KLOKKENLUIDERSBELEID SMULDERS GROUP

1 Klokkenluiders gebruikerspolicy – korte toelichting

De klokkenluidersregeling is de regeling waarmee je in een werkcontext op een veilige manier een mogelijke inbreuk of ernstige integriteitskwestie kunt melden. Deze korte toelichting zet het beleid in duidelijke taal op een rij. Zo zie je in één oogopslag wat je kunt melden, hoe je dat doet, wat er daarna met je melding gebeurt en welke bescherming je krijgt.
Belangrijk: dit is enkel een samenvatting. De uitgebreide policy bevat de volledige regels en blijft altijd leidend.
Let op: sommige regels verschillen naargelang het land waar jouw entiteit zich bevindt. Daarom vind je hieronder ook extra aandachtspunten per land. In de uitgebreide policy vind je ook de concrete meldingskanalen, e-mailadressen en telefoonnummers.

- **Wie kan melden?** Werknemers, ex-werknemers, sollicitanten, uitzendkrachten, stagiairs, freelancers, leveranciers, aannemers, aandeelhouders en anderen die via hun werk informatie kregen over een mogelijke inbreuk.
- **Wat kun je melden?** Mogelijke schendingen van wetgeving, fraude, corruptie, veiligheidsproblemen, privacyproblemen, milieuschade, financiële onregelmatigheden en andere ernstige integriteitsproblemen.
- **Wat valt meestal niet onder dit beleid?** Persoonlijke klachten over samenwerking, loon, arbeidsvoorwaarden of conflicten op het werk. Daarvoor gelden meestal HR- of klachtenprocedures.
- **Moet je bewijs hebben?** Nee. Je hoeft niets te bewijzen, maar je moet wel eerlijke en redelijke redenen hebben om te denken dat er iets mis is.
- **Hoe kun je melden?** Mondeling of schriftelijk, bijvoorbeeld via een intern meldingskanaal, e-mail, telefoon, een gesprek of – waar wettelijk mogelijk – extern bij een bevoegde autoriteit.
- **Mag je zelf een meldingskanaal kiezen?** Ja. Je mag in principe zelf het kanaal kiezen dat het best past bij je situatie en de toepasselijke regels, bijvoorbeeld intern of – waar wettelijk mogelijk – extern.
- **Kun je anoniem melden?** Ja, dat kan. Houd er wel rekening mee dat anoniem melden de opvolging soms moeilijker maakt.
- **Wat zet je best in je melding?** Beschrijf zo duidelijk mogelijk wat er is gebeurd, wie betrokken is, waar en wanneer het gebeurde en welke informatie of documenten je daarover hebt.
- **Blijft je melding vertrouwelijk?** Ja. Je identiteit en de informatie uit je melding worden vertrouwelijk behandeld. Alleen de mensen die je melding moeten ontvangen, beoordelen of opvolgen, krijgen toegang. Je identiteit wordt alleen gedeeld als dat wettelijk verplicht is of als jij daarmee uitdrukkelijk instemt.
- **Wat gebeurt er na je melding?** Je krijgt normaal binnen 7 dagen een ontvangstbevestiging. Daarna wordt bekeken of er een onderzoek moet volgen. Daarbij kunnen de bevoegde interne personen en, waar nodig, ook de CKI (Commissie Klachtenbehandeling Inbreuken) worden betrokken. Doorgaans krijg je binnen 3 maanden feedback over de opvolging of de volgende stappen.
- **Ben je beschermd?** Ja. Als je meldt volgens de geldende regels en je redelijke gronden hebt om te denken dat de informatie juist is, hoef je in principe geen represailles te vrezen. Ontslag, pesterijen, benadeling of andere negatieve gevolgen omdat je hebt gemeld, zijn verboden. De precieze voorwaarden verschillen per land.
- **Let op voor landverschillen** De belangrijkste aandachtspunten staan hieronder kort samengevat. Voor de volledige regels geldt altijd de uitgebreide policy.

1.1 Korte aandachtspunten per land

Verenigd Koninkrijk: hier geldt een ander wettelijk kader dan in de EU.
Frankrijk: hier gelden bijkomende voorwaarden voor bescherming.
Nederland: niet elke persoonlijke klacht gerelateerd aan de werkomgeving valt onder een misstand.
België en Polen: lokale regels kunnen verschillen voor scope, procedure en opvolging.

Voor de volledige en concrete regels, meldingskanalen, e-mailadressen, telefoonnummers en land-specifieke details geldt altijd de uitgebreide policy.

Twijfel je of iets onder dit beleid valt? Meld je bezorgdheid liever wél dan niet, of vraag advies via de voorziene kanalen. Raadpleeg altijd de uitgebreide policy voor het volledige en concrete kader, de juiste meldingskanalen, de toepasselijke land-specifieke regels en alle relevante e-mailadressen en telefoonnummers.

2 Inleiding

De gedragscode van SMULDERS GROUP NV (hierna “Smulders”) bevat kernwaarden, normen en spelregels die gelden voor de hele organisatie. Deze code moet worden gerespecteerd in onze relaties met alle stakeholders: klanten, leveranciers, overheden, aandeelhouders en medewerkers.

Smulders hecht veel waarde aan openheid, integriteit en naleving van wet- en regelgeving. Medewerkers en andere betrokkenen moeten mogelijke overtredingen veilig kunnen melden, zonder angst voor negatieve gevolgen. In dit klokkenluidersbeleid wordt uiteengezet hoe meldingen kunnen worden gemaakt, hoe ze worden behandeld en welke bescherming klokkenluiders genieten.
We verwijzen eveneens naar de “Klokkenluiders Gebruikers Policy”, die kort en krachtig de rode draad van de richtlijn aangeeft.

Dit beleid beschrijft:

- **wie** melding kan doen
- de **domeinen** waarover men melding kan doen (deze verschillen per locatie van de entiteit)
- **hoe** men melding kan doen: **bij wie** (kanalen) en **de wijze waarop**
- de **bescherming** die melders krijgen
- **de opvolging** die aan een melding wordt gegeven.

Smulders verwacht niet dat een individuele melder in staat is te bewijzen dat een beschuldiging terecht is. Hij/zij moet echter wel kunnen aantonen dat er voldoende reden is om te veronderstellen dat er iets niet klopt.

De organisatie van het intern meldingskanaal, de te volgen procedures voor de interne melding en de opvolging van meldingen worden opgezet na overleg met de sociale partners.

3 Definities

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.

CKI: Commissie Klachtenbehandeling Inbreuken. Dit betreft een commissie die uit drie personen bestaat (waaronder een voorzitter) binnen de Smulders Group en is aangesteld om meldingen over een vermoeden van een inbreuk/misstand te behandelen (hierna ‘CKI’).

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

Inbreuk : handelingen of nalatigheden die :

- onrechtmatig zijn en betrekking hebben op de domeinen opgesomd onder artikel 4 “Toepassingsgebied”, of
- die ingaan tegen het doel of de toepassing van de regelgeving die binnen de in artikel 4 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 (klokkenluider) : 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:

- werknemer
- ex-werknemer
- sollicitant
- Freelancer/consultant/ zelfstandige dienstverlener (ZZP-er)
- vrijwilliger
- (on)bezoldigde stagiair
- uitzendkracht (gedetacheerde)
- (werknemer bij een) klant
- leverancier
- (onder-)aannemer en/of diens werknemers
- 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.

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/haar indien nodig bijkomende informatie te verzoeken, hem/haar feedback te verstrekken en indien van toepassing meldingen te ontvangen en te behandelen. Voor Smulders is dat de Compliance Officer.

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

4 Toepassingsgebied

De regeling onderscheidt sociale en zakelijke integriteit. Hieronder wordt een lijst van domeinen opgenomen waarop een melding betrekking kan hebben, conform de EU-Richtlijn en aangevuld met de lokale afwijkingen voor België, Nederland, het Verenigd Koninkrijk en Polen.

4.1 Sociale integriteit

Deze categorie omvat ongewenste omgangsvormen zoals pesten, discriminatie, geweld en grensoverschrijdend gedrag. Deze behoren **niet** tot het toepassingsgebied van de klokkenluiderswetgeving, maar volgen andere interne procedures, zie hieronder:

- Voor Belgie: zie R-HRM-IEM-035 Arbeidsreglement Iemants/R-HRM-SPB-044 Arbeidsreglement Smulders Projects Belgium NL/R-HRM-WIL-040 Arbeidsreglement Willems
- Voor NL- Vlissingen zie: R-HRM-SPN-002 Personeelshandboek
- Voor NL- Schiedam zie: Integriteitsbeleid (2020)
- Voor Polen zie: P-HRA-SPP-002 Escalation Ladder.docx
- Voor UK zie: R-HRA-SPU-021 Employee Handbook en R-HRA-SPU-001 Anti-Bullying and Harassment policy
- Voor Frankrijk: socale integriteit (pesten, discriminatie, geweld, grensoverschrijdend gedrag) valt buiten dit klokkenluidersbeleid en moet gemeld worden via de lokale HR- preventieprocedures voor pshycosociale risico's (incl. harcèlement).

4.2 Zakelijke integriteit

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 beklaagde, tussen wie de ongewenste omgangsvormen zich voordoen, terwijl zakelijke integriteitskwesties 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.

4.3 RICHTLIJN 2019/1937 - Europees, Belgisch, Nederlands en Pools recht

De onderstaande domeinen gelden voor alle Belgische, Nederlandse en Poolse entiteiten van de Smulders Groep. Het betreft zakelijke integriteitschendingen die een schending vormen van EU-recht of de nationale implementatie daarvan (1-15)**:**

1. Overheidsopdrachten;
2. Financiële diensten, producten en markten, 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 en dierenwelzijn;
8. Volksgezondheid;
9. Consumentenbescherming;
10. Bescherming van de persoonlijke levenssfeer en persoonsgegevens, en beveiliging van netwerk- en informatiesystemen;
11. Inbreuken in verband met de interne markt van de Europese Unie zoals inbreuken op de staatssteun- en mededingingsregels: concurrentiebeperkende gedragingen en overeenkomsten afsluiten, misbruik van prijszetting, misbruik van dominante positie, …;
12. Belastingfraude;
13. Sociale fraudebestrijding;
14. Inbreuken waardoor de financiële belangen van de Unie worden geschaad

Voor alle entiteiten (ook UK) binnen de EIFFAGE GROUP geldt bovendien dat over onderstaande domeinen ook melding gemaakt kan worden:

Inbreuken op:

15. Mensenrechten en fundamentele vrijheden
16. Gezondheid en veiligheid van personen
17. Milieubescherming, zoals voorgeschreven door de Wet van 27 maart 2017, bekend als de ‘Loi sur le devoir de vigilance’ (Loi n° 2017-399) betreffende de zorgplicht van moedermaatschappijen en opdrachtgevers.
18. Het niet naleven van de gedragscode (Code of Conduct) van de EIFFAGE Group, in het bijzonder inbreuken op het verbod van corruptie, omkoping, of beïnvloeding, evenals elk ander onethisch of illegaal gedrag;
19. Misdrijven, overtredingen;
20. Bedreiging van of schade aan het algemeen belang;
21. Een schending (of een poging tot het verbergen van een schending) van het Unierecht een internationale verbintenis die door Frankrijk is geratificeerd of goedgekeurd, van een eenzijdige handeling van een internationale organisatie die is verricht op basis van een dergelijke verbintenis, het recht van de Europese Unie, de wet of van de regelgeving.

4.4 Land specifieke aanvullingen of afwijkingen

4.4.1 Nederland

Voor Nederland gelden de domeinen onder 4.3 even zeer, maar men werkt met het begrip ‘**misstand’**, wanneer het maatschappelijk belang in het gedrang is. Een melding kan betrekking hebben op:

- (Dreigend) gevaar voor veiligheid van personen;
- (Dreigend) gevaar voor volksgezondheid;
- (Dreigende) ernstige milieuschade;
- (Dreigende) ondermijning van het goed functioneren van een onderneming of publieke dienst;
- Schending van interne regels die een wettelijke verplichting bevatten.

Nederland wijkt niet af van de EU domeinenlijst (en de EIFFAGE domeinen), maar hanteert een bredere maatschappelijke toetsing.

4.4.2 Verenigd Koninkrijk (UK) — PIDA categorieën

EU-richtlijn 2019/1937 is niet van toepassing op het Verenigd Koninkrijk. De bescherming van klokkenluiders in het VK wordt geregeld door de Public Interest Disclosure Act 1998 (PIDA), zoals opgenomen in de Employment Rights Act 1996. Op grond van dit kader worden werknemers beschermd wanneer zij een 'beschermde melding' doen in de zin van de Employment Rights Act 1996 en redelijkerwijs van mening zijn dat de melding in het openbaar belang is.

4.4.2.1 Gerechtvaardigde meldingen

Bepaalde meldingen zijn bij wet aangemerkt als „gerechtvaardigde meldingen“. Een „gerechtvaardigde melding“ is een melding van informatie waarvan de werknemer oprecht en redelijkerwijs meent dat deze in het algemeen belang is en waaruit blijkt dat de onderneming een „relevante tekortkoming“ heeft begaan door:

- het plegen van een strafbaar feit;
- het niet nakomen van een wettelijke verplichting;
- een gerechtelijke dwaling;
- de gezondheid en veiligheid van een persoon in gevaar te brengen;
- milieuschade te veroorzaken;
- seksuele intimidatie te plegen (zoals gedefinieerd in artikel 26, lid 2, van de Equality Act 2010); of
- informatie met betrekking tot het bovenstaande te verzwijgen.

Elke vorm van "misstand" die mogelijk binnen de bovenstaande categorieën valt, ongeacht de sector, kan worden gemeld.

Deze handelingen kunnen in het verleden, het heden of de toekomst hebben plaatsgevonden, zodat bijvoorbeeld een melding in aanmerking komt als deze betrekking heeft op milieuschade die heeft plaatsgevonden, plaatsvindt of waarschijnlijk zal plaatsvinden. Het bedrijf neemt alle zorgen die u met betrekking tot bovengenoemde zaken naar voren brengt zeer serieus. De werknemer is niet verantwoordelijk voor het onderzoeken van de zaak – het is de verantwoordelijkheid van het bedrijf om ervoor te zorgen dat er een onderzoek plaatsvindt.

4.4.2.2 Beschermde meldingen (alleen VK)

Een melding die in aanmerking komt, wordt beschouwd als een beschermde melding in het kader van de Public Interest Disclosure Act 1998 (PIDA) en de Employment Rights Act 1996 wanneer de werknemer:

- redelijkerwijs gelooft dat de verstrekte informatie in wezen waar is en in het algemeen belang is; en
- de melding doet via een geschikte meldingsroute, zoals:
  - een intern meldingskanaal van het bedrijf;
  - een externe melding aan een relevante voorgeschreven persoon die binnen zijn wettelijke bevoegdheid handelt; of
  - – in beperkte omstandigheden – een bredere of openbare melding, indien aan de wettelijke voorwaarden voor een dergelijke melding is voldaan.

Wanneer een melding kwalificeert als een beschermde melding, is de werknemer wettelijk beschermd tegen ontslag, nadeel of enige andere vorm van vergelding als gevolg van het doen van de melding.

4.4.2.3 Klokkenluiden versus persoonlijke arbeidszaken (alleen VK)

In het Verenigd Koninkrijk is klokkenluiden bedoeld om het melden van zorgen in het algemeen belang mogelijk te maken.

Zaken die uitsluitend betrekking hebben op iemands persoonlijke arbeidssituatie, zoals persoonlijke klachten over salaris, arbeidsomstandigheden, interpersoonlijke conflicten of managementbeslissingen, vallen normaal gesproken niet onder “klokkenluiden” en dienen te worden gemeld via de daarvoor bestemde klachtenprocedure of HR-procedure, tenzij de kwestie ook een breder publiek belang raakt of binnen de reikwijdte van een kwalificerende melding valt zoals hierboven beschreven.
Wanneer een kwestie zowel een persoonlijke impact heeft als een breder publiek belang dient, kan deze binnen de reikwijdte van dit klokkenluidersbeleid vallen.

Alle vormen van 'wrong doing', die potentieel binnen bovenstaande categorieen vallen, ongeacht de sectoren, kunnen gemeld worden.

4.4.3 Frankrijk

Voor Frankrijk is het begrip "lanceur d'alerte" (wet n° 2016-1691 zoals gewijzigd in 2022) gekoppeld aan de voorwaarde dat de melder te goeder trouw handelt en zonder direct financieel eigenbelang.

5 Indienen melding en vervolgstappen

A. Bij wie?

Een klokkenluider heeft verschillende kanalen tot zijn/haar beschikking om een inbreuk te melden.

• Klokkenluiders worden aangemoedigd om, waar mogelijk en gepast, hun zorgen intern te uiten (bijvoorbeeld bij hun manager), aangezien dit vaak leidt tot een snelle en effectieve aanpak van problemen.

Interne melding is echter niet verplicht en klokkenluiders kunnen rechtstreeks via interne of externe meldingskanalen rapporteren, in overeenstemming met het toepasselijke wettelijke kader.

• Indien een klokkenluider ervoor kiest om een bezorgdheid bij zijn/haar manager te bespreken en de omstandigheden dit niet toelaten, of de manager niet adequaat reageert, kan de klokkenluider een (vermoedelijke) inbreuk melden bij de hiërarchisch meerdere van zijn/haar manager.

• De klokkenluider heeft ook altijd het recht om zijn of haar werknemersvertegenwoordigers of vakbonden te raadplegen en blijft beschermd tegen ongerechtvaardigde negatieve maatregelen als gevolg van deze raadplegingen.

• Indien de klokkenluider van mening is dat hij of zij zich om welke reden dan ook niet tot de bovengenoemde personen kan wenden, kan hij of zij een interne melding doen bij de CKI.

Een interne melding is een melding van een inbreuk binnen het bedrijf door mondelinge of schriftelijke informatie over overtredingen te verstrekken via het interne meldingskanaal. De procedure hiervoor wordt nader beschreven in paragraaf B, " HOE INDIENEN VAN EEN MELDING ".

• Klokkenluiders kunnen een externe melding doen, mondeling of schriftelijk, via het externe meldingskanaal dat is opgezet door de bevoegde autoriteit, zoals verder uitgelegd in paragraaf E, " INDIENEN VAN EEN MELDING VIA HET EXTERN MELDINGSKANAAL VAN DE OVERHEID ".

Dit kan zonder voorafgaande interne melding, of nadat het interne meldingskanaal is gebruikt, indien van toepassing en in overeenstemming met de geldende wetgeving.

• Een openbare melding of openbaarmaking van informatie over overtredingen is alleen mogelijk als aan de strikte voorwaarden van hoofdstuk 6, " OPENBAARMAKING VAN EEN INBREUK IN UITZONDERLIJKE OMSTANDIGHEDEN ", is voldaan.

De klokkenluider heeft de mogelijkheid om een anonieme melding in te dienen. Dergelijke meldingen worden met de nodige zorgvuldigheid ontvangen en behandeld.

Klokkenluiders dienen zich ervan bewust te zijn dat anonieme meldingen bepaalde praktische beperkingen met zich mee kunnen brengen, waaronder:

- het kan moeilijker zijn om verduidelijking of aanvullende informatie te verkrijgen wanneer dat nodig is; en
- het kan de mogelijkheden van Smulders beperken om individuele feedback te geven of persoonlijke bescherming te bieden tegen mogelijke represailles.

Deze beperkingen zullen op zich niet leiden tot het negeren van de melding.

B. Hoe indienen van een melding

Het indienen van een interne melding gebeurt mondeling of schriftelijk via:

a) e-mail ethics@smulders.com
b) webapplicatie https://eiffage.integrityline.org
c) telefoon/spraakberichtsysteem

- Voor Belgie:

Katy Rijnders: Mob.: +32 (0) 478 506 428

- Voor Nederland - Vlissingen:

Dhr. Sander Meijers: Mob.: +31 (0) 6 15426527

- Voor Nederland - Schiedam:

Dhr. Paul Wenting: Mob.: +31(0) 6 51370674

- Voor het Verenigd Koninkrijk:

Mrs. Amanda Young: Mob.: +44 7387 411624

- Voor Polen:

Katarzyna Dendewicz: Mob: +48 606252937

- Voor Frankrijk:

Samia Ben Belaïd: Tel.: +33 610 166 307

d) fysieke ontmoeting binnen een redelijke termijn:

- Voor Belgie:

Mw. Katy Rijnders: Katy.rijnders@smulders.com Mob.: +32 (0) 478 506 428

- Voor Nederland - Vlissingen:

Dhr. Sander Meijers: Sander.Meijers@smulders.com Mob.: +31 (0) 615426527

- Voor Nederland - Schiedam:

Dhr. Paul Wenting: paul.wenting@smulders-hsm.com Mob.: +31(0) 6 51370674

- Voor het Verenigd Koninkrijk:

Mrs. Amanda Young: Amanda.Young@smulders.com Mob.: +44 7387 411624

- Voor Polen:

Katarzyna Dendewicz: Katarzyna.Dendewicz@smulders.com Mob: +48 606252937

- Voor Frankrijk:

Samia Ben Belaïd: Samia.Ben.Belaid@smulders.com Tel. +33 610 166 307

Een melding bevat ten minste:

- De naam, het adres, 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 heeft 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

Ad b) Online meldingen kunnen steeds worden ingediend via het beveiligde interne meldingskanaal van de EIFFAGE GROUP: https://eiffage.integrityline.org

Raadpleeg de FAQ op deze site voor praktische vragen over indienen en opvolgen van meldingen door de EIFFAGE alert managers.
Het interne meldingskanaal wordt door EQS gehost en betreft een versleuteld platform met gegevensopslag binnen de Europese Unie.

Alleen door Eiffage aangewezen (lokale en groeps) **alert managers** hebben toegang. Wanneer een melding via een fysiek gesprek tot stand komt, wordt deze door bevoegde medewerkers in het platform geregistreerd; de melder kan het verslag nalezen, corrigeren en goedkeuren alvorens verdere opvolging gebeurt.

C. <u>Ontvankelijkheid en vooronderzoek</u>

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 de CKI. 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 betrokken HR directeur van Smulders.

D. <u>Onderzoek</u>

a) De CKI zal op basis van voormeld advies beslissen of en met welke onderzoekscommissie het onderzoek dient te worden uitgevoerd: ofwel enkel door de meldingsbeheerder, ofwel door de voltallige CKI en/of aangevuld met interne, dan wel externe experten, 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 CKI zal het onderzoek binnen een redelijke termijn uitvoeren, rekening houdend met de aard en complexiteit van de melding.
Waar mogelijk zal feedback over de opvolging, de geplande of genomen maatregelen en de redenen voor die opvolging doorgaans binnen drie (3) maanden na ontvangstbevestiging aan de klokkenluider worden verstrekt.
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.
e) Eindrapportering

De eindrapportering omvat de volgende stappen :

a) De meldingsbeheerder rapporteert haar bevindingen schriftelijk aan de voorzitter van het CKI 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 de voorzitter van het CKI 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 de voorzitter van het CKI van oordeel is dat er sanctionerend dient te worden opgetreden, zal hij de bevoegde persoon van het management een kopij bezorgen van het eindrapport.

E. <u>Indienen van een melding via het extern meldingskanaal van de overheid</u>

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.

De volgende contactpunten zijn officieel erkende nationale ombudsdiensten:

Let op: per land bestaan daarnaast meerdere bevoegde autoriteiten per onderwerp/domein (financiële diensten, privacy, zorg, consumentenrecht, enz.). De centrale instanties hieronder helpen melders bij doorverwijzing naar de juiste autoriteit of fungeren als vangnet.

België – Federale Ombudsman
Deze levert een overzicht van bevoegde autoriteiten, naar gelang het type inbreuk
• contact@federaalombudsman.be
• +32 2 289 27 27
• Leuvenseweg 48 bus 6, 1000 Brussel

Nederland – Huis voor Klokkenluiders- verwijzen naar de bevoegde autoriteit
• contact@huisvoorklokkenluiders.nl
• +31(0)88 13310 00
• Bezoekadres: Muzenstraat 89,2511 WB Den Haag.
Postadres: Postbus 85680, 2508 CJ Den Haag

Polen – Commissioner for Human Rights (Rzecznik Praw Obywatelskich, RPO)
De Ombudsman neemt meldingen in ontvangst, voert een eerste beoordeling uit en verwijst deze door naar de bevoegde publieke autoriteit.
• biurorzecznika@brpo.gov.pl
• 800 676 676
• Al. Solidarności 77, 00-090 Warszawa

Verenigd Koninkrijk – aangewezen instanties ("prescribed persons")
In het Verenigd Koninkrijk worden externe meldingen gedaan bij zogenaamde "prescribed persons". Dit zijn door de overheid aangewezen toezichthouders die bevoegd zijn om meldingen te ontvangen binnen hun specifieke domein. Het Verenigd Koninkrijk kent geen centrale autoriteit die meldingen ontvangt of doorverwijst. De melder is verantwoordelijk voor het kiezen van de juiste bevoegde instantie.
De volledige en meest actuele lijst van aangewezen instanties, inclusief hun contactgegevens, is beschikbaar via de Britse overheid: https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies

Voorbeelden van veelvoorkomende aangewezen instanties zijn:

Domain	Organisation	Contact
Telecommunicatie, media, online safety	Office of Communications (Ofcom)	Tel. 0300 123 3333 / 020 7981 3040; PO Box 1285, Warrington WA1 9GL; www.ofcom.org.uk [gov.uk]
Financiele diensten, markten, marktgedrag	Financial Conduct Authority (FCA)	Via GOV.UK prescribed list (online reporting) [gov.uk]
Mededingingsrecht	Competition and Markets Authority (CMA)	Via GOV.UK prescribed list [gov.uk]
Privacy en gegevensbescherming	Information Commissioner's Office (ICO)	Via GOV.UK prescribed list; www.ico.org.uk [gov.uk]
Welzijn op het werk	Health and Safety Executive (HSE)	Via GOV.UK prescribed list; www.hse.gov.uk [gov.uk]
Milieu & Milieuverontreiniging	Environment Agency (England)	Via GOV.UK prescribed list [gov.uk]
Belastingen, Douane, sociale zekerheid	HM Revenue & Customs (HMRC)	Via GOV.UK prescribed list [gov.uk]
Ernstige of complexe fraude, omkoping & corruptie	Serious Fraud Office (SFO)	Via GOV.UK prescribed list [gov.uk]

Politie optreden	Independent Office for Police Conduct (IOPC)	Via GOV.UK prescribed list [gov.uk]
Wangedrag van ondernemingen, insolventie, fraude door bestuurders/directie	Insolvency Service – Intelligence Team	Via GOV.UK prescribed list [gov.uk]

Frankrijk – Défenseur des droits (oriëntatie/doorverwijzing naar de bevoegde autoriteit)
De Défenseur des droits informeert melders over hun rechten, helpt bij het kiezen van het juiste externe meldingskanaal en kan meldingen doorverwijzen naar de bevoegde autoriteit (“autorité compétente”) afhankelijk van het onderwerp/domein.
• via een online formulier (site Défenseur des droits)
• +33 (0)9 69 39 00 00 (ma–vr, tijdens kantooruren; kost van een lokaal gesprek)
• Défenseur des droits – Libre réponse 71120, 75342 Paris CEDEX 07

Frankrijk – CNIL (bevoegde autoriteit: privacy/gegevensbescherming)
• depotplainte@cnil.fr
• +33 (0)1 53 73 22 22
• 3 Place de Fontenoy, TSA 80715, 75334 Paris Cedex 07

Melders die een externe melding willen doen, dienen de juiste instantie te selecteren op basis van het onderwerp van de misstand. Indien zij twijfelen, kunnen zij zich wenden tot een juridisch adviseur.

Het extern meldingskanaal zal **binnen de drie (3) maanden** of, in bijzondere gevallen, **zes (6) 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.

In geval van een melding aan een aangewezen instantie moet de klokkenluider redelijkerwijs geloven dat de verstrekte informatie in wezen waar is en dat de aangewezen instantie de juiste instantie is om de melding met betrekking tot de gemelde kwestie te ontvangen.

6 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 :

1. 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,
2. 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.

7 Waarborgen voor de positie van de melder

A. Beschermingsvoorwaarden

De melder krijgt bescherming wanneer hij gegronde redenen heeft om te geloven dat de informatie juist is en binnen het toepassingsgebied valt. Ook anonieme melders die later worden geïdentificeerd, kunnen bescherming genieten.

Niet alleen de melder, maar ook facilitators, familieleden of juridische entiteiten die aan de melder verbonden zijn, kunnen beschermd worden tegen represailles.

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.

B. 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.

C. 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 :

- schorsing, tijdelijke buitendienststelling, ontslag of soortgelijke maatregelen;
- degradatie of weigering van bevordering;
- overdracht van taken, verandering van locatie van de arbeidsplaats, loonsverlaging, verandering van de werktijden;
- het onthouden van opleiding;
- negatieve prestatiebeoordeling of arbeidsreferentie;
- het opleggen of toepassen van een disciplinaire maatregel, berisping of andere sanctie, zoals een financiële 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 omzetderving 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;
- intrekking van een licentie of vergunning;
- 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, de gedragscode van Smulders alsook schending van de gedragscode van EIFFAGE, in welk geval Smulders passende acties zal ondernemen om de melder te beschermen en om diegenen die verantwoordelijk zijn voor de represailles te sanctioneren.

Melders 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 Hoofdstuk 5 E. “INDIENEN VAN EEN MELDING VIA HET EXTERN MELDINGSKANAAL VAN DE OVERHEID’ zijn opgenomen.
De federale coördinator verifieert bij Smulders het bestaan van een redelijk vermoeden van een represaille. Smulders reageert binnen de twintig (20) dagen op het verzoek van de federale coördinator.

Wettelijke bescherming (VK)
In het Verenigd Koninkrijk hebben werknemers die een beschermde melding doen recht op wettelijke bescherming op grond van de Public Interest Disclosure Act 1998 en de Employment Rights Act 1996.
Dit omvat bescherming tegen elk nadeel dat wordt geleden op grond van het feit dat een beschermde melding is gedaan, evenals bescherming tegen automatisch onrechtmatig ontslag wanneer ontslag hoofdzakelijk plaatsvindt vanwege een dergelijke melding.

8 Misbruik van de meldingsregeling

Smulders 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.
Smulders kan evenwel niet toestaan dat melders opzettelijk meldingen indienen waarvan zij weten of geacht worden te weten dat deze onjuist zijn. Smulders 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.

9 Verwerking persoonsgegevens en uw rechten

Smulders is de verwerkingsverantwoordelijke van de persoonsgegevens in uitvoering van deze meldingsregeling. Voor klokkenluiders die in het Verenigd Koninkrijk gevestigd zijn en voor verwerkingsactiviteiten die in het Verenigd Koninkrijk plaatsvinden, moeten verwijzingen in dit beleid naar de AVG worden opgevat als verwijzingen naar de Britse AVG, zoals aangevuld door de Data Protection Act 2018.
Dit impliceert dat zowel de melder als de betrokkene bij Smulders 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 beklaagde, noch tot deze van een derde, tenzij na onderzoek blijkt dat de beklaagde 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 (politioneel/gerechtelijk/administratief) onderzoek loopt.
- De 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 Smulders 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).

De melder kan steeds terecht op het e-mailadres privacy@smulders.com wanneer de melder verdere vragen zou hebben betreffende de genomen waarborgen om de persoonsgegevens te beschermen en betreffende de verwerking van diens persoonsgegevens in het kader van de meldingsregeling of om diens recht van toegang tot, de verbetering of overdraagbaarheid van gegevens of verwijdering van diens persoonsgegevens te vragen voor zover de uitoefening van de rechten valt binnen de wettelijke voorwaarden.

Indien de melder, na contact te hebben opgenomen met Smulders, alsnog een klacht wil indienen met betrekking tot de verwerking van uw persoonsgegevens, kan de melder terecht bij de bevoegde toezichthoudende autoriteit, met name de Gegevensbeschermingsautoriteit.

De overheid die instaat voor het extern meldingskanaal handelt als verwerkingsverantwoordelijke. Dit betekent dat de melder bij externe meldingen, terecht kan bij de overheid voor de uitoefening van diens 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 of via info@firm-ifdh.be) zal de melder 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.

10 Bewaartermijn

De persoonsgegevens verwerkt in het kader van de meldingsregeling worden niet langer dan noodzakelijk voor het intern en/of extern (politioneel/gerechtelijk/administratief) onderzoek bewaard. In geval van politionele, 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.

11 Sancties

De inbreuken zoals onder andere opgesomd in "4. 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.

12 Medewerking management

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

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

13 Overige bepalingen

Deze regeling wordt binnen de twee jaar na inwerkingtreding geëvalueerd.

In de gevallen waarin de regeling niet voorziet, beslist de voorzitter van het CKI.