

# Registratie integriteitsschendingen

openbaar bestuur en politie





# Registratie Integriteitsschendingen openbaar bestuur en politie

Het landelijk model voor de registratie van de afhandeling van (vermoedens van) integriteitsschendingen is ontwikkeld door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties samen met vertegenwoordigers van ministeries, provincies, gemeenten, waterschappen en politie.

Het landelijk model kan worden aangepast aan de eigen behoeften, natuurlijk met inachtneming van de uniforme vragen. Hiertoe is een modelformulier met de basis items en een modelformulier inclusief de optionele items beschikbaar gesteld via relevante websites.

Voor gemeenten:	<a href="http://www.vng.nl">www.vng.nl</a> (beleidsveld arbeidsvoorwaarden)
Voor provincies:	<a href="http://www.ipo.nl">www.ipo.nl</a>
Voor waterschappen:	<a href="http://www.uvw.nl">www.uvw.nl</a> (dossier arbeidsvoorwaardenbeleid)
Overig:	<a href="http://www.minbzk.nl/onderwerpen/overheidspersoneel">www.minbzk.nl/onderwerpen/ overheidspersoneel</a> <a href="http://www.integriteitoverheid.nl">www.integriteitoverheid.nl</a>

vts Politie Nederland stelt via intranet informatie beschikbaar voor alle politiekorpsen.



## Voorwoord

De overheid kan alleen goed functioneren als er voldoende vertrouwen bestaat dat zij eerlijk, open, onpartijdig en onomkoopbaar is. Het maakt daarbij niet uit of dit vertrouwen ontbreekt in het Rijk of in de lokale overheden. Gebrek aan vertrouwen heeft gevolgen voor alle geledingen van de overheid.

Het is aan de overheid om te tonen dat ze het vertrouwen waard is. Daarvoor is het nodig te erkennen dat er soms zaken voorkomen die niet acceptabel zijn en om daar krachtig tegen op te treden. Er zal wel eens sprake zijn van een grensgeval maar meestal is het volstrekt duidelijk wat wel of niet door de beugel kan. Door op te treden tegen individuele schendingen beschermt de overheid de integriteit van de overheid als geheel.

Overheidsmedewerkers moeten accepteren dat integriteitsschendingen niet getolereerd worden of met valse solidariteit worden toegedekt. De ambtelijke leiding dient een zodanig klimaat te scheppen dat er geen moed voor nodig is om zaken te melden. En het bestuur dient de ambtelijke leiding aan te spreken als zij schendingen niet adequaat afhandelt.

Het is van groot belang dat de ambtelijke leiding en het bestuur weten wat er speelt in de eigen organisatie. In de praktijk blijkt dat dit nog niet altijd het geval is. Interne transparantie over de wijze waarop de organisatie omgaat met meldingen, bevordert bij medewerkers de bereidheid om te melden. Ik kan dan ook niet genoeg benadrukken dat registratie een normaal onderdeel is van een volwaardig en transparant integriteitsbeleid.

Om te tonen dat de overheid serieus optreedt tegen integriteitsschendingen en daarbij niets verbergt, hebben vertegenwoordigers van de gemeenten, de provincies, de waterschappen, de politie en het Rijk samengewerkt aan de ontwikkeling van het landelijk model voor de Registratie integriteitsschendingen openbaar bestuur en politie. Een dergelijke uniforme registratie biedt openheid over schendingen bij de overheid en geeft de mogelijkheid dit probleem te bespreken op basis van feiten in plaats van percepties.

DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES,

Mevrouw dr. G. ter Horst



# Inhoudsopgave

	<b><i>Voorwoord</i></b>	<b>3</b>
	<b><i>Inhoudsopgave</i></b>	<b>5</b>
	<b><i>Inleiding</i></b>	<b>7</b>
<b>1.</b>	<b><i>Het belang van registratie</i></b>	<b>9</b>
	Betrouwbare gegevens	9
	Verantwoording afleggen	10
	Aantal meldingen: 5 per 1000 medewerkers	10
	Zicht op signalen	11
	Instellen procedures	12
<b>2.</b>	<b><i>Definities en uitgangspunten</i></b>	<b>13</b>
	Beleidsrelevante informatie	13
	Bestuurlijk/disciplinair traject	13
	Integriteitsschendingen breed registreren	14
	Afhandeling van vermoedens	14
	Eén betrokkene per registratieformulier	15
	Wet bescherming persoonsgegevens	16
	Verantwoordelijkheid overheidsorganisaties	17
	Maatwerk	17
	Enkele praktijkvoorbeelden van schendingen	18
<b>3.</b>	<b><i>Inhoud van het landelijk model</i></b>	<b>19</b>
	Introductie	19
	A) Administratieve informatie	20
	B) Informatie over de melding	20
	C) Informatie over de betrokkene	20
	D) Type schendingen en conclusie onderzoek	22
	E) Bestuurlijke en ambtelijke afdoening	24
	F) Strafrechtelijk traject	25
	<b><i>Bijlage 1: Overige relevante informatie (optionele items)</i></b>	<b>27</b>
	<b><i>Bijlage 2: Definities van de typen integriteitsschendingen</i></b>	<b>33</b>
	<b><i>Bijlage 3: Modelformulier Registratie integriteitsschendingen</i></b>	<b>37</b>





## Inleiding

In het Bestuurlijk Overleg van september 2005 tussen de minister van Binnenlandse Zaken en Koninkrijksrelaties, de Vereniging van Nederlandse Gemeenten (VNG), het Interprovinciaal Overleg (IPO), de Unie van Waterschappen, de Raad van Hoofdcommissarissen en het Korpsbeheerdersberaad is het belang van een betrouwbare registratie van integriteitsschendingen besproken. In de Bestuursakkoorden met de VNG (juni 2007) en het IPO (juni 2008) is vervolgens opgenomen dat in 2011 het rijk en alle provincies en gemeenten gebruik maken van een registratiesysteem voor integriteitsschendingen. Het landelijk model Registratie integriteitsschendingen geeft hieraan invulling.

Het landelijk model is tot stand gekomen dankzij de inzet van ministeries, gemeenten, provincies, waterschappen en andere organisaties. In bijeenkomsten is gesproken over de eisen waaraan een betrouwbare registratie zou moeten voldoen. Ook is een aantal bestaande registratiesystemen bestudeerd. De ministeries hebben sinds januari 2007 ervaring opgedaan met een rijksbrede registratie. Een aantal gemeenten, provincies, waterschappen en andere organisaties zoals de UWV hebben in het najaar van 2007 in een pilot een registratieformulier getest. De ervaringen die hiermee zijn opgedaan hebben geresulteerd in het landelijk model.

In overleg met de portefeuillehouders integriteit bij de Vereniging van Nederlandse Gemeenten, het Interprovinciaal Overleg, de Unie van Waterschappen en de Raad van Hoofdcommissarissen is een gezamenlijke inzet afgesproken. Die moet ertoe leiden dat in 2011 het rijk, alle gemeenten, provincies, waterschappen en politiekorpsen op vergelijkbare wijze integriteitsschendingen registreren.

De sector Politie geeft hierin al sinds 2003 het goede voorbeeld: alle korpsen registreren beleidsrelevante informatie in de Registratie Interne Onderzoeken (RIO). De Raad van Hoofdcommissarissen gebruikt deze gegevens om verantwoording af te leggen door middel van een jaarlijks bericht en analyseert de gegevens om trends en risico's te signaleren. De Raad van Hoofdcommissarissen gaat haar registratiesysteem begin 2009 herzien waarbij afstemming wordt gezocht met het landelijk model.



## 1. Het belang van registratie

Elke overheidsorganisatie kan te maken krijgen met schendingen van de integriteit. U kunt hierbij denken aan het lekken van informatie door een provincieambtenaar, een politieambtenaar die bijklust als portier bij een louche nachtclub of een gemeenteambtenaar die een lokaal aannemersbedrijf bevoordeelt. Ook binnen uw organisatie kunnen situaties voorkomen waarin sprake is van een (vermoedelijke) integriteitsschending. In dat geval is adequaat en consequent optreden gewenst. Want een volwaardig integriteitsbeleid is niet alleen het vaststellen en implementeren van het beleid: het is ook het handhaven ervan. Dus moeten ook signalen over vermoedelijke schendingen serieus worden opgepakt en onderzocht.

Als, na onderzoek, de schending is vastgesteld, moet er worden opgetreden tegen de overtreders. Het is belangrijk om vermoedens van schendingen, de aard van het daaropvolgend onderzoek en de afdoening gelijkloidend te registreren. Hierdoor krijgt het management inzicht in de aard en de omvang van integriteitsschendingen en kan het gerichte maatregelen nemen om schendingen in de toekomst te voorkomen. Het landelijk model en het bijbehorende modelformulier ondersteunen hierbij.

### Betrouwbare gegevens

In 2005 bleek uit twee onderzoeken<sup>1</sup> dat nog maar weinig overheidsorganisaties een goede en betrouwbare registratie hebben van (vermoedens van) integriteitsschendingen en de afhandeling ervan. En de organisaties die wel registreren, gebruiken vaak verschillende definities. Dit zorgt ervoor dat er geen duidelijk beeld is van de aard en omvang van de integriteit van de overheid. Het landelijk model verhoogt de transparantie rondom integriteitsschendingen. Overheidsorganisaties kunnen dan vergelijkbare en betrouwbare cijfers presenteren over de aard, omvang en afhandeling van meldingen van (vermoedelijke) integriteitsschendingen. Met een eerlijke en uniforme manier van registreren zorgen we ervoor dat discussies over de aard en omvang van integriteitsschendingen bij de overheid zich in de toekomst baseren op feiten in plaats van percepties.

<sup>1</sup> Algemene Rekenkamer, 'Integriteit bij het Rijk', 2005 en Vrije Universiteit, 'Corruptie in het Nederlands openbaar bestuur: omvang aard en afdoening', september 2005

## Verantwoording afleggen

Eén van de onderdelen van goed integriteitsbeleid is het verantwoording afleggen over integriteit en integriteitsbeleid. Sinds 1 maart 2006 is de Ambtenarenwet gewijzigd op het onderdeel goed ambtelijk handelen (Staatsblad 2005, 695). Hierin is opgenomen dat het bevoegde orgaan éénmaal per jaar schriftelijk het tegenwoordigende orgaan informeert over het gevoerde integriteitsbeleid en over de naleving van de gedragscode. Dit laatste onderdeel impliceert dat het bevoegd orgaan zicht heeft op de afhandeling van de (vermoedens van) integriteitsschendingen binnen de organisatie.

### Aantal meldingen: 5 per 1000 medewerkers

Het afleggen van verantwoording is makkelijker gezegd dan gedaan. Het aantal medewerkers dat een schending heeft gepleegd, kan door derden worden opgevat als een teken dat de organisatie niet goed functioneert. Organisaties kunnen door zorgen hierover terughoudend zijn om betrouwbare gegevens te presenteren. Daarentegen heeft de maatschappelijke aandacht voor integriteit er onder andere toe geleid dat het tegenwoordig ongeloofwaardig overkomt als een bestuur stelt geen tot weinig meldingen te kennen. Inzicht in het aantal meldingen en de afhandeling hiervan, wordt daarmee steeds meer gezien als een teken van een goed functionerend integriteitsbeleid.

Maar wat is een 'normaal' aantal schendingen? Dit verschilt per sector en per organisatie, mede door verschillen in de inherente risico's die samenhangen met de taken van de organisatie. Een voorzichtige aanname is dat een gemiddelde overheidsorganisatie per jaar over ongeveer 5 per 1.000 medewerkers een melding zal ontvangen. Voor grotere organisaties, met een centraal meldpunt en specifieke risicovolle taken, ligt dit meestal - beduidend - hoger.

De gemeente Amsterdam heeft in 2006 109 meldingen ontvangen met betrekking tot 100 bekende en 19 onbekende medewerkers. Dit leidde vijftien keer tot strafontslag en zes keer tot voorwaardelijk ontslag.

Gemiddeld kent de gemeente Amsterdam ongeveer 7 onderzoeken per 1.000 medewerkers.  
*Bron: 2e Haljaarreportage Centraal Registratiepunt Integriteitsschendingen 2007, Bureau Integriteit Amsterdam*

Het UWV heeft in 2006 naar aanleiding van 225 meldingen feitenonderzoeken ingesteld. In 2006 is ten aanzien van 45 medewerkers arbeidsrechtelijke maatregelen getroffen (7 beëindigingen van het dienstverband en in 38 gevallen preventieve maatregelen). Tegen 5 medewerkers is ook aangifte gedaan. Bij de UWV werken ongeveer 18.000 medewerkers. Per 1.000 medewerkers zijn dus 12 meldingen ontvangen.

*Bron: UWV Jaarverslag 2006*

De politiekorpsen beschikken sinds 2003 over een centraal registratiesysteem. In 2007 werden in totaal 1498 onderzoeken geregistreerd, waarbij 1551 politieambtenaren betrokken waren. Dit leidde 120 keer tot strafontslag, 89 keer tot voorwaardelijk ontslag en 55 politiemensen namen gedurende het onderzoek zelf ontslag. Bij de politiekorpsen zijn 55.000 medewerkers in dienst.

Het onderzoek leidde in 43% tot de conclusie dat de verdenking weerlegd was of niet kon worden aangetoond. In 10% was er sprake van een strafbaar feit en in 31% kon plichtsverzuim worden aangetoond. De top drie van aangetoonde typen schendingen is: rechtspositieve kwesties (vooral het niet volgen van procedures), geweld en misbruik positie (vooral het lekken en misbruik maken van informatie).

Per 1.000 medewerkers zijn bij de politie 28 politieambtenaren onderzocht. Een derde hiervan betrof de verplichte melding van geweldsincidenten.

*Bron: Registratie Interne Onderzoeken naar integriteitsschendingen 2007 bij de Nederlandse politie, vtsPN, september 2008.*

De praktijk laat zien dat organisaties die de verantwoordelijkheid voor integriteit en de afhandeling van schendingen op één centraal punt hebben neergelegd vaak een (sterke) stijging van het aantal casussen kenden. Door centrale registratie stijgt meestal het aantal bekende casussen. Als een organisatie weinig signalen van (vermoedelijke) schendingen ontvangt, is dat dus niet bij voorbaat reden tot zelfgenoegzaamheid.

## Zicht op signalen

In veel organisaties reageren medewerkers en leidinggevendenden niet altijd adequaat op (vermoedens van) integriteitsschendingen. Uit onderzoek blijkt dat één op de vier ambtenaren vindt dat de eigen organisatie geen open organisatiecultuur heeft en dat er te weinig ruimte is voor het uiten van kritiek en het geven van eerlijke adviezen.<sup>2</sup>

Maar niet alleen een open organisatiecultuur is belangrijk. Het moet voor medewerkers en leidinggevendenden ook helder zijn hoe ze om moeten gaan met (vermoedens van) schendingen. Zijn er vertrouwenspersonen integriteit binnen de

<sup>2</sup> Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2007), *Integriteit van de overheid: Een onderzoek naar de integriteitsbeleving van het overheids personeel*, januari 2007.

organisatie en zijn deze bekend bij medewerkers? Zijn er heldere procedures voor de afhandeling van (vermoedelijke) schendingen? Is er een centraal punt in de organisatie dat een overzicht heeft van de signalen die serieus zijn opgepakt? Dergelijke vragen maken duidelijk dat registratie geen sluitstuk vormt van een goed integriteitsbeleid, maar een startpunt. Het draagt bij aan een kritische reflectie op het eigen beleid.

Verschillende functionarissen hebben informatie over de afhandeling van meldingen van (vermoedelijke) integriteitsschendingen, zoals:

- Vertrouwenspersonen integriteit
- Vertrouwenspersonen ongewenste omgangsvormen
- Arbeidsjuristen en HRM-adviseurs
- Leidinggevenden en het bestuur
- Coördinator integriteit
- Beveiligingsambtenaren

## Instellen procedures

Het landelijk model is slechts een startpunt voor registratie: overheidsorganisaties bepalen zelf welke functionarissen dit invullen, toegang hebben tot de verzamelde gegevens et cetera. Overheidsorganisaties moeten zelf aanvullende procedures formuleren en deze, als dat nodig is, voorleggen aan de ondernemingsraad en het bevoegd orgaan. Deze procedures moeten natuurlijk aansluiten op de procedures voor het melden van misstanden en op de procedures voor het verrichten van een intern onderzoek en de afhandeling van een schending.

Meer informatie hierover kunt u vinden op [www.integriteitoverheid.nl/handreikingen](http://www.integriteitoverheid.nl/handreikingen).

## 2. Definities en uitgangspunten

Bij het modelformulier is een aantal algemene uitgangspunten gehanteerd die hieronder kort zijn weergegeven.

### **Beleidsrelevante informatie**

Het landelijk model richt zich op een beperkt aantal beleidsmatig relevante gegevens die elke organisatie moet registreren.<sup>3</sup> Zo wordt informatie over de melder van een (vermoedelijke) schending, de betrokkene, de (vermoedelijke) schending, het onderzoek en de afdoening in onderlinge samenhang vastgelegd. Bij de afdoening gaat het niet alleen over het bestuurlijke traject, maar ook over het doen van aangifte bij het OM.

Naast informatie die deel uit maakt van het landelijk model, is ook een aantal optionele items ontwikkeld (zie bijlage 1).

Het landelijk model betreft alleen gegevens die relevant zijn voor analyse. Het betreft dus geen bedrijfsmatige informatie en het heeft ook geen betrekking op het opbouwen van een volledig dossier met alle gegevens uit het onderzoek.

### **Bestuurlijk/disciplinair traject**

Het landelijke model gaat uit van het bestuurlijke/disciplinaire traject met mogelijke bestuurlijke afdoening. Daarom is het traject gericht op de betrokkene. Het strafrechtelijke traject heeft een eigen procesgang van aangifte tot OM-beslissing. Alleen bij organisaties die beschikken over medewerkers met opsporingsbevoegdheden kan het bestuurlijk en strafrechtelijk traject binnen dezelfde organisatie worden verricht.

### **Melder, betrokkene en casus**

De melder is de persoon of functionaris (van binnen of buiten de organisatie) die een signaal over een (vermoedelijke) integriteitsschending geeft. De melder geeft het signaal aan de relevante verantwoordelijke voor de afhandeling van dat vermoeden. Een melder hoeft geen klokkenluider te zijn. Onder betrokkene verstaan we de (vermoedelijke) pleger van de (vermoedelijke) schending. De casus betreft de gegevens in het registratieformulier zoals die per betrokkene zijn vastgelegd.

3 Zie Algemene Rekenkamer, 'Integriteit bij het Rijk', 2005 en Vrije Universiteit, 'Corruptie in het Nederlands openbaar bestuur: omvang aard en afdoening', september 2005

### ***Plichtsverzuim***

De ambtenaar die zich niet als een goed ambtenaar gedraagt, maakt zich schuldig aan plichtsverzuim. We spreken hiervan als de ambtenaar geschreven regels, zoals wet- en regelgeving, overtreedt. Van plichtsverzuim kan ook sprake zijn wanneer algemeen aanvaarde normen worden geschonden, ook al zijn deze niet schriftelijk vastgelegd.

### **Integriteitsschendingen breed registreren**

Over de definitie en de reikwijdte van het begrip integriteit kan lang worden gesproken. Voor het landelijk model is niet gekozen voor een abstracte definitie, maar voor een overzicht van type schendingen. Deze is gebaseerd op wet- en regelgeving en model-gedragscodes. Meegewogen is welke type schendingen vaker voorkomen en welke maatschappelijke onrust oproepen.

Maar het gaat niet alleen om ernstige schendingen die de publiciteit halen. Ernstige integriteitsschendingen staan namelijk vaak niet op zichzelf. Zij kunnen bijvoorbeeld gepaard gaan met andere integriteitsschendingen, of de pleger heeft al eerder kleinere type schendingen gepleegd. Het is daarom vanuit preventief oogpunt belangrijk dat ook minder ernstige incidenten worden gesignaleerd en opgepakt door de organisatie.

Verder is preventie vooral effectief als zij zich kan richten op specifieke typen schendingen. Het landelijke model bevat daarom gedetailleerde informatie over de aard van de schending.

### **Afhandeling van vermoedens**

Het vertrouwen van de burger in de integriteit van de overheid wordt mede beïnvloed door een correcte afhandeling van signalen van (vermoedelijke) schendingen. Daarom is het belangrijk dat organisaties ook vermoedelijke schendingen registreren. Zelfs als dit tot de conclusie leidt dat er geen sprake is gebleken van een schending. Het ontzenuwen van geruchten en het vrijspreken van een medewerker is tenslotte ook een functie van een intern onderzoek. Het bevoegd gezag kan vervolgens aangeven hoe vaak een signaal resulteerde in een onderzoek, en vervolgens hoe vaak een onderzoek leidde tot een vastgestelde schending met een afdoening.

### ***Registreren van adviezen?***

Vertrouwenspersonen ontvangen niet alleen meldingen, maar geven ook advies bij persoonlijke integriteitsvraagstukken. Daarnaast kan een vertrouwenspersoon meldingen krijgen die geen (directe) relatie hebben met de integriteit van de



organisatie. Dergelijke adviezen en meldingen maken geen onderdeel uit van het landelijk model. De organisatie kan deze natuurlijk desgewenst wel registreren voor de interne verantwoording.

### **Eén betrokkene per registratieformulier**

Bij de rapportage over de geregistreerde casussen moeten de belangrijkste gegevens direct te herleiden zijn tot het aantal betrokkenen. De volgende mogelijkheden zijn hierbij vooral relevant:

#### ***Eén signaal, meerdere personen betrokken***

Eén signaal kan betrekking hebben op meerdere betrokkenen. Daarbij kunnen het onderzoek, afdoening en/of sanctie al snel uit elkaar lopen. Per betrokkene moet dan ook een apart registratieformulier worden ingevuld. Dat neemt niet weg dat er wel sprake kan zijn van een gezamenlijk onderzoeksdossier.

#### ***Meerdere signalen***

Over een incident, of over een betrokkene, kunnen meerdere melders signalen doorgeven. Voor het landelijk model is alleen de eerste melder relevant. Maar voor de opbouw van een (onderzoeks)dossier is dit wel relevante informatie.

#### ***Eén betrokkene, meerdere soorten schendingen***

Een betrokkene kan meerdere soorten schendingen plegen. Bijvoorbeeld fraude en een ongewenste nevenfunctie. In de registratie kan dit in dezelfde casus worden geregistreerd. Bij de uiteindelijke afdoening worden, indien van toepassing, de conclusie over elk van deze schendingen meegewogen.

#### ***Vaker de fout in***

Sommige betrokkenen gaan meer dan eens de fout in. Er moet dan opnieuw een registratieformulier worden ingevuld. Het eerdere signaal heeft tenslotte al geleid tot een bepaalde afdoening en is daarmee afgerond.

<i>Vraag en antwoord</i>	
<b>Casuïstiek</b>	<b>Antwoord</b>
Zijn er drie betrokkenen en één soort schending? (met z'n drieën één kopieerapparaat gestolen)?	Elke betrokkene wordt in een apart registratieformulier geregistreerd. Dat eidt tot drie verschillende l formulieren die desgewenst via het dossiernummer met elkaar kunnen worden verbonden.
Komen er meerdere (anonieme) meldingen binnen over één schending?	Alleen enkele gegevens van de eerste melder worden geregistreerd.
Is er één dader, maar zijn er twee of meer soorten schendingen? (bijvoorbeeld diefstal en ongewenste nevenfuncties)?	Er wordt één registratieformulier ingevuld waarin per type schending de conclusie wordt vastgelegd.
De betrokkene heeft eerder in het jaar al een voorwaardelijke disciplinaire straf ontvangen.	Er is sprake van een nieuwe melding die moet worden afgehandeld. Dit wordt vastgelegd in een nieuw registratie formulier. Desgewenst kan er verwezen worden naar het oude dossiernummer.

## **Wet bescherming persoonsgegevens**

De registratie van integriteitschendingen bij de overheid moet voldoen aan relevante wet- en regelgeving. Omdat de registratie gevoelige gegevens kan bevatten, moet het goed worden beveiligd zodat ongeautoriseerde derden geen toegang kunnen krijgen. Zelfs als de informatie zich beperkt tot managementinformatie en deze niet is te herleiden tot personen. Als de registratie zodanig wordt ingericht en gebruikt dat de ingevoerde gegevens direct of indirect herleidbaar zijn tot personen, dan is de organisatie verantwoordelijk voor het melden van de verwerking van persoonsgegevens bij het College Bescherming Persoonsgegevens (CBP). Bij gebruik van het landelijk formulier met alleen de basisvragen, is melding bij het CBP niet nodig.

Als de organisatie er voor kiest om persoonsgegevens te registeren is, op grond van artikel 27 van de Wet op de ondernemingsraden, voor de registratie instemming vereist van de ondernemingsraad.

## Verantwoordelijkheid overheidsorganisaties

Moet een fraude ter waarde van twintig euro worden geregistreerd? Of een discriminerende opmerking van een ambtenaar tegen een burger waarover een klacht is ingediend? Hiervoor zijn geen algemene regels te stellen. Alleen het bevoegd orgaan van een overheidsorganisatie bepaalt op grond van wet- en regelgeving en haar integriteitsbeleid wanneer een signaal betrekking heeft op mogelijk plichtsverzuim en daarmee relevant om te registreren.

De algemene normen die aan de integriteit van de overheid worden gesteld, gelden voor alle overheidsorganisatie. Maar sommige organisaties (of organisatieonderdelen) zijn strenger in de leer. Een algemene norm is dat geschenken in principe toelaatbaar zijn mits zij een waarde onder de vijftig euro vertegenwoordigen. Maar sommige organisaties hanteren vanwege hun voorbeeldfunctie een nullijn en vinden geen enkel geschenk aanvaardbaar. Verschillen in beleid tussen overheidsorganisaties vertalen zich daarom naar verschillende aantallen geregistreerde casussen van (vermoedelijke) schendingen. Om dergelijke verschillen goed te kunnen interpreteren is het wel van belang dat de organisatie de eigen normen helder heeft geformuleerd. De kracht van het landelijk model schuilt dan ook vooral in de uniformiteit van de definities, deze maakt vergelijking tussen organisaties mogelijk.

## Maatwerk

Het landelijk model ontslaat organisaties niet van hun verantwoordelijkheid om te bepalen welke aanvullende gegevens relevant zijn, gezien de eigen specifieke integriteitsrisico's. Een registratie dient aan te sluiten bij de kenmerken en de informatiebehoefte van de organisatie. Het gebruik van drugs, het helpen bij de ontsnapping van gedetineerden en belastingfraude zijn slechts voorbeelden van schendingen die voor bepaalde organisaties relevant zijn en gespecificeerd kunnen worden in de registratie.

Ook op andere punten kan maatwerk wenselijk zijn. Zo neemt het uitgangspunt dat de belangrijkste gegevens op de betrokkene zijn te herleiden (kenmerken van de betrokkenen, type schending en afdoening) niet weg dat het mogelijk is om de overige gegevens per onderzoek te registreren. Voor organisaties met een eigen bureau integriteit en grotere aantallen onderzoeken per jaar kan dit beter aansluiten bij de inrichting van hun werkprocessen.

## Enkele praktijkvoorbeelden van schendingen

Zie meer praktijkvoorbeelden op [www.integriteitoverheid.nl/jurisprudentie](http://www.integriteitoverheid.nl/jurisprudentie).

Financiële schendingen

### **Ontbreken van controle op financieel beheer ontslaat ambtenaar niet van eigen verantwoordelijkheid**

Provincieambtenaar houdt (bij herhaling) de opbrengst van verkocht dienstmateriaal gedeeltelijk achter en krijgt strafontslag. De Centrale Raad oordeelt dat het achterwege blijven van controle van bovenaf, of het eventueel ontbreken aan regels over kasbeheer, geen vrijbrief oplevert voor dergelijk gedrag. Op de ambtenaar rust een eigen verantwoordelijkheid jegens de werkgever.

*Centrale Raad van Beroep, 13-4-2006, TAR 2006/117, LJN AX1635.*

Misbruik positie en belangenverstrengeling

### **Gemeenteambtenaar bouwzaken maakt voor derden (privé en tegen betaling) bouwtekeningen voor onder zijn toezicht staande percelen**

Gemeenteambtenaar bij bouwzaken heeft tegen betaling bestek- en bouwtekeningen gemaakt voor particulieren, ook voor locaties die onder zijn toezicht stonden. Hij heeft hiervan geen melding gemaakt bij de leiding. Hierdoor is zijn onafhankelijkheid in het geding gekomen en is er sprake van ontoelaatbare belangenverstrengeling. Aan hem is strafontslag verleend. De rechtbank laat het ontslag in stand.

*Rechtbank Den Haag, 5-11-2003, TAR 2003/201.*

Misbruik bedrijfsmiddelen en overschrijding interne regels

### **Downloaden van muziek door systeembeheerder leidt tot strafontslag**

Een systeembeheerder bij een informatiegevoelige dienst van een ministerie heeft meermaals muziekbestanden gedownload met behulp van een speciaal downloadprogramma KaZaA dat door hem is geïnstalleerd. Dit is in strijd met de interne regels voor gebruik van internet en met nadere expliciete aanwijzingen (tijdens werkoverleg en functioneringsgesprek). Aan hem is strafontslag verleend. De Raad acht het strafontslag niet onevenredig omdat bij deze dienst met staatsgeheimen wordt gewerkt en beveiliging een zeer hoge prioriteit geniet. Bovendien is de functie van systeembeheerder een vertrouwensfunctie waaraan zeer hoge eisen worden gesteld met betrekking tot integriteit. Het ontslag blijft in stand.

*Centrale Raad van Beroep, 02-03-2006, LJN AV3950, TAR 2006/165*

Misdragingen in de privé-sfeer

### **Plichtsverzuim gemeenteambtenaar vanwege hennepplantage**

Een gemeenteambtenaar blijkt thuis een hennepplantage te hebben. Hij is eerder al door de strafrechter veroordeeld voor overtreding van de Opiumwet. Aan hem is strafontslag verleend. Het verweer van de ambtenaar dat zijn gedraging uitsluitend zijn privé-sfeer raakt, wordt door de Raad verworpen omdat het voor het aanzien van de gemeente onaanvaardbaar is dat een ambtenaar betrokken is bij het illegaal kweken van hennepplanten. De Raad laat het ontslag in stand.

*Centrale Raad van Beroep, 28-9-2006, LJN AY9666, TAR 2007/7.*

## 3. Inhoud van het landelijk model

### Introductie

Het landelijk model voor de registratie van de afhandeling van (vermoedens van) integriteitsschendingen heeft de volgende indeling:

1. Algemeen: A) administratieve informatie, B) informatie over de melding en C) informatie over de betrokkene.
2. Type schendingen: D) het type schending en de conclusie van het onderzoek.
3. Afdoening: de E) bestuurlijke en F) strafrechtelijke afdoening.

Per onderdeel wordt beschreven welke informatie deel uitmaakt van het landelijk model. Ook staan er korte toelichtingen en, waar nodig, definities. De optionele items staan beschreven in bijlage 1.

### A) Administratieve informatie

In het registratiesysteem zijn de algemene administratieve zaken grotendeels optioneel, met uitzondering van de volgende vragen:

#### **1-2. Start- en einddatum**

Voor het kunnen maken van jaarrapportages is de start- en einddatum noodzakelijk. De startdatum betreft de datum waarop de (vermoedelijke) schending is gemeld. De einddatum kan betrekking hebben op:

- de datum waarop wordt besloten geen onderzoek te verrichten dan wel,
- de datum van afronding van het onderzoek dan wel,
- de datum van het primaire besluit van het bevoegde orgaan.

#### **3. Meerdere betrokkenen**

Het landelijk model registreert per betrokkene. Dat neemt niet weg dat het kan voorkomen dat er meerdere betrokkenen zijn. Het is belangrijk om bij de registratie hierop alert te zijn en om per betrokkene één formulier in te vullen.

## **B) informatie over de melding**

### ***4. Interne of externe melding***

Er wordt vaak gewezen op het belang van een open en veilige organisatiecultuur waarin medewerkers zich vrij voelen om integriteitskwesties te bespreken en om hun (vermoedens van) schendingen te melden. Ook is er veel maatschappelijke aandacht voor de positie van interne melders van misstanden, ook wel klokkenluiders genoemd. Om deze redenen is het belangrijk om te weten hoe een (vermoeden van) schending aan het licht is gekomen. Wat was de eerste aanleiding? Om het eenvoudig te houden is een onderscheid gemaakt tussen een interne melding (vanuit de eigen organisatie) en een externe melding (buiten de organisatie).

### ***5. Melding klokkenluidersregeling***

Aanvullend is relevant of de melding valt onder de regeling melding misstanden (klokkenluidersregeling). Het bevoegd gezag van overheidsorganisaties is op grond van de Ambtenarenwet (art. 125 quinquies) en de Politiewet 1993 (art. 50) verplicht om procedurevoorschriften vast te stellen voor het omgaan met interne meldingen van vermoedens van misstanden. De procedures zijn gericht op een goede afhandeling van de melding en op de bescherming van de melder.

### ***6. Meldpunt M***

Een specifieke externe aanleiding betreft een melding van Meldpunt M. Dit is de meldlijn waar iedere burger of medewerker van een organisatie anoniem kan melden over ernstige integriteitsschendingen. Dit Meldpunt is bedoeld voor melders die niet durven te melden bij de betreffende organisatie of de politie uit angst voor wraak of confrontatie met de dader.

Zie voor meer informatie [www.meldmisdaadanoniem.nl](http://www.meldmisdaadanoniem.nl)

## **C) informatie over de betrokkene**

Met betrokkene bedoelen we de (vermoedelijke) pleger van de schending. Daarbij zijn vooral de volgende gegevens relevant:

### ***7. Betrokkene onbekend***

Bij bepaalde schendingen, zoals diefstal en het lekken van informatie, is vaak niet te achterhalen wie deze schendingen heeft gepleegd. Voor een goed inzicht in het aantal schendingen is het wel gewenst om deze te registreren.

## 8. In dienst van de organisatie

De betrokkene is niet altijd in dienst van de organisatie: de schending kan ook gepleegd worden door uitzendkrachten, gedetacheerden, schoonmakers of beveiligers. Dergelijke functionarissen kunnen ook de integriteit van de organisatie aantasten. Het is van belang dat een organisatie zich bewust is van mogelijke risico's met betrekking tot externe inhuur. Toch is het bestuur niet direct verantwoordelijk voor schendingen gepleegd door deze externe inhuur. Vaak leidt een schending van een dergelijke functionaris dan ook niet tot een uitgebreid onderzoek, maar tot opzegging van het contract.

## 9-10. Politieke ambtsdragers en leidinggevenden

Het belang van integriteit weegt voor bepaalde functionarissen zwaarder gezien hun voorbeeldfunctie. Bijvoorbeeld voor politieke ambtsdragers (bestuurders en volksvertegenwoordigers) en leidinggevenden. Zij moeten de integriteit van de organisatie bewaken. Dat neemt niet weg dat ook zij een schending kunnen plegen. Gezien hun voorbeeldfunctie is transparantie in de afhandeling van (vermoedens van) schendingen van groot belang. Bij schending door een bestuurder of volksvertegenwoordiger wordt vaak voor een andere wijze van afdoening gekozen. Maar het registratieformulier biedt wel de mogelijkheid tot registratie.

Vraag en antwoord	
De betrokkene	Antwoorden
Bij de melding is (nog) niet bekend wie de betrokkene is.	Er wordt een casus aangemaakt waarin wordt vastgelegd dat de betrokkene onbekend is. Als ook na een (voor) onderzoek de betrokkene onbekend blijft, leidt dit tot conclusie onderzoek 'niet aangetoond, betrokkene onbekend'.
De betrokkene is niet in dienst van de organisatie die registreert, maar de integriteit van de organisatie is (vermoedelijk) wel aangetast door de betrokkene.	Registreren als een normale casus. In het registratiesysteem kan worden aangegeven dat de betrokkene niet in dienst is van de organisatie.
De betrokkene is een bestuurder.	Registreren als een normale casus. In het registratiesysteem kan worden aangegeven dat de betrokkene een bestuurder is.

## D) Type schendingen en conclusie onderzoek

De schendingen zijn in te delen in verschillende typen. In de bijlage is een overzicht opgenomen met de subtypen en een definitie.

### **11a. Financiële schendingen**

Bij financiële schendingen is er vaak sprake van diefstal, verduistering of fraude. Optioneel kan worden vastgelegd of de schendingen intern plaatsvond (gericht op functionarissen binnen de organisatie en de organisatie zelf) of extern (gericht op burgers, klanten of bedrijven).

### **11b. Misbruik positie en belangenverstrengeling**

Deze schending kent verschillende vormen en verschillende gradaties van ernst. Bij belangenverstrengeling is vaak sprake van ongewenste nevenactiviteiten of financiële belangen. Maar het betreft ook omkoping en corruptie. Het aannemen van geschenken is niet altijd gewenst en deze worden ook niet altijd gemeld.

### **11c. Lekken en misbruik van informatie**

Overheidsinformatie is een kwetsbaar goed. Informatie uit concept-rapporten lekt voortijdig uit. Het lekken en misbruik maken van informatie omvat ook het raadplegen van informatie uit vertrouwelijke registers waartoe men niet bevoegd is of voor privé-doeleinden. Usb-sticks met gevoelige informatie liggen bijna letterlijk op straat. Verlies en diefstal van informatiedragers is daarmee een risico voor organisaties.

### **11d. Misbruik bevoegdheden**

We spreken van misbruik van bevoegdheden wanneer het doel of gevolg van iemands acties het belemmeren of verhinderen van een juiste rechtsgang is. Het misbruik heeft onder meer betrekking op ongeoorloofde opsporingsmethoden, misbruik van dwangmiddelen, meened en valsheid in geschrifte. Ook de afgifte van vergunningen en identiteitsbewijzen kan worden gemanipuleerd. Voorbeelden van opsporings- en dwangmiddelen zijn aanhouden, fouilleren, inverzekeringstelling, huiszoeking en het afluisteren van telefoons. Hoe zwaarder het middel is, des te meer voorwaarden zijn aan de toepassing ervan verbonden. Bij zware middelen is bijvoorbeeld altijd toestemming van de rechter vereist. Bij meened en valsheid in geschrifte is sprake van het afleggen van een valse verklaring.

### **11e. Misbruik geweldsbevoegdheid**

Politieambtenaren, bijzondere opsporingsambtenaren en militairen zijn vanuit hun taak en functie bevoegd om fysiek geweld toe te passen. Dit is echter wel aan



strengere regels gebonden: het toegepaste geweld moet subsidiair en proportioneel zijn. Is dat niet het geval dan is er sprake van misbruik van de geweldsbevoegdheid. Naast fysiek geweld is vuurwapengebruik onderscheiden.

### **11f. Ongewenste omgangsvormen**

Ongewenste omgangsvormen vallen niet alleen onder de Arbowetgeving, maar ook onder het integriteitsbeleid. Zij worden onderscheiden naar discriminatie, seksuele intimidatie, verbale agressie en geweld, fysieke agressie en geweld. Deze ongewenste omgangsvormen kunnen intern plaatsvinden (gericht op medewerkers en/of leidinggevend) en extern (gericht op burgers, klanten, bedrijven).

Bij ongewenste omgangsvormen kan een advies van de vertrouwenspersoon vaak tot een oplossing leiden. Dit betekent dat er in die gevallen geen formele klachtenprocedure volgt. Zie bijlage 1 met optionele items voor mogelijkheden om ook adviezen te registreren. Deze gegevens zijn vooral voor de interne verantwoording relevant.

### **11g. Misbruik bedrijfsmiddelen en overschrijding van interne regels**

Hier gaat het deels om het oneigenlijk gebruiken van materialen van de organisatie voor privé-doeleinden. Het bekendst zijn het ongewenst gebruik van e-mail en internet en het misbruik van de (mobiele) telefoon, auto en andere bedrijfsmiddelen. Ook schending van overige interne regels kunnen leiden tot het nemen van disciplinaire maatregelen. Voorbeelden hiervan zijn ongeoorloofd werkverzuim, het niet volgen van procedures en slordig omgaan met bedrijfsmateriaal.

### **11h. Misdragingen in privé-sfeer**

Niet alleen tijdens werktijden hebben ambtenaren een voorbeeldfunctie: voor sommigen onder hen kan ook het gedrag buiten werktijden en buiten de plaats waar de functie wordt uitgeoefend van belang zijn. Dit geldt vooral voor ambtenaren met een publieke functie: hun gedrag straalt uit op de overheidsorganisatie. Zo kan een politieambtenaar of een hoge ambtenaar zijn eigen functioneren en het imago van de organisatie schaden door het plegen van diefstal of mishandeling in de privé-sfeer. Hoewel de schending in de privé-sfeer heeft plaatsgevonden en er geen directe relatie is met de uitoefening van de functie, is er - door de voorbeeldfunctie van de betrokkene - wel sprake van een aantasting van de integriteit van de overheid.

### **11i. Misstanden volgens de klokkenluidersregeling**

Er is veel maatschappelijke aandacht voor klokkenluiders (regelingen). Het is daarom relevant om te kunnen achterhalen hoeveel signalen via de klokkenluidersrege-

lingen zijn afgedaan en op welke type misstanden, conform de bestaande wet- en regelgeving, deze betrekking hebben.

Onder misstand wordt verstaan een op redelijke gronden gebaseerd vermoeden van het zich voordoen van: een schending van wettelijke voorschriften of beleidsregels; een gevaar voor de gezondheid, de veiligheid of het milieu; of een onbehoorlijke wijze van functioneren die een gevaar vormt voor het goed functioneren van de openbare dienst.

### **12. Conclusie**

Het is belangrijk om per type schending aan te geven wat de conclusie is van het onderzoek. Zo is in de praktijk fraude gemakkelijker aan te tonen dan diefstal. Uit het onderzoek kan blijken dat de betrokkene een schending heeft gepleegd, er is dan sprake van plichtsverzuim. De verdenking is weerlegd als uit het onderzoek blijkt dat er geen schending is gepleegd, of dat de schending niet door de onderzochte betrokkene is gepleegd. Er is sprake van ‘verdenking is niet aangetoond’ als de schending niet kan worden bewezen of als de betrokkene niet kan worden achterhaald.

## **E) Bestuurlijke en ambtelijke afdoening**

### **13. Instellen van een onderzoek**

Na de eerste weging van de melding besluit de organisatie tot het al dan niet instellen van een onderzoek. Dit kan een volledig feitenonderzoek zijn, bijvoorbeeld naar aanleiding van een vooronderzoek. Bij een vaag signaal (dat is gebaseerd op geruchten) of bij een onbekende betrokkene, kan het zijn dat alleen een vooronderzoek wordt gehouden. Hiermee wordt bepaald of het signaal voldoende aanwijzingen bevat voor het houden van een volledig – en ingrijpend – feitenonderzoek. Soms blijkt dat er geen onderzoek gewenst is naar aanleiding van het signaal. Het is wenselijk om de motivatie hiervoor vast te leggen: zo wordt verantwoord dat de organisatie op correcte wijze heeft gereageerd op het signaal. In de praktijk vragen medewerkers een vertrouwenspersoon of andere functionaris vaak alleen om advies, in dergelijke gevallen is het verrichten van een onderzoek veelal niet van toepassing.

### **14. Afdoening**

De casus is al dan niet in behandeling genomen. Het eindresultaat kan zijn dat er geen afdoening plaatsvindt en ook niet plaats zal gaan vinden. Dat is echter niet hetzelfde als afdoening onbekend. Hiervan is alleen sprake als de functionaris die verantwoordelijk is voor de registratie niet kan achterhalen of er een afdoening heeft plaatsgevonden.

Als er sprake is van plichtsverzuim heeft het bestuur, op grond van wet- en regelgeving, de beschikking over verschillende disciplinaire afdoeningen. De afdoeningen kunnen voorwaardelijk en onvoorwaardelijk plaatsvinden. Voorwaardelijke afdoeningen worden niet meteen ten uitvoer gelegd, maar pas op het moment dat de betrokkene opnieuw plichtsverzuim pleegt. Bij onvoorwaardelijk gaat het om maatregelen die onmiddellijk ten uitvoer worden gelegd.

De afhandeling van een casus kan ook leiden tot een ambtelijke afdoening: afdoeningen die niet disciplinair van aard zijn. Zo zijn er verschillende vormen van ontslag mogelijk. Ook wordt wel in plaats van de disciplinaire schriftelijke berisping de waarschuwingsbrief gehanteerd. Afdoeningen die zich richten op het functioneren van de betrokkene zijn overplaatsing, training/coaching en het corrigerende gesprek.

Bij externe inhuur zal veelal het contract worden beëindigd.

Een betrokkene kan op grond van een disciplinaire afdoening worden overgeplaatst. Dit wordt bij disciplinaire afdoening geregistreerd. Als een betrokkene op andere gronden wordt overgeplaatst, dan kan dit bij ambtelijke afdoeningen worden geregistreerd.

## **F) Strafrechtelijk traject**

### ***15. Inschakeling van politie, OM of Rijksrecherche***

Bij de afhandeling van een casus beoordeelt het bevoegd gezag of de politie, het OM of de Rijks-recherche ingeschakeld wordt. In een aantal gevallen, zoals beschreven in artikel 162 Wetboek van strafvordering, is het doen van aangifte zelfs wettelijk verplicht. Desondanks doet het bevoegd gezag in de praktijk nog weinig aangifte van (mogelijk) strafbare feiten.

Het doen van aangifte moet onderscheiden worden van het doen van een melding. Bij aangifte wordt een procesverbaal of een aangifteformulier opgemaakt en ondertekend. Het melden van een integriteitsschending is het op de hoogte stellen van Justitie in de breedste zin van het woord. In overleg met Justitie kan dan bepaald worden of het zinvol is om formeel aangifte te doen.

### ***16. Strafrechtelijke afdoening***

Als de strafrechtelijke afdoening wel bekend is, wordt er onderscheid gemaakt tussen seponering door het OM, transactie/boete en veroordeling.

Een besluit van het openbaar ministerie om niet te vervolgen heet een sepot. Het openbaar ministerie kan om twee redenen seponeren. Ten eerste omdat een veroordeling van de verdachte niet haalbaar lijkt, bijvoorbeeld door gebrek aan bewijs. Ten tweede kan het openbaar ministerie seponeren wanneer het belang van vervolging niet opweegt tegen andere belangen.

Een transactie is een toezegging van de officier dat hij de verdachte niet zal vervolgen, wanneer deze aan bepaalde voorwaarden heeft voldaan. Deze voorwaarden houden meestal de betaling van een geldbedrag in. Gaat de verdachte op het aanbod in en betaalt hij het bedrag, dan is daarmee de zaak afgedaan. Er kan over deze zaak dan geen rechtszaak meer volgen.

## **Bijlage 1:**

### **Overige relevante informatie (optionele items)**

De behoefte aan informatie tussen organisaties kan verschillen. Om die reden is een beperkt aantal basis items geformuleerd. Daarnaast is een aantal gegevens geformuleerd die relevant kunnen zijn voor het eigen integriteitsbeleid. Hierbij is aangegeven op welk onderdeel zij betrekking hebben.

#### **A) Administratieve informatie**

##### ***Invoerende functionaris***

Bij de melding en afhandeling van (vermoedens van) integriteitsschendingen zijn meestal verschillende functionarissen betrokken (zoals een arbeidsjurist, een vertrouwenspersoon en natuurlijk het management). Juist vanwege deze veelheid aan functionarissen, is het aan te bevelen dat de organisatie vastlegt welke functionaris(sen) verantwoordelijk zijn voor het bijhouden van de registratie. Als meerdere personen een registratie bijhouden, dan is het wenselijk om bij elke casus ook de naam en de functie van de invoerder te vermelden.

##### ***Intern dossiernummer***

Het formulier is maar een beknopte weergave van mogelijk achterliggende dossiers. Om de registratie goed te kunnen bijhouden is daarom veelal een achterliggend intern dossiernummer nodig.

##### ***Meerdere betrokkenen***

Het kan voorkomen dat een betrokkene eerder geregistreerd is in het kader van een (vermoedelijke) integriteitsschending. Weliswaar moet voor elke betrokkene een apart formulier ingevuld worden, maar het kan handig zijn om een verband met andere formulieren te kunnen leggen op grond van een dossiernummer of andere relevante tekst.

##### ***Korte casusomschrijving en overige toelichtingen***

Soms is het wenselijk om in een korte casusomschrijving de schending en de omstandigheden kort te omschrijven. Het is daardoor gemakkelijker om de specifieke kwestie weer helder voor ogen te hebben zonder het hele dossier erbij te moeten pakken. Wel is het belangrijk om, in verband met de Wet Bescherming Persoonsgegevens, informatie te vermijden die, in combinatie met andere gegevens, direct herleidbaar is tot de melder(s) of de betrokkene(n). Dit betreft

vooral de naam, sekse, leeftijd en gedetailleerde informatie over de functie en werkplek. Dit geldt ook voor de overige mogelijkheden op het formulier om een korte toelichting te geven.

### ***Vertrouwenspersonen***

Vertrouwenspersonen adviseren medewerkers over integriteitskwesaties en over ongewenste omgangsvormen. Ook begeleidt en ondersteunt de vertrouwenspersoon de melder bij het aanklaarten van vermoedens van niet-integer handelen bij het bevoegd gezag. Daarnaast komt het voor dat de vertrouwenspersoon meldingen ontvangt die niet tot zijn of haar takenpakket behoren, zoals arbeidsconflicten. Het is wenselijk dat de vertrouwenspersoon de vragen en meldingen registreert die hij/zij ontvangt. In de registratie kan worden opgenomen dat er alleen advies is gegeven, of dat het geen integriteitskwesatie betrof. Op deze wijze kan de vertrouwenspersoon ook de overige werkzaamheden centraal registreren waardoor er geen gescheiden registraties nodig zijn voor de interne verantwoording.

## **B) Informatie over de melding**

### ***Specificeren van de melding***

Het specificeren van de interne en/of externe aanleiding is optioneel. Een interne aanleiding kan de directe collega zijn, maar ook een andere interne medewerker, leidinggevende, het bestuur of een standaard controle/audit waarbij bijvoorbeeld de interne accountantdienst verdachte zaken aantreft. De externe aanleiding is een persoon of instelling van buiten de organisatie. Denk hierbij aan een burger of bedrijf, de media, de politie of Rijksrecherche of overige opsporings- en inspectiediensten zoals de belastingdienst.

Aanvullend is een relevante vraag of de melder belanghebbende is in de zaak, bijvoorbeeld als slachtoffer.

### ***Meerdere melders***

Vooraf voor vertrouwenspersonen kan het wenselijk zijn om te registreren of er sprake is van meerdere melders. Ook staat bij bepaalde procedures, zoals de procedure ongewenste omgangsvormen, niet het onderzoek centraal, maar de vraag of de melder tevreden is over de afhandeling van de melding.

## C) Informatie over de betrokkene

### *Functionele kenmerken*

Naast de basiselementen kunnen ook andere functionele kenmerken van de betrokkene relevant zijn. Zo zijn het houden van risicoanalyses en het aanwijzen van kwetsbare functies onderdeel van een goed integriteitsbeleid dat voldoet aan de basisnormen integriteit. Voorbeelden van kwetsbare taken zijn:

- taken waar gelden en budgetten bij betrokken zijn;
- taken betreffende externe inhuur en inkoop;
- taken waarbij vertrouwelijke informatie betrokken is;
- taken rondom vergunningen en legitimatiebewijzen en inspectie en handhavende taken.

Ook is het bevoegd gezag verplicht om functies aan te wijzen die verplicht zijn tot het melden van hun financiële belangen.

Bij de politie is daarnaast het onderscheid tussen een executieve en niet-executieve politieambtenaar relevant vanwege de vergaande bevoegdheden waarover een executieve politieambtenaar beschikt. Binnen het openbaar bestuur kan het op vergelijkbare wijze relevant zijn om te registeren of de betrokkene een bijzonder opsporingsambtenaar (BOA) is.

Ook heeft de politie bijvoorbeeld ervaring opgedaan met het registeren van leeftijd en dienstjaren in categorieën.

### *Organisatieonderdeel*

Voor grote organisaties kan het relevant zijn om het organisatieonderdeel van de betrokkene te registeren. Op basis hiervan kan managementinformatie per organisatieonderdeel worden gegeven. Als ervoor wordt gekozen om op het laagste organisatieniveau te registreren, kan dit leiden tot de registratie van persoonsgegevens. Zo kent een afdeling veelal maar één leidinggevende waardoor deze als betrokkene snel herkenbaar is. In dergelijke gevallen is het beter om deze persoon onder een hoger organisatieonderdeel te registeren, of zelfs op algemeen organisatieniveau. Als dit wordt nagelaten, dan valt de registratie onder de Wet Bescherming Persoonsgegevens.

### *Naam van de betrokkene*

Als de naam van de betrokkene wordt geregistreerd, moet de organisatie voldoen aan de Wet Bescherming Persoonsgegevens.

## D) Type schendingen en conclusie onderzoek

In het modelformulier is per type schending een beperkt aantal subtype schendingen gespecificeerd. In bijlage 2 vindt u ook nog een aantal optionele subtypen. Daarnaast kan de organisatie nog type schendingen toevoegen die relevant zijn voor de eigen organisatie.

## E) Bestuurlijke en ambtelijke afdoening

### *Typen procedures*

Een casus kan worden opgepakt in het kader van de meerdere procedures. Vanwege mogelijk plichtsverzuim zal dit al snel een disciplinaire procedure zijn. Maar ook de procedure melden ongewenste omgangsvormen, de procedure melden misstand (klokkenluiders) en de klachtenprocedure burgers kunnen (naast elkaar) worden gebruikt.

### *Onderzoeksinstanties*

Als er is besloten tot een onderzoek, dan kunnen hierbij meerdere onderzoeksinstanties worden betrokken. Sommige organisaties beschikken over een intern bureau integriteit, andere dienen hiervoor een interne ad hoc commissie samen te stellen met bijvoorbeeld de leidinggevende en een arbeidsjurist. Ook kan de organisatie een extern onderzoeksbureau inhuren. Of verschillende commissies worden betrokken, zoals de commissie melden misstand (klokkenluiders), de klachten-commissie ongewenste omgangsvormen of de klachtencommissie burger.

### *Organisatorische maatregelen*

De meeste afdoeningen zijn gericht op de betrokkene. De afhandeling van de casus kan echter ook leiden tot organisatorische maatregelen. In dat geval heeft de organisatie lering getrokken uit de casus en zijn er maatregelen getroffen om herhaling te voorkomen. Voorbeelden zijn het aanpassen van procedures of het informeren van alle medewerkers van het organisatiestandpunt in een bepaalde kwestie.



## **F) Strafrechtelijk traject**

### ***Politie-/OM-zaaknummer***

Als de politie of het OM is ingeschakeld, dan is het zeer aan te raden om het politie-/OM-zaaknummer te noteren. Zonder zaaknummer is het namelijk moeilijk om informatie in te winnen over de afloop van een aangifte. Dit is een van de redenen dat het in de praktijk voorkomt dat de strafrechtelijke afdoening niet bekend is bij de organisatie die aangifte heeft gedaan.

### ***Sepot en artikel van Wetboek van Strafrecht***

Als het OM de zaak seponeert, is het aan te bevelen om de reden voor het sepot te noteren. Indien sprake is van vervolging en/of veroordeling is het aan te bevelen om het artikel van Wetboek van Strafrecht te noteren. Het artikel van Wetboek van Strafrecht geeft aan op grond van welk type schending het OM de zaak heeft kunnen vervolgen. Dat kan afwijken van de type schending op grond waarvan een bestuurlijk traject is ingezet.

## **G) Bezwaar en beroep bestuurlijk traject**

De betrokkene heeft het recht op bezwaar en (hoger) beroep tegen een bestuurlijke afdoening. Dit kan ertoe leiden dat deze (gedeeltelijk) in het gelijk wordt gesteld en de afdoening moet worden aangepast. De bezwaarprocedure wordt het meest toegepast en is gehouden aan wettelijke termijnen. Het is daarom relatief eenvoudig om bij te houden of een betrokkene bezwaar heeft ingediend en wat hiervan de uitkomst is. Daarnaast kan nog worden geregistreerd of de betrokkene vervolgens in beroep is gegaan en eventueel zelfs in hoger beroep en wat hiervan de uitkomst is.

## **H) Rectificatie en eerherstel betrokkene**

Voor de integriteit van de organisatie is het van belang om signalen over vermoedelijke schendingen serieus op te pakken. Het credo ‘waar rook is, is vuur’ blijkt echter vaak niet op te gaan. Bij een deel van de signalen blijkt tijdens het (voor) onderzoek dat de betrokkene geen schending heeft gepleegd. Soms kan dat pas worden aangetoond na een zwaar onderzoek waarbij de betrokkene in het belang van het onderzoek is geschorst. In dergelijke gevallen is het belangrijk om de betrokkene in ere te herstellen zodat deze opnieuw volwaardig kan functioneren in de organisatie.

Om het belang hiervan te benadrukken zijn enkele optionele items opgenomen over de wijze waarop in voorkomende gevallen eerherstel heeft plaatsgevonden en door welke functionaris dit is gedaan.



## Bijlage 2:

# Definities van de typen integriteitsschendingen

<b>1. Financiële schendingen</b>	
Diefstal / verduistering	Opzettelijk enig goed dat geheel of ten dele aan een ander toebehoort zichzelf toeëigenen.
Fraude	Betreft intern misbruik, zoals bij vervalsing van administratie of ontduiking van voorschriften. Een concreet voorbeeld is declaratiefraude. Doel van de fraude is materieel persoonlijk gewin.
Overig	Bijvoorbeeld afpersing, afdreiging en oplichting.
<b>2. Misbruik positie en belangenverstrengeling</b>	
Ongeoorloofde nevenactiviteiten	Het verrichten van nevenwerkzaamheden die de belangen van de organisatie (kunnen) schaden. Dit kan ook het niet melden van de (ongeoorloofde) nevenactiviteit omvatten als dat bijvoorbeeld aanleiding is voor een onderzoek of leidt tot een (disciplinaire) maatregel.
Ongeoorloofde financiële belangen	Het hebben van bepaalde financiële belangen of het verrichten van bepaalde financiële transacties kan oorzaak zijn van (de schijn van) belangenverstrengeling. Dit kan ook het niet melden van het (ongeoorloofde) financiële belang omvatten als dit bijvoorbeeld aanleiding is voor een onderzoek of leidt tot een (disciplinaire) maatregel.
Omkoping (corruptie)	Van corruptie is sprake wanneer een persoon een gift, dienst of belofte vraagt en/of aanneemt; en (vermoedelijk) als doel heeft om in zijn functie iets te doen of na te laten, al dan niet in strijd met zijn plicht. Zie verder WvS, art. 362.
Aannemen / vragen van geschenken, uitnodigingen etc.	Hieronder vallen zowel het aannemen van geschenken boven de vijftig euro, als ook het niet melden van geschenken.
Favoritisme	Oneigenlijke bevoordeling van medewerkers, vrienden, familie, partijgenoten.
Misbruik van legitimatiebewijs	In sommige functies kan een functioneel legitimatiebewijs misbruikt worden voor het verkrijgen van enig persoonlijk voordeel. Bijvoorbeeld om korting of gratis toegang te bedingen, of om toegang te verkrijgen tot anders niet toegankelijk terrein. Bijvoorbeeld een medewerker van de buitendienst die in zijn vrije tijd naar een afgesloten stuk strand gaat.

Overig	Voorbeelden zijn draaideurconstructies, vriendjespolitiek, deelname aan aannemingen en leveringen aan openbare diensten.
<b>3. Lekken en misbruik van informatie</b>	
Lekken van informatie	Het bewust of onbewust geven van informatie aan onbevoegde derden.
Misbruik van informatie	Het misbruik maken van informatie ten voordelen van de eigen persoon of derden, of ten nadelen van derden.
Raadplegen informatie uit vertrouwelijke registers	Het onbevoegd raadplegen van vertrouwelijke registers, of deze raadplegen voor andere doeleinden dan waarvoor deze bestemd zijn.
Verlies/diefstal informatiedragers	Verlies of diefstal van computers, laptops, usb-sticks, cd-roms et cetera.
Overig	Overige vormen van lekken en misbruik van informatie die de integriteit van de organisatie aantasten, bijvoorbeeld het achterhouden van informatie.
<b>4. Misbruik bevoegdheden</b>	
Ongeoorloofde opsporingsmethoden en dwangmiddelen	Het inzetten van bepaalde opsporingsmethoden en/of dwangmiddelen zonder de daarvoor vereiste officiële goedkeuring of zonder enige gegronde noodzaak.
Meineed	Het onder eed of belofte verkondigen van een onwaarheid.
Valsheid in geschrifte	Indien onwaarheid in officiële stukken wordt verkondigd. Ook het aanbrenge van veranderingen in stukken waarop moet kunnen worden vertrouwd, valt hieronder.
Afgifte van vergunningen en legitimatiebewijzen	Het in afwijking van geldende voorschriften afgeven van vergunningen, legitimatiebewijzen, sluiting van huwelijken en dergelijke.
Overig	Overige vormen van misbruik van bevoegdheden die de integriteit van de organisatie aantasten.
<b>5. Misbruik geweldsbevoegdheid</b>	
Fysiek geweld	Het niet subsidiair en proportioneel toepassen van geweld in de uitoefening van de functie.
Vuurwapengebruik	Het niet subsidiair en proportioneel toepassen van het vuurwapen in de uitoefening van de functie.

Overig	Overige vormen van het niet subsidiair en proportioneel toepassen van de geweldsbevoegdheid.
<b>6. Ongewenste omgangsvormen</b>	
Discriminatie	Discriminatie is het maken van een ongerechtvaardigd onderscheid (bijvoorbeeld in de vorm van een belediging of het achterstellen van individuen). Het betreft onderscheid op grond van godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht, nationaliteit, seksuele geaardheid, handicap, chronische ziekte of leeftijd.
Seksuele intimidatie	Variërend van dubbelzinnige opmerkingen, seksuele grappen of mededelingen over lichamelijke kenmerken tot aan ongewenste handtastelijkheden en poging tot aanranding en verkrachting.
Verbale agressie en geweld	Betreft verbaal geweld (uitschelden, treiteren, grapjes ten koste van) en psychisch geweld (bedreigen, intimideren, onder druk zetten, pesten). Kenmerk van pesten is dat het regelmatig voorkomt, vaak door dezelfde persoon of personen, gericht tegen dezelfde persoon of groep personen.
Fysieke agressie en geweld	Omvat onder andere slaan, schoppen, spugen en vernielen van eigendommen.
Overig	Overige ongewenste omgangsvormen die de integriteit van de organisatie aantasten.
<b>7. misbruik bedrijfsmiddelen en overtreding interne regels</b>	
Ongewenst gebruik e-mail / internet	Dit betreft niet alleen het (buitensporig) gebruikmaken van email/internet voor privédoeleinden, maar ook het gebruik van email/internet voor het bekijken en/of verspreiden van informatie die de integriteit van de organisatie aantast.
Misbruik van bedrijfsmiddelen	Het (buitensporig) gebruikmaken van bedrijfsmiddelen voor privédoeleinden. Zoals (mobiele) telefoon en bedrijfsauto.
Werkverzuim	Het op zodanige wijze niet naleven van werkuren of het misbruik maken van ziekteverzuim, dat disciplinair optreden passend is.
Niet volgen van de procedures	Door het niet naleven van procedures kan een goede taakvervulling van de organisatie in gevaar worden gebracht.

Slordig omgaan met bedrijfsmateriaal	Het op zodanig wijze omgaan met bedrijfsmateriaal dat deze beschadigd raken of zoekraken.
Gebruik van alcohol of drugs	Het op zodanig wijze gebruikmaken van alcohol- of drugs, dat disciplinair optreden passend is. Dit staat los van een eventuele begeleidingstraject met het bedrijfsmaatschappelijk werk.
Overig	Overige vormen van misbruik bedrijfsmiddelen en overtreding van interne regels die de integriteit van de organisatie aantasten.
<b>8. Misdragingen in privé-sfeer</b>	
Financiële schendingen	Zoals diefstal, fraude, oplichting
Ongewenste omgangsvormen	Zoals discriminatie, seksuele intimidatie en agressie en geweld. Dit kan ook huiselijk geweld betreffen.
Alcohol of drugs	Dit betreft niet alleen alcohol- en drugsmisbruik, maar ook (gelegenheid geven tot) drugshandel. Bijvoorbeeld door het kweken van hennepplanten.
Ongewenste contacten	Het onderhouden van ongewenste contacten in de privé-sfeer. Bijvoorbeeld het aangaan van een relatie met een persoon met criminele antecedenten.
Overig	Overige vormen van misdragingen in de privésfeer die de integriteit van de organisatie aantasten.
<b>9. Misstanden volgens de klokkenluidersregeling</b>	
<i>De specifieke invulling van de type misstanden hangt af van de klokkenluidersregeling die voor de eigen organisatie geldt.</i>	
Een schending van wettelijke voorschriften of beleidsregels.	
Een gevaar voor de gezondheid, de veiligheid of het milieu.	
Een onbehoorlijke wijze van functioneren die een gevaar vormt voor het goed functioneren van de openbare dienst.	

# Bijlage 3:

# Modelformulier registratie integriteitsschendingen

## Landelijk modelformulier Registratie integriteitsschendingen

<b>A Administratieve informatie</b> 1 Wat is de datum van de melding? _____ 2 Wat is de datum van afronding? _____ 3 Zijn er meerdere betrokkenen? <input type="checkbox"/> ja, aantal _____ <input type="checkbox"/> Nee		<b>E Bestuurlijke en ambtelijke afdoening</b> 13 Is er onderzoek gedaan? <input type="checkbox"/> ja, volledig feitonderzoek <input type="checkbox"/> ja, alleen vooronderzoek <input type="checkbox"/> Nee, geen onderzoek <input type="checkbox"/> Onbekend 14 Welke afdoening heeft er plaatsgevonden? (meerdere antwoorden mogelijk) <input type="checkbox"/> Geen <input type="checkbox"/> Onbekend <b>Disciplinair:</b> <input type="checkbox"/> Strafbotslag onvoorwaardelijk <input type="checkbox"/> Strafbotslag voorwaardelijk <input type="checkbox"/> Schriftelijke berisping onvoorwaardelijk <input type="checkbox"/> Overige disciplinaire afdoening <b>Overige afdoeningen:</b> <input type="checkbox"/> Overig ontslag (ongeschiedheidsomslag, zelf ontslag) <input type="checkbox"/> Ambtelijke afdoening (waarschuwingsbrief, coaching, ed)	
<b>B Informatie over de melding</b> 4 Is de melding afkomstig uit de eigen organisatie? <input type="checkbox"/> ja: interne melding <input type="checkbox"/> Nee: externe melding 5 Betreft het een melding in het kader van de klokkenluidersregeling? <input type="checkbox"/> ja <input type="checkbox"/> Nee 6 Betreft het een melding van Meldpunt MI? <input type="checkbox"/> ja (voor anonieme melders) <input type="checkbox"/> Nee		<b>F Strafrechtelijk inzicht</b> 15 Is de politie, het OM of de Rijksrecherche ingeschakeld? <input type="checkbox"/> ja, aangifte <input type="checkbox"/> Nee <input type="checkbox"/> ja, alleen melding <input type="checkbox"/> Onbekend 16 Wat is, indien van toepassing, de strafrechtelijke afdoening? <input type="checkbox"/> Niet bekend <input type="checkbox"/> Separering door OM <input type="checkbox"/> Transactie / boete <input type="checkbox"/> Veroordeling <input type="checkbox"/> Overig, namelijk _____	
<b>C Informatie over de betrokkene</b> (de – vermoedelijke – pleger van de schending) 7 Is bekend wie de – vermoedelijke – pleger van de schending is? <input type="checkbox"/> ja <input type="checkbox"/> Nee 8 Is de betrokkene in dienst van de organisatie? <input type="checkbox"/> ja <input type="checkbox"/> Nee <input type="checkbox"/> Onbekend 9 Heeft de betrokkene een leidinggevende functie? <input type="checkbox"/> ja <input type="checkbox"/> Nee <input type="checkbox"/> Onbekend 10 Is de betrokkene een bestuurder of volksvertegenwoordiger? <input type="checkbox"/> ja <input type="checkbox"/> Nee <input type="checkbox"/> Onbekend		<b>D Type schending en conclusie onderzoek</b> (U kunt meerdere type – vermoedelijke – schendingen aanwijzen) 11a <b>Financiële schendingen</b> <input type="checkbox"/> Diefstal / verduistering <input type="checkbox"/> Fraude <input type="checkbox"/> Overig, namelijk _____ 11b <b>Misbruik positie en belangenverstrengeling</b> <input type="checkbox"/> Nevenactiviteiten, financiële belangen <input type="checkbox"/> Omkoping (corruptie) <input type="checkbox"/> Geschenken, uitnodigingen. <input type="checkbox"/> Overig, namelijk _____ 11c <b>Lakken en misbruik van informatie</b> <input type="checkbox"/> Lekken, misbruik van informatie <input type="checkbox"/> Verlies/diefstal informatiedragers (laptop, usb-sticks ed.) <input type="checkbox"/> Overig, namelijk _____ 11d <b>Misbruik bevoegdheden</b> <input type="checkbox"/> Opsporingsmethoden, dwangmiddelen <input type="checkbox"/> Meeneed, valsheid in geschrifte <input type="checkbox"/> Afgifte vergunningen, identiteitsbewijzen <input type="checkbox"/> Overig, namelijk _____ 11e <b>Misbruik geweldsbevoegdheid</b> <input type="checkbox"/> Fysiek geweld <input type="checkbox"/> Vuurwapengebruik <input type="checkbox"/> Overig, namelijk _____ 11f <b>Ongewenste omgangsvormen</b> (met specificatie naar interne en externe benadeelde) <input type="checkbox"/> Intern (organisatie) <input type="checkbox"/> Extern (burger, bedrijf) <input type="checkbox"/> Discriminatie <input type="checkbox"/> Seksuele intimidatie <input type="checkbox"/> Verbale agressie en geweld <input type="checkbox"/> Fysieke agressie en geweld <input type="checkbox"/> Overig, namelijk _____ 11g <b>Misbruik bedrijfsmiddelen en overschrijding interne regels</b> <input type="checkbox"/> Misbruik en ongewenst gebruik van e-mail / internet <input type="checkbox"/> Misbruik van bedrijfsmiddelen (telefoon, auto ed.) <input type="checkbox"/> Overig, namelijk _____ 11h <b>Misdadigheden in privé-sfeer</b> <input type="checkbox"/> Namelijk _____	
11i <b>Mistanden volgens de klokkenluidersregeling</b> <input type="checkbox"/> Een schending van wettelijke voorschriften of beleidsregels <input type="checkbox"/> Een gevaar voor de gezondheid, de veiligheid of het milieu <input type="checkbox"/> Een onbehoorlijke wijze van functioneren die een gevaar vormt voor het goed functioneren van de openbare dienst		12 <b>Conclusie onderzoek per type schending</b> <input type="checkbox"/> Geen onderzoek <input type="checkbox"/> Conclusie onderzoek onbekend	
13 Vul het type schending in:		Aangeetoond <input type="checkbox"/> Weerlegd <input type="checkbox"/> Niet aangeetoond <input type="checkbox"/> Overig, namelijk _____ 1e <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 2e <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 3e <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 4e <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

## **Colofon**

### **Uitgave**

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties  
Vereniging van Nederlandse Gemeenten  
Interprovinciaal Overleg  
Unie van Waterschappen  
en vts Politie Nederland

### **Redactie**

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties  
Vereniging van Nederlandse Gemeenten  
Interprovinciaal Overleg  
Unie van Waterschappen  
en vts Politie Nederland

### **Vormgeving en print**

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties  
Directie Communicatie en Informatie / Grafische en Multimediale Diensten

Den Haag, oktober 2008