



HUIS VOOR  
KLOKKENLUIDERS

PUBLICATIE KENNIS & PREVENTIE

# Brochure 'Kwetsbare functies'

april 2026

# 1. OOG VOOR INTEGRITEITSRISICO'S OP HET WERK

## 1.1 INTEGRITEITSRISICO'S EN HET EFFECT VAN SCHENDINGEN

Iedere organisatie loopt risico op een integriteitsschending. De mogelijke gevolgen van integriteitsschendingen zijn divers, denk aan financiële-, materiele- en/of reputatieschade. Ook kunnen integriteitsschendingen schade aanrichten bij de betrokken medewerkers. Organisatiebreed kunnen integriteitsschendingen leiden tot minder vertrouwen van werknemers, klanten, patiënten of andere stakeholders in (de integriteit van) de organisatie.

De gevolgen van een schending kunnen groot zijn en daarom dragen organisaties een grote verantwoordelijkheid om integriteit over de gehele lijn te bevorderen en schendingen zoveel als mogelijk te helpen voorkomen. Zo beschermen zij zowel de eigen organisatie als de medewerkers en overige betrokkenen. Het is belangrijk dat een werkgever oog houdt voor bredere maatregelen, die alle werknemers en de gehele organisatie aangaan (denk aan een meldregeling, gedragscode, de inzet van vertrouwenspersonen, etc.). Daarnaast moet een werkgever ook oog hebben voor het individu. Immers, uiteindelijk is iedere integriteitsschending terug te brengen tot het doen of juist laten van een (of meerdere) individu(en). Ook wanneer zij handelen als onderdeel van een groter collectief.

### **Wat is een integriteitsschending?**

Integriteitsschendingen kunnen serieuze vormen aannemen. Het niet handelen overeenkomstig de daarvoor geldende morele waarden en normen en de daarmee samenhangende (spel)regels in een organisatie noemen we een integriteitsschending. De integriteitsschending noemen we een misstand als het maatschappelijk belang in het geding is. Dat is in het geding als de schending een of meerdere individuele belangen overstijgt en als er ook sprake is van een patroon of structureel karakter of als de handeling of nalatigheid ernstig en omvangrijk is. Elke misstand is een integriteitsschending. Andersom is dat niet altijd zo. Bij integriteitsschendingen wordt vaak gedacht aan fraude of corruptie. Een integriteitsschending is echter niet beperkt tot misbruik van (financiële) middelen. Denk ook aan het misbruiken van zakelijke contacten voor privédoeleinden of het verstrekken van informatie of andere gunsten die een waarde vertegenwoordigen, zoals het verlenen van een vergunning. Al deze vormen van integriteitsschendingen kunnen zich voordoen hoe groot het risico is, hangt onder meer af van de functie en de middelen of bevoegdheden die aan een medewerker zijn toegekend.

## 1.2 PROCESSEN VERSUS HET INDIVIDU

Deze brochure richt zich op risicobeheersing op het gebied van integriteit. Hierin is het identificeren en beoordelen van risico's op **procesniveau** de meest gangbare wijze. We nemen de individuele medewerkers als startpunt en kijken naar integriteitsrisico's op **functieniveau**. Door integriteitsbeleid te richten op de werknemer neemt de werkgever

diens verantwoordelijkheid op het gebied van goed werkgeverschap<sup>1</sup>. Zo kan de werkgever gericht beheersmaatregelen nemen en maakt hij zowel de organisatie als werknemers weerbaarder tegen integriteitsrisico's.

De impact van een integriteitsschending door een medewerker hangt onder meer af van de mate waarin die schade kan aanrichten in diens functie. Immers, verduistering door een medewerker die geautoriseerd is om de zakelijke rekeningen van een onderneming te beheren kan potentieel meer (financiële) schade aanrichten dan een medewerker die geen directe toegang heeft tot zakelijke rekeningen.

Of een medewerker in de toekomst misbruik zal maken van zijn bevoegdheden of van de middelen die de werkgever hem ter beschikking stelt, laat zich moeilijk voorspellen. Het is niet de bedoeling dat een werkgever al zijn medewerkers op voorhand als onbetrouwbaar ziet en met argwaan benadert. Dit kan een negatief effect hebben op de organisatiecultuur. Wel zijn er vaak kwetsbaarheden aan te wijzen die het risico op een integriteitsschending vergroten. Soms liggen deze verscholen in de organisatie zelf (niet of niet juist toepassen van vier-ogen principe), soms bij de werknemer (wanneer deze bijvoorbeeld financiële problemen heeft). Het is zowel in het belang van de organisatie als de werknemer dat de werkgever deze kwetsbaarheden detecteert, erkent en zoveel mogelijk wegneemt. In het volgende hoofdstuk wordt middels een plan van aanpak toegelicht hoe een werkgever dit kan doen.

---

<sup>1</sup> Artikel 7:611 van het Burgerlijk Wetboek.

*De werkgever en de werknemer zijn verplicht zich als een goed werkgever en een goed werknemer te gedragen.*

## 2. EEN ANALYSE OP FUNCTIENIVEAU

### HET PLAN VAN AANPAK

Om medewerkers weerbaarder te maken tegen integriteitsrisico's is het belangrijk om hen bewust te maken van de mogelijke integriteitsrisico's die kleven aan de werkzaamheden die zij vervullen. Als er organisatiebreed en op individueel niveau bewustzijn is over de integriteitsrisico's van bepaalde functies in een organisatie, dan kunnen zowel directie als medewerker zich makkelijker voorbereiden en maatregelen nemen om risico's te vermijden of te verminderen. In het vervolg van deze publicatie doorlopen we aan de hand van een voorbeeld (zie **kader 1**) verschillende stappen die helpen bij het in kaart brengen van integriteitsrisico's op functieniveau. Dit doen we in een aantal stappen:

1. Identificeren van de **verschillende functietypen** binnen een organisatie;
2. Per functietype in kaart brengen welke **taken** en **bevoegdheden** risicogevoelig zijn voor misbruik door de medewerker(s) of (een) derde(n);
3. Identificeren van de **kwetsbaarheden** die kunnen bijdragen aan een toename van dit risico;
4. Inventariseren van **bestaande maatregelen** die dit risico verminderen;
5. Bepalen welke **maatregelen** nog moeten worden genomen om het risico te verminderen.

#### Tip!

Het kritisch bekijken van functies en handelen doet u bij voorkeur op periodieke basis. Sommige risico's zijn namelijk situationeel en contextafhankelijk. Ook kunnen er ontwikkelingen zijn in het (privé)leven van een medewerker wat hem op een moment kwetsbaarder maakt in de uitoefening van zijn functie dan het geval was ten tijde van zijn aanstelling. Daarnaast kunnen bijvoorbeeld de verandering van een functie, de interne processen of een bepaalde ontwikkeling in de maatschappij aanleiding vormen om risico's opnieuw in kaart te brengen. Een goede manier om dit in te richten is door minimaal een keer per jaar met medewerkers te spreken over of er iets veranderd is in hun (thuis)omstandigheden of werkzaamheden. Bespreek met de medewerkers welke impact deze verandering heeft op hun werk.

### STAP 1: DE FUNCTIES IN KAART BRENGEN

Voor het doorlopen van deze stappen is het belangrijk om (indien aanwezig) functieprofielen te raadplegen. Bij afwezigheid van een functieprofiel kunnen vacatureteksten met beschrijving van taken worden geraadpleegd. Hiermee wordt de papieren werkelijkheid van een functie in kaart gebracht. Vervolgens is het belangrijk te toetsen of dit overeenkomt met de praktische werkelijkheid. Dat kan door meerdere personen op de afdeling te spreken en inzicht te krijgen in de interne verhoudingen, tussen functies onderling, en externe verhoudingen, met stakeholders buiten de organisatie. Zo ontstaat een beeld van wat een medewerker zou moeten doen en wat daadwerkelijk bij een functie komt kijken. Dit is een belangrijk startpunt om te bepalen of de organisatiebelangen voldoende beschermd zijn en of de werkgever ook de medewerker voldoende beschermt vanuit het oogpunt van goed werkgeverschap.

### Voorbeelden in deze brochure

In dit document wordt de voorbeeldcasus gebruikt van een vertegenwoordiger die namens een bedrijf producten en diensten verkoopt aan potentiële nieuwe klanten. In het voorbeeld gaat het steeds om één **werkgebied** en **risico** waarop de activiteiten van deze vertegenwoordiger betrekking hebben, zodat het voorbeeld overzichtelijk blijft. Bij iedere stap wordt de tabel verder ingevuld, met hierbij een toelichting. Wanneer u zelf met de analyse aan de slag gaat, zult u verschillende **werkgebieden, risico's** en **maatregelen** per functie herkennen. Ook de vertegenwoordiger heeft namelijk een breder takenpakket, welke aan verschillende werkgebieden raakt. In eerste instantie ligt het, gezien het vele contact met klanten, voor de hand om te denken aan risico's die gerelateerd zijn aan corruptie en het geven/ontvangen van giften. Maar denk ook aan zijn rol in de financiële administratie: de vertegenwoordiger heeft contact met de financiële afdeling over de afhandeling van facturen. Ook declaratiegedrag kan een risicogebied zijn, zeker wanneer de vertegenwoordiger vaak alleen reist. Hierbij passen verschillende risico's en maatregelen. Een niet-uitputtende lijst met voorbeelden van werkgebieden, taken, bevoegdheden, kwetsbaarheden en maatregelen vindt u in de [bijlage](#).

## STAP 2: IDENTIFICEER RISICOVOLLE TAKEN EN BEVOEGDHEDEN

Om te bepalen welke taken en bevoegdheden, die bij een functie horen, risicogevoelig zijn, is het belangrijk om te bedenken of het (al dan niet) uitvoeren of inzetten van een taak of bevoegdheid een bepaalde waarde vertegenwoordigt in het economische verkeer of voor bepaalde groepen in de maatschappij. Dat maakt deze taken en bevoegdheden namelijk aantrekkelijk voor verschillende vormen van misbruik.

Een medewerker die toegang heeft tot financiële middelen van een onderneming, bijvoorbeeld in het kader van het overboeken van transacties uit naam van een onderneming, kan zelf in de verleiding komen tot misbruik van deze bevoegdheid en is een aantrekkelijk doelwit voor derden (denk aan *phishing*). Uit de omvang van de geldstromen is makkelijk een waarde toe te kennen aan de bevoegdheid van de medewerker. Die waarde is moeilijker uit te drukken wanneer het gaat om een medewerker die databases met gevoelige data beheert. Ook iets ogenschijnlijk eenvoudigs als het uitgeven van paspoorten kan een integriteitsrisico opleveren wegens de waarde die een authentiek paspoort vertegenwoordigt voor criminelen. Organisaties moeten alert zijn op functies waar het werken met klantgegevens (zoals adressen, BSN-nummers) of bedrijfs- of concurrentiegevoelige gegevens onderdeel van uitmaakt.

Wanneer we letten op risicovolle taken en bevoegdheden moeten we niet alleen de blik naar buiten richten. Ook bevoegdheden ten opzichte van ander personeel kan een risico zijn. Bijvoorbeeld wanneer een medewerker vanuit zijn of haar functie autorisaties aan andere collega's kan verlenen of een leidinggevende die de bevoegdheid heeft om nieuwe collega's aan te nemen.

Iedere functie in een organisatie kan dus (andere) integriteitsrisico's met zich meebrengen. In de voorbeeldcasus die in deze brochure gebruikt wordt (zie het blauwe kader hierboven), is er zowel sprake van een intern als een extern integriteitsrisico bij de functie van 'vertegenwoordiger'. In de tabel ziet u ten eerste het **werkgebied** waar de functie zich in bevindt, de specifieke **situatie** waarin integriteitsrisico's kunnen ontstaan en het mogelijke **risico** dat aan deze situatie verbonden is.

<b>Naam functie:</b> vertegenwoordiger		
<b>Taken:</b> verkopen van producten en diensten, identificeren van mogelijke afnemers en afzetmarkten in binnen- en buitenland.		
Werkgebied	Situatie	Mogelijk risico
Contacten met derden	<b>Medewerker is verantwoordelijk voor het contact met en de aanname van nieuwe klanten</b>	<b>Medewerker accepteert malafide klant door manipulatie</b>

**Toelichting:** In deze tabel richten we ons op de risico's die bestaan in de contacten die de vertegenwoordiger heeft met klanten. In deze voorbeeldcasus is de vertegenwoordiger verantwoordelijk voor het onderhouden van contact met bestaande klanten en de aanname van nieuwe klanten. Veel organisaties hebben een aannamebeleid voor nieuwe klanten. Enerzijds om zicht te hebben op de handelsketen (voorkomen dat u via de keten bijdraagt aan of geassocieerd wordt met bijvoorbeeld misstanden). Andere redenen zijn, bijvoorbeeld, om te bepalen of een nieuwe klant in staat is om (langdurig) verplichtingen na te komen, of een klant past binnen de waarden waar de organisatie zich aan verbindt en te bepalen of een nieuwe klant wel bestaat. In het voorbeeld is een van de geïdentificeerde risico's dat de vertegenwoordiger zich verleidt of laat verleiden tot het aannemen van klanten die niet binnen het aannamebeleid van de organisatie passen. Een ander risico is dat de vertegenwoordiger bestaande klanten een te gunstig tarief verleent, welke niet past binnen het beleid van de organisatie. Een te hechte band met de klant, of bepaalde voordelen die door de klant in het vooruitzicht worden gesteld zouden de vertegenwoordiger hiertoe kunnen verleiden.

### STAP 3: (H)ERKEN KWETSBAARHEDEN

Wanneer een functie zich afspeelt binnen één of meer kwetsbare werkgebieden, dan is het belangrijk om te in kaart te brengen welke omstandigheden ertoe kunnen leiden dat er een verhoogd risico bestaat op een integriteitsschending. Deze omstandigheden noemen we ook wel 'red flags', omstandigheden die de kwetsbaarheid van een functie verhogen.

Kwetsbaarheden kunnen zowel van organisatorische als individuele aard zijn. De medewerker die meer uitgeeft dan hij verdient en met loonbeslag wordt geconfronteerd (individuele kwetsbaarheid) zal alle mogelijkheden om uit zijn moeilijke financiële situatie te raken overdenken en, in het uiterste geval, mogelijk aangrijpen. Dat betekent dat ook minder gewenste oplossingen, zoals fraude plegen of openstaan voor corruptie, niet (langer) zijn uitgesloten.

Ook de wijze waarop het werk is georganiseerd, heeft directe invloed op de integriteit van de medewerkers. Met name medewerkers die een rol spelen in kwetsbare processen (bijv. met gevoelige data of geld) of in een machtspositie horen precies te weten wat voor taken zij moeten uitvoeren en/of welke verantwoordelijkheden en bevoegdheden zij daarbij hebben. Vaagheid en onduidelijkheid kunnen leiden tot een grote vrijheid van handelen zonder duidelijke grenzen (organisatorische kwetsbaarheid).

Enkele voorbeelden van mogelijke kwetsbaarheden (organisatorisch en individueel) vindt u hieronder, een langere lijst is te vinden in de [bijlage](#) :

Kwetsbaarheden	
Complexiteit	Ingewikkelde constructies (juridisch/fiscaal), onoverzichtelijke (productie)keten
Verandering/dynamiek	Sterke groei/krimp, crisissituaties
Management	Houding & (voorbeeld)gedrag management, tone at the top
Persoonlijkheidskenmerken en situatie medewerker	(Gok)verslaving, gevoel onheus behandeld te zijn
Probleemhistorie	Werkachterstand, integriteitsincidenten, 'slechte' cultuur

Naam functie: Vertegenwoordiger Taken: vervoeren van goederen of personen, beheer van voertuig, soms contact met klanten of leveranciers.			
Werkgebied	Situatie	Mogelijk risico	Kwetsbaarheden
Contacten met derden	Medewerker is verantwoordelijk voor het contact met en de aannahme van nieuwe klanten	Medewerker accepteert malafide klant door manipulatie	<b>Financiële bonus per aangedragen klant</b>

**Toelichting:** In het geval van de vertegenwoordiger zijn er verschillende kwetsbaarheden aan te wijzen die als trigger kunnen dienen voor de vertegenwoordiger om het aannamebeleid te negeren. Waar de vertegenwoordiger onder normale omstandigheden niet zou zwichten voor bijvoorbeeld geschenken van potentiële klanten, zou hij wellicht wel overstag gaan indien er sprake is van een beloningsbeleid waarin prikkels zijn opgenomen. Denk aan een financiële bonus voor de vertegenwoordiger per klant die hij aandraagt. Een dergelijk beloningsbeleid is een voorbeeld van een organisatorische kwetsbaarheid. Er zijn ook persoonlijke kwetsbaarheden aan te wijzen. Denk aan een kwetsbaarheid in de persoonlijkheid van de vertegenwoordiger. Iemand die veel belang hecht aan macht en status zou zich sneller door een klant kunnen laten beïnvloeden dan een medewerker die daar niet of minder gevoelig voor is.

#### STAP 4: BESTAANDE MAATREGELLEN IN KAART BRENGEN

Om de organisatie en medewerkers weerbaarder te maken tegen integriteitsrisico's, is het nodig dat een organisatie maatregelen neemt. Maatregelen kunnen variëren in reikwijdte en insteek. Vaak zijn er al enkele maatregelen genomen. Soms zonder dat deze maatregelen expliciet gelinkt zijn aan de specifieke risico's van een functie. Maatregelen kunnen generiek (organisatiebreed) of specifiek (op een functie gericht) zijn. Beiden zijn belangrijk en vereisen doorlopend aandacht.

##### SOORTEN MAATREGELLEN: REIKWIJDTE

- Bij **generieke maatregelen** gaat het om maatregelen die gericht zijn op het gehele personeelsbestand. Bijvoorbeeld onderdelen van de integriteitsinfrastructuur die gericht zijn op het stimuleren van een veilige werkomgeving waarin medewerkers geen drempels ervaren om eventuele bezorgdheden te uiten en te melden wanneer zij een integriteitsschending vermoeden.

- **Specifieke maatregelen** zijn bedoeld om de weerbaarheid van een bepaald werkgebied of taak te verbeteren of om concrete functiespecifieke risicofactoren te verminderen. U kunt hierbij denken aan een strengere screening bij medewerkers met risicovolle taken of invoeren van het vierogenprincipe bij bepaalde taken.

#### SOORTEN MAATREGELLEN: INSTEEL

- **Preventieve** maatregelen hebben als doel risico's te voorkomen en verminderen.
- **Controlerende** maatregelen zijn bedoeld om te achterhalen of bepaalde risico's zich voordoen.
- **Remediërende** maatregelen kunnen gebruikt worden om situaties te herstellen waarin risico's zich voordoen.

Maatregelen moeten regelmatig tegen het licht worden gehouden om te checken of ze nog afdoende zijn. Verder moeten de maatregelen uiteraard toepasbaar zijn en effectief worden toegepast. Er is wellicht niet direct zicht op alle maatregelen die er in een organisatie bestaan. Het is daarom belangrijk om in gesprek te gaan met het betreffende team, de leidinggevende en vakspecialisten om goed op de hoogte te zijn van de maatregelen. Houdt hierbij ook rekening met ongeschreven regels op de werkvloer en de cultuur binnen teams. Ook dergelijke aspecten kunnen bijdragen aan het verminderen van risico's. Wanneer u een goed overzicht heeft kunt u in de volgende stap effectief verder gaan met het aanscherpen of updaten van bestaande maatregelen en werk maken van passende maatregelen waar die nog ontbreken.

Naam functie: Vertegenwoordiger				
Taken: Nieuwe klanten binnenhalen en onderhouden bestaande relaties.				
Werkgebied	Situatie	Mogelijk risico	Kwetsbaarheden	Preventieve maatregelen
Contacten met derden	Medewerker is verantwoordelijk voor het werven en de aanneming van nieuwe klanten	Medewerker accepteert malafide klant door manipulatie	Financiële bonus per aangedragen klant	<b>Verplicht advies van de juridische afdeling</b>

**Toelichting:** In het voorbeeld blijkt uit de inventarisatie dat er al preventieve maatregelen aanwezig zijn. Een hiervan is een verplicht advies van de juridische afdeling op het moment dat een klant wordt aangenomen. Hierdoor wordt de bevoegdheid van de vertegenwoordiger voor een deel ingeperkt.

#### STAP 5: NIEUWE MAATREGELLEN AANWIJZEN

Nu in kaart is gebracht welke taken en bevoegdheden risicogevoelig zijn voor misbruik, welke factoren kunnen bijdragen aan extra kwetsbaarheid voor integriteitsrisico's en welke maatregelen jouw organisatie al genomen heeft om integriteitsrisico's te verminderen, is het belangrijk om te beoordelen of de risico's voldoende vermeden en/of verminderd zijn.

Of geïdentificeerde maatregelen doeltreffend zijn, hangt af van omstandigheden zoals de **samenhang** met bestaande maatregelen en de **organisatiecultuur**. Daarnaast is het van belang dat maatregelen **bekend** zijn bij degenen die het betreft en dat de maatregelen **actueel** zijn.

Vaak kunnen organisaties al met kleine aanpassingen integriteitsrisico's verminderen. Bijvoorbeeld door een bepaalde (controle)taak bij een andere functionaris te beleggen. Zo

kan een organisatie die interne controles uitvoert op de geldstromen bijkomende maatregelen nemen door te zorgen dat het beslissings- en controleproces voor de uitgaven niet bij één persoon ligt, maar dat er tenminste twee mensen op verschillende momenten in het proces de nodige controles doen. Dit is een voorbeeld van **functiescheiding**. Zie voor een omvangrijke (niet uitputtende) lijst met voorbeelden van maatregelen de bijlage.

Wanneer u nieuwe maatregelen toevoegt, bedenk dan goed of deze maatregelen qua zwaarte passend zijn bij de risico's (**proportioneel**) en ga na of er minder ingrijpende maatregelen zijn die hetzelfde effect kunnen beogen (**subsidiar**). U wilt medewerkers niet onnodig belasten met controles en moet waken voor onnodige inbreuken op de privacy van medewerkers.

In het geval van de accountmanager kunnen bijvoorbeeld de volgende extra maatregelen genomen worden: een verplichte screening van nieuwe klanten door een andere afdeling/medewerker dan de vertegenwoordiger, de aanwezigheid van twee medewerkers bij cruciale onderhandelingen met de potentiële klant.

### TOT SLOT: ZELF AAN DE SLAG

De hierboven beschreven aanpak is toepasbaar op organisaties binnen verschillende branches en sectoren, onafhankelijk van de grootte van het personeelsbestand. Waar in kleine organisaties de vermenging van functies bij verschillende medewerkers een uitdaging is, is het bij een grote organisaties een uitdaging om alle activiteiten gerelateerd aan de verschillende functies in kaart te brengen. Het is in dat geval een optie om bijvoorbeeld met de functies binnen een bepaalde afdeling te beginnen. De aanpak zal in de praktijk op bepaalde punten kunnen afwijken, maar het is belangrijk om alle beschreven stappen in de eigen organisatiespecifieke aanpak terug te laten komen.

Daarnaast is het van belang om de analyse **preventief** in te zetten. Dat wil zeggen; liefst nog voordat er signalen zijn van mogelijke integriteitsschendingen. Juist dan is een organisatie in staat om risico's op een zo vroeg mogelijk stadium te signaleren en actie te ondernemen. Daarmee kan deze analyse zo efficiënt mogelijk worden ingezet als instrument om te helpen integriteitsschendingen en misstanden te voorkomen.

Wie de analyse uitvoert, is afhankelijk van de wijze waarop de organisatie is ingericht en de aanwezige expertises. In grotere organisaties ligt het voor de hand dat een functionaris belast met toezicht op integriteitsbeleid of een medewerker van de Risk & Control, of vergelijkbare, afdeling de analyse uitvoert. Belangrijk is dat er inzicht is in de verschillende functies en processen, en er kennis aanwezig is over (het inschatten) van integriteitsrisico's. Een kleine werkgroep instellen om verschillende expertises bij elkaar te brengen kan leiden tot een betere analyse. Kleine organisaties kunnen overwegen externe expertise in te schakelen.

Een ander aandachtspunt is het op een zodanige wijze inrichten van het proces dat er kritisch en constructief wordt gekeken naar de zwakke plekken binnen functies. Het mag geen afvink oefening of knip-en-plakwerk worden. Daarom heeft het Huis ervoor gekozen om geen volledig uitgewerkte analyse te gebruiken. Voor wie op zoek is naar inspiratie en enkele voorbeelden van werkgebieden, taken, bevoegdheden, kwetsbaarheden en maatregelen is, zoals eerder beschreven, een **bijlage** met voorbeelden beschikbaar.

### **Over het Huis voor Klokkenluiders**

Het Huis voor Klokkenluiders is een organisatie die zich bezig houdt met alles rondom klokkenluiden en integriteit. Van advies tot hulp, van onderzoek tot preventie. Wilt u meer weten? Onze website is een bron van informatie voor zowel werkgever als werknemers en beleidsmakers. U kunt ons vinden op <http://www.huisvoorklokkenluiders.nl>.

Dit is een uitgave van het Huis voor Klokkenluiders.

### **Contactgegevens**

Muzenstraat 89-91, 2511 WB Den Haag

Telefoon: 088-13 31 000

E-mail: <mailto:info@huisvoorklokkenluiders.nl>

© Huis voor Klokkenluiders, april 2026

[www.huisvoorklokkenluiders.nl](http://www.huisvoorklokkenluiders.nl)

