het verstrijken van de periode van zeven dagen na de melding - ontvangt de klokkenluider feedback over de geplande of reeds genomen maatregelen en de redenen voor de gekozen opvolging, op voorwaarde dat de klokkenluider zijn of haar contactgegevens heeft verstrekt of een ander communicatiemiddel heeft ingesteld. Vertrouwelijke informatie kan worden meegedeeld om feedback te garanderen.

E. Afsluiting van de procedure en bewaring

Aan het einde van de procedure worden de resultaten en de genomen maatregelen gedocumenteerd en opgeslagen op een manier die toegangsbescherming biedt. De wettelijke verwijderingsplicht en bewaarplicht worden nageleefd.

4.2. Extern meldingskanaal

Naast het interne meldingskanaal kan de klokkenluider een vermoedelijke inbreuk ook melden via externe meldingskanaal, zoals de kanalen die door de Belgische bevoegde autoriteiten⁵ ter beschikking worden gesteld. Dit kan zowel na eerst een interne melding te hebben gedaan, hetzij door rechtstreeks via een extern meldingskanaal een melding in te dienen.

Deze externe autoriteiten zijn belast met het ontvangen van externe meldingen, het verstrekken van feedback aan de melder en het uitvoeren van de taken die zijn voorzien in de Belgische Klokkenluiderswet, met name met betrekking tot de opvolging van de melding.

De Federale Ombudsman is verantwoordelijk voor de coördinatie van meldingen die via externe kanalen worden ingediend. Concreet houdt dit in dat de Ombudsman belast is met het ontvangen van externe

⁵1° de Federale Overheidsdienst Economie, K.M.O., Middenstand en Energie;
2° de Federale Overheidsdienst Financiën;
3° de Federale Overheidsdienst Volksgezondheid, Veiligheid van de voedselketen en Leefmilieu;
4° de Federale Overheidsdienst Mobiliteit en Vervoer;
5° de Federale Overheidsdienst Werkgelegenheid, Arbeid en Sociaal Overleg;
6° de Programmatie Overheidsdienst Maatschappelijke Integratie, Armoedebestrijding, Sociale Economie en Grootstedenbeleid
7° het Federaal Agentschap voor Nucleaire Controle;
8° het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten;
9° het Federaal Agentschap voor de veiligheid van de voedselketen;
10° de Belgische Mededingingsautoriteit;
11° de Gegevensbeschermingsautoriteit;
12° de Autoriteit voor Financiële Diensten en Markten;
13° de Nationale Bank van België;
14° het College van toezicht op de bedrijfsrevisoren;
15° de autoriteiten gemeld in artikel 85 van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;
16° het Nationaal Comité voor de beveiliging van de levering en distributie van drinkwater;
17° het Belgisch Instituut voor postdiensten en telecommunicatie;
18° het Rijksinstituut voor ziekte- en invaliditeitsverzekering;
19° het Rijksinstituut voor de Sociale Verzekeringen der Zelfstandigen;
20° de Rijksdienst voor Arbeidsvoorziening;
21° de Rijksdienst voor Sociale Zekerheid;
22° de Sociale Inlichtingen en Opsporingsdienst;
23° de Autonome dienst Coördinatie Anti-Fraude (CAF);
24° de Scheepvaartcontrole.

meldingen, het beoordelen van hun ontvankelijkheid en het doorsturen ervan naar de bevoegde autoriteit voor verder onderzoek, afhankelijk van het onderwerp van de melding.

Wanneer een autoriteit een melding ontvangt maar niet bevoegd is om de gemelde inbreuk te behandelen, stuurt zij de melding door naar de Federale Ombudsman, die deze vervolgens binnen een redelijke termijn en op een veilige manier doorstuurt naar de bevoegde instantie.

Indien geen enkele autoriteit zich bevoegd acht om een melding te ontvangen, treedt de Federale Ombudsman als bevoegde instantie voor het ontvangen van externe meldingen.

De contactgegevens van de Federale Ombudsman zijn als volgt:

Adres: Leuvenseweg 48, bus 6 1000 Brussel
Online klacht: <https://www.federaalombudsman.be>
E-mail: contact@federaalombudsman.be
Telefoon: 0800 99 961 of +32 2 289 27 27 vanuit het buitenland
Faxnummer: +32 2 289 27 28

Aanbevolen wordt om waar mogelijk prioriteit te geven aan het interne meldingskanaal. In het geval van een externe klokkenluidersmelding zijn de beschermingsmaatregelen tegen represailles alleen gegarandeerd indien voldaan wordt aan de voorwaarden vermeld in artikel 5.2.3.

Artikel 5. Bescherming van klokkenluiders

5.1. Vertrouwelijkheid

De identiteit van de klokkenluider wordt gedurende de hele procedure strikt vertrouwelijk behandeld en wordt niet bekendgemaakt aan anderen dan (1) de personen die bevoegd zijn om de melding te ontvangen en op te volgen en dan (2) tenzij een wettelijke uitzondering van toepassing is, aan de persoon die door de melding wordt geïdентificeerd, binnen een redelijke termijn omwille van de vereisten inzake gegevensbescherming, die termijn mag niet langer zijn dan één maand na de verkrijging van de persoonsgegevens, tenzij er een wettelijke verplichting tot openbaarmaking⁶ bestaat, of de klokkenluider uitdrukkelijk toestemming tot openbaarmaking geeft.

Dit geldt ook voor alle andere informatie waaruit de identiteit van de klokkenluider direct of indirect kan worden afgeleid.

Alle interne en externe partijen die betrokken zijn bij het onderzoek en de opvolging zijn verplicht tot geheimhouding.

5.2. Bescherming tegen represailles

5.2.1. Beschermden personen

⁶ De identiteit van de klokkenluider kan worden bekendgemaakt wanneer dit noodzakelijk en evenredig is op grond van een bijzondere wetgeving in het kader van onderzoeken door nationale autoriteiten of in het kader van gerechtelijke procedures, met name om de rechten van verdediging van de betrokken persoon te waarborgen (dat wil zeggen: "een natuurlijke persoon of rechtspersoon die in de melding of publieke bekendmaking wordt genoemd als de persoon aan wie de inbreuk wordt toegeschreven of met wie die persoon in verband wordt gebracht"). In dat geval wordt de klokkenluider vooraf geïnformeerd over de bekendmaking van zijn of haar identiteit, tenzij een dergelijke kennisgeving het betrokken onderzoek of de betrokken gerechtelijke procedures in gevaar zou kunnen brengen.

Elke in artikel 2 bedoelde persoon kan niet worden onderworpen aan represailles, met inbegrip van dreigingen of pogingen tot represailles, als gevolg van de gemelde feiten. De bescherming tegen represailles is tevens van toepassing op de volgende personen, mits er redelijke gronden waren om aan te nemen dat de klokkenluider binnen het toepassingsgebied van de Belgische Klokkenluiderswet viel:

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

Een represaille wordt gedefinieerd als elke 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.

5.2.2. Represailles

Tenzij naar behoren gerechtvaardigd, kunnen de volgende maatregelen worden beschouwd als represailles:

- Tewerkstellingsmaatregelen, bijv. schorsing, tijdelijke buitendienststelling, ontslag, loonsverlaging, weigering van bevordering, verandering van functie, disciplinaire sancties of maatregelen, berisping of andere sancties, zoals een financiële sanctie, degradatie, onthouden van bevordering, lage of negatieve prestatiebeoordeling of arbeidsreferentie;
- Beslissingen die negatieve gevolgen hebben voor de werkomstandigheden, bijv. overdracht van taken, verandering van locatie van de arbeidsplaats, loonsverlaging, het onthouden van opleiding, verandering van de werktijden, weigering van verlof;
- Bepaalde gedragingen, zoals dwang, intimidatie, pesterijen, ostracisme, discriminatie, nadelige of oneerlijke 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 omzetsderving en inkomstenderving;
- 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;
- Vroegtijdige beëindiging of opzegging van een contract voor de levering van goederen of diensten;
- Uitsluiting of schorsing van een lid of zijn benoemde afgevaardigde;
- Intrekking van een licentie of vergunning;
- Psychiatrische of medische verwijzingen.

5.2.3. Voorwaarden voor de bescherming - wat als de inhoud van de melding achteraf vals blijkt te zijn?

Bescherming tegen represailles is gegarandeerd indien aan de volgende voorwaarden is voldaan:

- De klokkenluider handelde te goeder trouw op het moment van de melding. Dit betekent dat hij redelijke gronden had om aan te nemen dat de gemelde informatie juist was en dat de inbreuk onder het toepassingsgebied van huidige Policy viel.
- De melding werd ingediend in overeenstemming met deze Policy en de Belgische Klokkenluiderswet.

Het eerste criterium wordt beoordeeld vanuit het perspectief van een persoon in een vergelijkbare situatie met een vergelijkbare kennis. Het is van belang dat de klokkenluider op het moment van de melding geloofde of aannam dat de inhoud gegrond was en niet met kwade bedoelingen handelde. Van de klokkenluider wordt niet verwacht dat deze zelf bewijs verzamelt of het incident opheldert. Uit het onderzoek kan later bijgevolg blijken dat er geen strafbaar feit is gepleegd. In dat geval verliest de klokkenluider niet het voordeel van bescherming alleen op grond van het feit dat de te goeder trouw gedane melding onjuist of ongegrond is gebleken.

Indien er sprake is van misbruik, een opportunistische melding, kwade trouw of een melding die uitsluitend bedoeld is om de Onderneming of derden schade te berokkenen, kan de klokkenluider worden onderworpen aan disciplinaire sancties (met inbegrip van de sancties voorzien in het arbeidsreglement), juridische stappen of strafrechtelijke sancties⁷.

Het is verboden het indienen van een melding te belemmeren. Eenieder die een klokkenluider belemmert om een melding in te dienen, stelt zich bloot aan mogelijke disciplinaire sancties (met inbegrip van de sancties voorzien in het arbeidsreglement), juridische stappen of strafrechtelijke sancties⁸.

Artikel 6. Gegevensbescherming

De persoonsgegevens die via de klokkenluidersprocedure worden verstrekt, worden verwerkt door **Carat NV**, Ambachtenstraat 7, 2260 Westerlo, ingeschreven in de Kruispuntbank van Ondernemingen onder het nummer 0445.993.726 .

De Onderneming verzamelt en verwerkt dergelijke persoonsgegevens in overeenstemming met de wetgeving inzake de bescherming van klokkenluiders, waaronder de Belgische Klokkenluiderswet, en de wetgeving inzake gegevensbescherming, waaronder Verordening (EU) 2016/679 (de "AVG").

De verwerking van deze gegevens gebeurt ter naleving van een wettelijke verplichting en/of op basis van het legitieme belang van de Onderneming, voor zover het interne meldingskanaal de wettelijke doelstellingen overstijgt. Dit omvat met name de opsporing van misdrijven en het waarborgen van de veiligheid en het ethisch gedrag binnen de Onderneming.

De relevante informatie over gegevensbescherming is beschikbaar via het online meldingssysteem: <https://koki-group-eu.integrityline.app/app-page;appPageName=Privacy%20policy?lang=nl>

Meer informatie over gegevensbescherming is tevens te vinden op de volgende websites: <https://www.carat-tools.com/be-nl/content/privacy>

⁷ Wanneer kan worden aangetoond dat iemand opzettelijk valse informatie heeft gemeld of openbaar heeft gemaakt, kunnen strafrechtelijke sancties worden opgelegd overeenkomstig art. 443-450 van het Belgische Strafwetboek en kan een burgerrechtelijke schadevergoeding worden geëist (cf. art 33, § 3 van de Belgische Klokkenluiderswet).

⁸ Het belemmeren van iemand om een melding in te dienen of het nemen van represailles wordt bestraft met een gevangenisstraf van zes maanden tot drie jaar en/of met een geldboete van 600 tot 6.000 euro. De straf kan worden uitgesproken tegen de onderneming en/of de leden van haar personeel (cf. art 33, § 2 van de Belgische Klokkenluiderswet).

<https://www.carat-tools.com/be-fr/content/privacy>

Artikel 7. Inwerkingtreding

Deze Policy treedt op 16/12/2025 in werking en blijft van kracht voor onbepaalde duur.

De Onderneming behoudt zich het recht voor om deze Policy op elk moment aan te passen, met inbegrip van, maar niet beperkt tot, wijzigingen in relevante wetgeving en/of operationele vereisten.