Reactie internetconsultatie AMvB namens De Integriteitscoördinator BV

Rotterdam, 14 mei 2024

Betreft: reactie consultatie AMvB anoniem melden vermoedens van misstanden.

De Integriteitscoördinator B.V. (hierna: De Integriteitscoördinator) is een onafhankelijke, externe coördinator van klokkenluider- of speak-up procedures. Daarnaast geven wij cursussen hierover. Wij maken graag gebruik van de mogelijkheid om te reageren op de concept-AMvB 'Anoniem melden bij de werkgever van vermoedens van misstanden' en de bijbehorende Nota van toelichting.

Voordat we dit doen moet ons wel iets van het hart. In het begeleidende BK formulier wordt de vraag aan welke duurzame ontwikkelingsdoelen dit bijdraagt beantwoordt met: "niet van toepassing"[1]. Dit lijkt ons onjuist. Ontwikkelingsdoel nummer 16 betreffende 'Peace, Justice and Strong Institutions' lijkt ons wel degelijk van toepassing. Door de mogelijkheid te creëren om anoniem bij onafhankelijke functionarissen mogelijke misstanden te melden wordt bijgedragen aan de doelstellingen van rechtvaardigheid en sterke instituties, alsmede aan andere duurzame ontwikkelingsdoelen als bescherming van de veiligheid, gezondheid, het milieu, welzijn en dergelijke[2]. Het gaat hier om grote maatschappelijke belangen.

Observaties

Helaas merken we in onze praktijk dat de Wet bescherming klokkenluiders (Wbk) op dit moment nog steeds onderbelicht is. Hopelijk gaat de verplichting om anonieme meldkanalen in te richten zorgen voor meer aandacht voor de Wbk.

De Integriteitscoördinator bestaat inmiddels vier jaar, maar onze medewerkers hebben al meer dan 15 jaar ervaring met anonieme meldkanalen en hebben honderden meldingen behandeld. Wij zijn een groot voorstander van het aanbieden van anonieme meldkanalen. De belangrijkste reden om niet te melden is vaak angst voor vergelding. Echter, als je niet weet wie er heeft gemeld, dan kun je ook geen maatregelen nemen tegen deze persoon. Het aanbieden van de mogelijkheid om anoniem te melden werkt drempelverlagend. Uit de literatuur[3] en uit onze eigen ervaring weten we dat een substantieel aantal meldingen door anonieme melders wordt ingediend. Waarschijnlijk zou een groot aantal van deze meldingen niet ingediend worden als er geen anonieme meldkanalen worden

[1] Zie hulpvraag 2b van het Beleidskompasformulier voor internetconsultatie.
[2] Dit wordt nog geïllustreerd doordat grote ondernemingen binnenkort verplicht worden om te rapporteren over hun meldkanalen in het kader van hun ESG-rapportage, bijvoorbeeld als gevolgd van de CSRD en CSDDD.
[3] Zie bijvoorbeeld 'Navex Whistleblowing & Incident Management Benchmark Report 2024' of de rapportages van individuele ondernemingen. Vaak zijn meer dan 50% van de meldingen van anonieme melders.

aangeboden. En dan wordt de kans kleiner dat mogelijke misstanden in een vroeg stadium ontdekt en geadresseerd kunnen worden.

Tegelijkertijd is het ook onze ervaring dat anonieme meldingen moeilijker te onderzoeken zijn. Zeker als er na de melding geen mogelijkheid meer is om te communiceren met de melder. Het Huis voor klokkenluiders (verder: het Huis) geeft dit ook aan in hun reactie van 26 april 2024. Dit kan ervoor zorgen dat een terechte melding ten onrechte wordt afgedaan als 'niet onderzoek waardig'. Het helpt als de mogelijkheid bestaat tot het voeren van een dialoog met anonieme melders, zodat er om aanvullende informatie of verduidelijking gevraagd kan worden. Maar ook om aan te geven dat de onderzoeksmogelijkheden beperkter zijn als er geen hoor en wederhoor kan plaatsvinden. Overigens is het onze ervaring dat sommige anonieme melders tijdens het meld- en onderzoeksproces zoveel vertrouwen krijgen in de procedure, dat ze alsnog besluiten om hun identiteit te onthullen. Ook daarom is het belangrijk dat er een mogelijkheid tot communicatie met anonieme melders bestaat.

Derhalve stellen wij dat communicatie met de anonieme melder cruciaal is voor een correcte en volledige opvolging van de melding[4]. En dat kan het gemakkelijkst via gespecialiseerde software[5].

Aan de anonieme melder horen dezelfde rechten toe te komen als aan de niet anonieme melder. Deze dient dus ook een ontvangstbevestiging te ontvangen en feedback te krijgen van de onafhankelijke functionaris die de melding opvolgt[6]. Wij voorzien hierbij problemen als dit niet via gespecialiseerde software verloopt. Sommigen hebben aangegeven dat een ontvangstbevestiging aan een anonieme klokkenluider wel publiekelijk gedaan kan worden, bijvoorbeeld via het intranet van de organisatie of een email aan alle medewerkers vanuit de directie. Het is echter niet altijd zeker dat een anonieme melding van een medewerker afkomstig is. En aangezien een ontvangstbevestiging van een melding van een gekende klokkenluider ook niet publiekelijk gedaan wordt, lijkt het De Integriteitscoördinator vreemd om dit anders in te richten ten aanzien van een anonieme melder. Belangrijker nog, een dergelijke publicatie kan veel onrust veroorzaken in de organisatie en het onderzoek bemoeilijken. Het is juist de rol van de onafhankelijke functionaris om de melding en het onderzoek vertrouwelijk te houden. Dit is ook in het belang van de beschuldigde(n), die natuurlijk ook rechten hebben. Als de melding niet bewezen kan worden, dan ondervinden deze personen daar zo min mogelijk schade van. De rol van de onafhankelijke functionaris, als centraal communicatie- en coördinatiepunt, is hierbij cruciaal.

Wij zijn ook geen voorstander van een speciale postbus die wordt neergezet in de organisatie of van het versturen van fysieke brieven. Zoals ook het Huis signaleert, brengt het melden via een analoog systeem beperkingen met zich mee, die de mogelijkheid voor het waarborgen van een anonieme melding kunnen bemoeilijken. Bovendien: volgens de EU-richtlijn dienen de meldkanalen dusdanig beveiligd te zijn dat zij de vertrouwelijkheid van de identiteit van de melder en van eventuele in de melding genoemde derden beschermen. Niet-gemachtigde personeelsleden mogen geen toegang hebben tot deze gegevens[7]. Deze bepaling is helaas niet overgenomen in de Wbk, maar geldt natuurlijk wel. Bij de anonieme meldkanalen is dit nog belangrijker. Het lijkt ons dat analoge meldkanalen in de praktijk onvoldoende beveiligd kunnen worden.

Als meldingen op digitale wijze ingediend worden via de website van de organisatie, is via het IP-adres vaak wel te achterhalen wie de melding heeft ingediend. Als de melding wordt ingediend via

---

[4] Zie ook dit rapport van de Universiteit Utrecht in opdracht van het Huis voor klokkenluiders, waaruit duidelijk naar voren komt hoe belangrijk de communicatie tussen alle betrokkenen is.
[5] Wij zijn zelf geen fabrikant van dergelijke software maar helpen onze klanten vaak wel bij de selectie.
[6] Zie artikel 9, lid 1c van de EU-richtlijn 2019/1937 inzake de bescherming van klokkenluiders.
[7] Zie artikel 9, lid 1a van de EU-richtlijn.

een, speciaal daarvoor aangemaakt, anoniem email adres dan is dit doorgaans ook wel te achterhalen. Al was het maar door de aanbieder van de email adressen. Bovendien kan de IT-manager van de organisatie zich dan vaak nog wel toegang verschaffen tot de melding, al dan niet op instructie van een hogere leidinggevende.

De werkgever wordt (vanuit het oogpunt van De Integriteitscoördinator) bij de inrichting van deze meldprocedure, door de inbreng van de verplichting van de mogelijkheid tot anoniem melden, wel haast verplicht om te werken met software, omdat er anders onvoldoende waarborgen zijn om daadwerkelijk anoniem te kunnen melden. Een bijkomend voordeel hiervan is overigens, dat de organisatie dan meteen beschikt over een centraal register van alle meldingen, wat ook een wettelijke eis is. Deze software kent tegenwoordig vaak ook de mogelijkheid om een mondelinge boodschap in te spreken, waarbij de stem dusdanig vervormd kan worden, dat de melder anoniem blijft. Er kan dan zowel schriftelijk als mondeling anoniem gemeld worden.

Wij zijn ons ervan bewust dat een abonnement op dergelijke software een kostenverhogende factor is. Echter, voor € 50- € 100 per maand kan elke organisatie een abonnement nemen op een basis-versie van meldsoftware die aan de basiseisen voldoet. De kosten kunnen nog verder gedrukt worden als er vanuit een brancheorganisatie of koepelvereniging een gezamenlijke faciliteit wordt aangeboden.

Vanuit het perspectief van De Integriteitscoördinator is de enige mogelijkheid om anoniem analoog te melden in de praktijk mondeling via een onafhankelijke interne Ethics & Compliance Officer/Integriteitsmanager of via een (externe) persoon. De onafhankelijkheid van deze interne Ethics & Compliance Officer/Integriteitsmanager dient dan wel goed gewaarborgd te worden[8]. Bijvoorbeeld door middel van een onafhankelijkheidsstatuut en een meervoudige rapportagelijn. Dit moet meer zijn dan een papieren exercitie; het moet geloofwaardig zijn naar de medewerkers toe. Om de onafhankelijkheid verder te waarborgen, zou deze persoon bij voorkeur geen andere functie binnen de organisatie moeten bekleden[9]. Voor kleinere organisaties is dit vaak geen haalbare optie. Zij kunnen deze rol het beste uitbesteden aan een externe functionaris.

Zoals aangegeven in de AMvB, zou deze interne of externe functionaris zich dan wel op voldoende wijze moeten hebben geschoold om de taak op een correcte wijze uit te kunnen voeren. Daar zijn wij het mee eens. Deze persoon vervult een cruciale rol en dient daarbij over de nodige kennis van de Wet bescherming klokkenluiders en overige relevante wetgeving te beschikken. Het helpt natuurlijk ook als de functionaris de nodige ervaring heeft met het behandelen van meldingen en het management en de melder kan begeleiden in dit proces. De complexiteit van deze functie wordt nog wel eens onderschat[10].

---

[8] Zie ook dit artikel in het Journal of Business Ethics van Smaili, Vandekerckhove en Arroyo Pardo (2023), waarin het belang van de onafhankelijkheid van de rol wordt onderstreept, een pleidooi wordt gehouden voor versterking van deze functie en aangegeven wordt dat de complexiteit van de functie vaak onderschat wordt.

[9] Op zich zou een Functionaris Gegevensbescherming of een Interne Auditor ook een dergelijke rol kunnen spelen. Echter, de Functionaris Gegevensbescherming gaat dan zelf – soms gevoelige – persoonsgegevens verwerken. En de Interne Auditor zou dan de klokkenluiderprocedure niet meer kunnen auditen. Daarom zien deze functies vaak af van deze rol. Een advocaat in dienstbetrekking zou deze rol ook kunnen vervullen. Maar wordt deze wel vertrouwd door de medewerkers, als een medewerker in een rechtszaak soms tegenover deze advocaat kan komen te staan? Een uitzondering vormt wellicht nog een onafhankelijke Kwaliteitsmanager in een productieomgeving, die de autoriteit heeft om de processen stil te leggen als het product niet aan de eisen voldoet.

[10] Zie ook het artikel genoemd in voetnoot 8.

Het Huis heeft aangegeven dat het gebruik van de open normen met betrekking tot de eisen aan de functionarissen kan leiden tot een anonieme meldprocedure die met onvoldoende waarborgen omkleedt is. Ook wij zijn van mening dat dit een probleem kan zijn voor kleinere organisaties waarbij de functie intern belegd wordt. In een kleine organisatie waar zelden meldingen plaatsvinden, kan immers moeilijk voldaan worden aan de vereiste dat de functionaris 'voldoende ervaren' is. Dit gebrek aan ervaring kan leiden tot een risico voor zowel de positie van de melder als voor de positie van de functionaris. Ook dit pleit dan vóór uitbesteding van deze rol.

Gelet op het maatschappelijk belang van dit onderwerp, de impact die de meldingen en de onderwerpen van de meldingen (kunnen) hebben op de levens van de betrokkenen maar ook op het goed functioneren of zelfs voortbestaan van de werkgever, dient er vanuit ons oogpunt meer houvast gegeven te worden met betrekking tot de invulling van de rol van de functionaris.

Daarnaast is het van belang dat er meer duidelijkheid komt over de rechtspositie van de functionaris die de meldingen in ontvangst moet nemen en opvolgen. Zo is de functionaris die volgens artikel 2, lid 2 onder d het vermoeden van een misstand in ontvangst neemt en/of opvolgt beschermd tegen benadeling zoals beschreven in artikel 17ec. Dit zou ook moeten gelden voor de functionarissen die de anonieme meldingen in ontvangst nemen en opvolgen, conform artikel 2, lid 2 onder e. Om de anonimiteit bij analoge meldingen écht te waarborgen, zou deze functionaris bovendien een verschoningsrecht moeten krijgen in juridische procedures. Ons inziens zou dat overigens ook moeten gelden voor de functionaris(sen) uit artikel 2, lid 2 onder d, om de vertrouwelijkheid van die meldingen echt te waarborgen.

Aandachtspunten

Vanuit de Integriteitscoördinator zijn er een aantal aandachtspunten die wij van belang achten bij de verdere ontwikkeling van deze wetgeving.

Zoals hierboven aangehaald, dient er meer aandacht uit te gaan naar de positie van de functionaris die de -al dan niet analoge - meldingen moet ontvangen en verwerken. De Integriteitscoördinator vindt het belangrijk dat deze functionaris echt onafhankelijk is, over voldoende ondersteunende middelen beschikt en deskundig en ervaren is.

In artikel 3 van de concept-AMvB wordt aangegeven dat hiertoe tenminste één functionaris wordt aangesteld die niet tevens werkzaam is in een leidinggevende functie, dan wel een functie die primair betrokken is bij het werven, aannemen en ontslaan van medewerkers binnen de organisatie van de werkgever. Wij nemen aan dat het de bedoeling is dat de directie en de P&O-afdeling deze functie niet mogen vervullen. Het kan namelijk ook nog zo gelezen worden dat een werkgever ook de algemeen directeur én iemand van P&O aanstelt als mogelijke meldkanalen. Dat lijkt ons niet de bedoeling, aangezien beiden niet onafhankelijk zijn.

Wij zien graag dat er een duidelijk kader geschetst wordt voor de organisaties, waarin de eisen aan maar ook de waarborgen voor deze functionaris zijn opgenomen. Deze functionarissen moeten zich voor de activiteiten die zij uitvoeren binnen deze functie namelijk vrijuit kunnen spreken en niet onder druk gezet (kunnen) worden ten aanzien van hun eigen positie. Voor de interne functionaris kan een onafhankelijkheidsstatuut en een meervoudige rapportagelijn hierbij helpen. Voor kleinere organisaties ligt het voor de hand dat deze rol geoutsourced wordt.

Daarnaast zou de bescherming tegen benadeling uitgebreid moeten worden tot de functionarissen die de anonieme meldingen ontvangen en/of opvolgen. Een verschoningsrecht voor deze functionarissen zou een verdere versterking van de positie opleveren.

In aanvulling hierop moet de functionaris ook voldoende kennis op kunnen doen. Hiervoor dienen geaccrediteerde opleidingen ontwikkeld te worden, waarin (toekomstige) functionarissen op uniforme wijze getraind kunnen worden en er een kennisstandaard, en daarmee waarborgen voor de melders, kunnen worden aangebracht.

De Integriteitscoördinator is, zoals aangegeven, een voorstander van het gebruik van gespecialiseerde meldsoftware. Aangezien dit een kostenverhogende factor is, begrijpen we dat sommige partijen dit niet verplicht willen stellen. Ons inziens is het gebruik van deze software vrijwel onontkoombaar, als men de klokkenluiderprocedure op een goede manier wilt inrichten. Echter, wij merken ook dat er een wildgroei plaatsvindt van meldsoftware, waarbij het soms onduidelijk is wie de uiteindelijke aanbieder van de software is en aan welke eisen de software voldoet. Voor werkgevers is het soms lastig om een passende keuze te maken in het aanbod van softwareaanbieders. De Integriteitscoördinator adviseert dan ook te kijken naar minimale vereisten voor meldsoftware, dit om melder en werkgever te beschermen tegen onjuiste software, mogelijk door de invoering van een generiek keurmerk.

Overigens is door de recente groei van deze sector, het aanbod ook aanzienlijk goedkoper geworden, waardoor het lasten verhogende effect wel meevalt. Dit kan nog verder gereduceerd worden als branche- en koepelorganisaties gezamenlijke faciliteiten aan zouden bieden aan kleine organisaties.

Er is overigens steeds meer bewijs dat organisaties met meer meldingen en een goede speak-up cultuur financieel beter presteren[11]. Het is zeer waarschijnlijk dat een investering in dit soort meldsoftware en in een gespecialiseerde functionaris zichzelf zal terugverdienen.

Termijn

Tot slot wijden wij nog enkele woorden aan de redelijke termijn voor deze regeling zodat werkgevers voldoende tijd hebben om zich voor te bereiden. De Wet bescherming klokkenluiders is in de huidige vorm in december 2022 aangenomen door de Tweede Kamer en een maand later door de Eerste Kamer. Werkgevers weten dus al bijna anderhalf jaar dat zij binnenkort anonieme meldkanalen moeten inrichten. Sommigen hebben hier al op voorgesorteerd en bieden dit nu al aan. Of zij vinden dit sowieso al jaren een ‘good practice’. Anderen dienen wellicht nog software te selecteren, uit te vinden wie de onafhankelijke functionaris moet worden en instemming te vragen aan de ondernemingsraad, personeelsvertegenwoordiging of de medewerkers voor de aangepaste procedure. Dat had men al lang kunnen doen, maar wellicht wilde men de AMvB nog afwachten. Het lijkt ons dat dit nu al voorbereid kan worden, waarna ondernemingen een half jaar de tijd krijgen na inwerkingtreding van de AMvB om dit te regelen. Hopelijk zo snel mogelijk, bijvoorbeeld per 1 januari 2025. Het valt nog te overwegen om dit pas een half jaar later actief te laten handhaven door het Huis voor klokkenluiders, aangezien de toezicht- en handhavingsbepalingen uit de Wbk ook nog niet definitief zijn vastgesteld. Dit zou dan per 1 juli 2025 kunnen zijn.

De Integriteitscoördinator BV
Erasmus Enterprise
Burgemeester Oudlaan 50
3062 PA Rotterdam
www.deintegriteitscoordinator.nl
info@deintegriteitscoordinator.nl

[11] Zie bijvoorbeeld Transparency International – The business case for “speaking up” (2017), Amy Edmondson – The fearless organization (2018) of Stubben & Welch – Evidence on the use and efficacy of internal whistleblowing systems (2020).