



**Nota Misbruik en Oneigenlijk gebruik  
(M&O) BSR 2024**

## Colofon

Titel: Nota Misbruik & Oneigenlijk gebruik (M&O)

Opdrachtgever: Dagelijks bestuur

Auteur: B.E. de Weerd, Business controller

Versie: 1.0

Vastgesteld op: 21 november 2024

## Inhoud

Colofon .....	2
1 Inleiding .....	4
2. Definities .....	5
3 Doelstelling en uitgangspunten .....	6
3.1 Doelstelling M&O-beleid .....	6
3.2 Rollen en verantwoordelijkheden .....	6
3.3 Uitgangspunten .....	7
3.4 Relatie M&O met rechtmatigheid, integriteit, fraude en ondermijning .....	7
3.5 Misbruik van data .....	8
4 Beheersmaatregelen ter voorkoming M&O .....	10
4.1 Preventieve maatregelen .....	10
4.2 Repressieve maatregelen .....	11
4.3 Sanctionering/maatregelenbeleid .....	11
4.4 Evaluatie .....	12
5 Risicogebieden .....	13
5.1 Intensiteit M&O-beleid .....	13
5.2 Risicovolle processen .....	13
6 Verantwoording .....	15

## 1 Inleiding

Met de invoering van de nieuwe rechtmatigheidsverantwoording wordt de toets op misbruik en oneigenlijk gebruik één van de voorwaarden waaraan het dagelijks bestuur de uitvoering van haar taken toetst op rechtmatigheid. Daarmee komt dit onderwerp nog nadrukkelijker op de agenda van het dagelijks bestuur en het algemeen bestuur.

Deze nota misbruik en oneigenlijk gebruik gaat over het geheel van maatregelen dat Belasting Samenwerking Rivierenland (BSR) neemt om misbruik en oneigenlijk gebruik van wet- en regelgeving zoveel als mogelijk te voorkomen en de gevolgen ervan te beperken. Deze maatregelen hebben betrekking op wet- en regelgeving, voorlichting, controlebeleid, sancties en evaluatie.

Dit overkoepelend beleid is daarmee een onderdeel van het toetsingskader bij de uit te voeren interne audits. De accountant doet bij de controle nog wel een uitspraak in hoeverre misbruik en oneigenlijk gebruik wordt voorkomen en bestreden en of de genomen maatregelen werken.

In de op 12 december 2024 vastgestelde "Verordening financieel beleid, beheer en organisatie (artikel 212 Gemeentewet) Belasting Samenwerking Rivierenland 2024" is in artikel 13 opgenomen dat het dagelijks bestuur de regels voor het voorkomen van misbruik en oneigenlijk gebruik van de regelingen en eigendommen verzorgt en vastlegt.

## 2. Definities

De commissie BBV<sup>1</sup> heeft in de kadernota Rechtmatigheid de volgende definities van misbruik en oneigenlijk gebruik (M&O) opgenomen. De commissie zorgt voor eenduidige uitvoering en toepassing van het BBV door decentrale overheden.

### Misbruik

*Het opzettelijk niet, niet tijdig, onjuist of onvolledig verstrekken van gegevens met als doel ten onrechte overheidssubsidies of -uitkeringen te verkrijgen of niet dan wel een te laag bedrag aan heffingen aan de overheid te betalen.*

Het opzettelijk niet, niet tijdig, onjuist of onvolledig verstrekken van informatie betreft een bewuste misleiding om een onrechtmatig of onwettig voordeel te behalen. Misbruik kan gelijk worden gesteld met het plegen van fraude om zich onrechtmatig overheidsgelden toe te eigenen. Niet elke misstap (fout) geldt als misbruik. Bij het maken van fouten is er meestal geen sprake van een opzettelijke handeling. Daarnaast is het begrip misleiding van betekenis in deze definitie. Misleiding heeft betrekking op het bewust verborgen houden van het misbruik.

'Misbruik' is onrechtmatig en telt mee als fout voor de Rechtmatigheidsverantwoording wanneer dit niet is gecorrigeerd en/of teruggevorderd.

Bij het bestrijden van misbruik passen beheersmaatregelen zoals misbruikpreventie, handhaving, misbruik en fraudeopsporing en sancties.

### Oneigenlijk gebruik

*Het door het aangaan van rechtshandelingen, al dan niet gecombineerd met feitelijke handelingen, verkrijgen van overheidsbijdragen of het niet dan wel tot een te laag bedrag betalen van heffingen aan de overheid, in overeenstemming met de bewoordingen van de regelgeving maar in strijd met het doel en de strekking daarvan.*

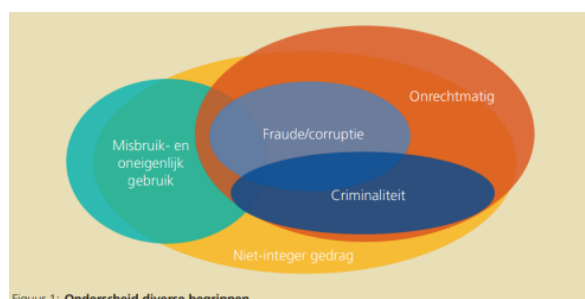
Bij oneigenlijk gebruik wordt feitelijk gehandeld in overeenstemming met wet- en regelgeving. Daarmee zijn dergelijke handelingen niet onrechtmatig. Wel is sprake van het in strijd handelen met het doel en de strekking ervan. Indien de wet- en regelgeving oneigenlijk gebruik mogelijk maakt (de "mazen van de wet") is het blijkbaar noodzakelijk dat de wet- en regelgeving wordt aangepast en/of duidelijker wordt toegelicht.

Misbruik is dus onrechtmatig, oneigenlijk gebruik niet.

### Fraude

*Dit omvat opzettelijke handelingen door één of meerdere personen binnen de organisatie, waarbij gebruik wordt gemaakt van misleiding teneinde een onrechtmatig of onwettig voordeel te behalen.*

Fraude is een vorm van bedrog. De zaken worden anders voorgesteld dan deze zijn, door op papier of digitaal een onjuiste weergave te geven van de werkelijkheid.



Figuur 1: Onderscheid diverse begrippen

In figuur 1 is het onderscheid tussen misbruik en oneigenlijk gebruik en criminaliteit, fraude, corruptie, onrechtmatig handelen, misbruik en oneigenlijk gebruik en niet-integer gedrag in beeld gebracht (Deloitte 2007).

<sup>1</sup> De regelgeving voor de begroting en de jaarstukken is vastgelegd in het Besluit begroting en verantwoording (BBV). De commissie heeft als doel nadere duiding te geven aan deze regelgeving.

## 3 Doelstelling en uitgangspunten

### 3.1 Doelstelling M&O-beleid

Het doel van het M&O-beleid is het voorkomen en bestrijden van misbruik en oneigenlijk gebruik van overheidsgelden.

In eerste instantie is het doel misbruik en oneigenlijk gebruik te voorkomen (preventief beleid). In tweede instantie ligt de focus op het achteraf controleren, het zo nodig bijstellen van beleidskaders en het repareren of zelfs bestraffen van M&O (repressief beleid).

Het is van belang om vast te stellen dat wij in de bedrijfsvoering effectieve maatregelen treffen om misbruik te voorkomen dan wel tijdig op te sporen en daarnaast dat de wet- en regelgeving duidelijk en te handhaven is. Op dit moment maken specifieke (beheers)maatregelen in het kader van M&O-beleid al onderdeel uit van de diverse processen van BSR. Het is wenselijk om overkoepelende algemene kaders vast te leggen in een nota M&O.

De redenen hiervoor zijn:

- Vastleggen van algemeen M&O-beleid draagt niet alleen bij aan transparantie en consistentie van het beleid. Het is ook behulpzaam bij het maken van afwegingen in hoeverre extra beheersmaatregelen en controles benodigd en tegelijkertijd doeltreffend zijn. Maatregelen die veel geld en energie kosten moeten worden voorkomen als deze slechts beperkt financieel nut opleveren.
- De betrouwbaarheid van door derden verstrekte gegevens kan niet altijd worden gegarandeerd via reguliere beheersingsinstrumenten, die vaak beperkt zijn tot de eigen organisatie. Specifieke maatregelen zijn nodig bij de controle op gegevens van derden.
- De werking van beheersmaatregelen en interne controle is voor een belangrijk deel afhankelijk van de integriteit van medewerkers. Het is mogelijk dat in de contacten tussen medewerkers en belanghebbenden bestaande procedures en interne controles onvoldoende effectief zijn. Het is dan ook goed om, in aanvulling op reguliere beheersmaatregelen, alert te zijn op deze risico's.
- Een wettelijk kader voor de invulling en uitvoering van M&O-beleid ontbreekt. Het is alleen een gegeven dat M&O een rechtmatigheidscriterium is en dat wettelijke eisen in specifieke regelingen zijn opgenomen.

### 3.2 Rollen en verantwoordelijkheden

Het in deze nota geformuleerde beleid vormt een kapstok voor de opsomming en inkadering van bestaand beleid en bevat geen nieuwe regels.

Rollen en verantwoordelijkheden zijn in lijn met de inrichtingsprincipes van de organisatie. Het managementteam van BSR is verantwoordelijk voor het actueel houden van het specifieke M&O-beleid en het treffen van passende M&O-beheersmaatregelen voor de risicogebieden.

Ook leggen directie en management verantwoording af over de wijze waarop het M&O-beleid wordt uitgevoerd en wordt nageleefd.

Het dagelijks bestuur ziet erop toe dat directie en management deze taak oppakken en dat waar nodig risico's tijdig worden besproken. Het algemeen bestuur vervult een kaderstellende rol door het beleid en de periodieke actualisaties daarvan vast te stellen.

Samengevat kan als doelgroep voor dit M&O-beleid worden aangemerkt:

- **het algemeen bestuur**, die het M&O-beleid vaststelt;
- **het dagelijks bestuur**, ter ondersteuning om toe te zien op uitvoering, controle en evaluatie van het M&O-beleid;
- **de ambtelijke organisatie**, als hulpmiddel om in de uitvoering, controle en evaluatie ten aanzien van op te stellen regelgeving bewust de aandacht op M&O-aspecten te vestigen en passende preventieve dan wel repressieve maatregelen te nemen, dan wel bewust te onderbouwen waarom van maatregelen wordt afgezien.

### 3.3 Uitgangspunten

De volgende uitgangspunten liggen ten grondslag aan het M&O-beleid van BSR:

1. Wij werken vanuit een basishouding van vertrouwen in een juiste omgang met collega's, inwoners, gemeenten, instellingen en bedrijven.
2. Maatregelen die worden getroffen ter bevordering van een juist gebruik van de verordening en bedrijfsvoering zijn proportioneel. Dat wil zeggen dat zij in verhouding moeten staan tot de risico's die worden gelopen. Beheersmaatregelen worden ingezet op basis van een analyse van de risico's en na afweging van de kosten en baten.
3. De beheersmaatregelen zijn zowel extern als intern gericht. Intern kijken wij naar ons eigen handelen. Extern geldt dat zaken niet de deur uitgaan zonder toetsing aan de geldende wetgeving.
4. De betrouwbaarheid van aangeleverde informatie, afgezet tegen het mogelijk optreden van risico's, is bepalend voor de mate van controle en eventuele sanctionering.
5. Voorkomen is beter dan genezen. De inzet van beleid en maatregelen is primair gericht op preventie van misbruik en oneigenlijk gebruik van de regelingen.
6. Van derden ontvangen gegevens worden indien mogelijk gecontroleerd.
7. Na constatering van een overtreding wordt de rechtmatige situatie zo snel als mogelijk hersteld en zo nodig worden er passende maatregelen getroffen.
8. Directie en management zijn verantwoordelijk voor het nemen van beheersingsmaatregelen om misbruik en oneigenlijk gebruik te voorkomen.
9. Deze nota M&O actualiseren wij eens in de vier jaar of eerder als daarvoor specifieke aanleiding is. Actualiseren is van belang voor het op orde houden van de maatregelen ter bestrijding van misbruik en oneigenlijk gebruik en voor het alert houden van de organisatie.

### 3.4 Relatie M&O met rechtmatigheid, integriteit, fraude en ondermijning

#### *Rechtmatigheid*

Misbruik en oneigenlijk gebruik is één van de drie criteria van rechtmatigheid. Misbruik en oneigenlijk gebruik heeft een relatie met rechtmatigheid, in die zin dat misbruik een onrechtmatige handeling is, maar dit is bij oneigenlijk gebruik niet het geval. Bij oneigenlijk gebruik wordt feitelijk gehandeld in overeenstemming met wet- en regelgeving.

#### *Integriteit*

Integriteit richt zich op de eigen organisatie en medewerkers en is intern gericht. Intern gelden de gedragscode integriteit BSR, de ambtseed, functiescheiding in (financiële) processen, maar ook aanspreekgedrag en collegiale toetsing. De interne auditor toetst steekproefsgewijs of deze waarborgen ook structureel worden toegepast en of ze effectief zijn.

De Gedragscode integriteit BSR geeft uitgebreide richtlijnen voor medewerkers op het gebied van o.a.:

1. Goed ambtenaarschap (eed of belofte);
2. Vertrouwelijk omgaan met gevoelige informatie (Gedragscode integriteit BSR H1);
3. Verantwoord omgaan met organisatievoorzieningen en personeelsregelingen (Gedragscode integriteit BSR H2);
4. Nevenfuncties en andere privé-activiteiten (Gedragscode integriteit BSR H3);
5. Belangen van familieleden, vrienden en ex-collega's (Gedragscode integriteit BSR H4);
6. Geschenken, aanbiedingen en incidentele vergoedingen (Gedragscode integriteit BSR H5 en H6);
7. Uitnodigingen voor reizen, congressen, evenementen en diners (Gedragscode integriteit BSR H7);
8. (Schijn van) belangenverstremgeling (Gedragscode integriteit BSR H8);
9. Gewenst en ongewenst gedrag (Gedragscode integriteit BSR H9);
10. Handelwijze bij (het vermoeden van) een misstand (Gedragscode integriteit BSR H10);
11. Te nemen maatregelen door BSR (Gedragscode integriteit BSR H11).

### *Fraude*

Misbruik en oneigenlijk gebruik gaat zowel over mogelijkheden voor fraude, diefstal of andere vormen van zelfverrijking in de organisatie, ambtelijk en bestuurlijk, als over misbruik van regelingen door burgers, bedrijven en instellingen. De meeste regelingen bevatten waarborgen om misbruik te voorkomen. In ieder geval middels de voor die regelingen geldende voorwaarden (voorwaardencriterium).

Daarnaast is in onze interne procedures geborgd dat bij het nemen en uitvoeren van besluiten altijd toepassing gegeven wordt aan de Algemene beginselen van behoorlijk bestuur<sup>2</sup>. Zo bevatten alle besluiten een grondslag en een motivatie. Voor belanghebbenden bestaat altijd de mogelijkheid van bezwaar en beroep om dit te toetsen.

### *Ondermijning*

Een bijzondere vorm van misbruik is 'ondermijnende criminaliteit'. Als de bovenwereld en onderwereld met elkaar verweven raken, noemen we dat ondermijning. Voorbeelden zijn wietplantages of xtc-labs in loodsen of woningen en het witwassen van geld via bedrijven.

Om illegale praktijken te kunnen uitvoeren, maken criminelen vaak gebruik van de bovenwereld. Denk daarbij aan transport, opslag, huisvesting en financiële voorzieningen. Deze verwevenheid heeft vergaande consequenties. Door de invloed en ongewenste druk van criminelen vervagen normen en waarden en wordt, soms zonder dat we het meteen merken, onze veiligheid aangetast. De consequenties van ondermijning worden een steeds groter probleem voor de samenleving als deze niet worden aangepakt.

De Wet Bevordering Integriteitsbeoordelingen (Wet Bibob) staat voor bevordering integriteitsbeoordeling door het openbaar bestuur. Door middel van de Wet Bibob kan BSR bijvoorbeeld voorkomen dat er onbedoeld medewerking wordt verleend aan misbruik van aanbestedingsopdrachten.

## 3.5 Misbruik van data

Misbruik en oneigenlijk gebruik heeft niet alleen betrekking op misbruik van middelen. Het kan ook gaan om misbruik van data. Dit kan een inbreuk op privacy betreffen met identiteitsfraude als meest vergaande vorm. Het kan gaan om het lekken van vertrouwelijke informatie of persoonsgegevens.

### *Algemene Verordening Gegevensbescherming (AVG)*

Om persoonsgegevens van de inwoners binnen Europa beter te beschermen, is vanaf 25 mei 2018 de Europese privacywet van kracht, namelijk de Algemene Verordening Gegevensbescherming (AVG). Voorbeelden van persoonsgegevens zijn: naam, adres, geboortedatum, BSN, medische informatie en geloofsovertuiging. De AVG legt vast dat persoonsgegevens alleen verzameld en bewaard mogen worden als daar een wettelijke grondslag voor is en zo lang dat strikt noodzakelijk is.

---

<sup>2</sup> Bij besluitvorming zijn wettelijke regels en ongeschreven recht van toepassing. Het ongeschreven recht zijn de Algemene beginselen van behoorlijk bestuur.



BSR houdt een register bij met een beschrijving van alle processen en de persoonsgegevens die daarin verwerkt worden. Als andere organisaties persoonsgegevens verwerken in opdracht van BSR worden hierover afspraken gemaakt en vastgelegd in een verwerkersovereenkomst. In de organisatie zijn specifieke functionarissen hiervoor actief bestaande uit de Functionaris Gegevensbescherming (FG), de Chief Information Security Officer (CISO) en de Privacy Officer (PO).

*Baseline Informatiebeveiliging Overheid (BIO)*

Informatiebeveiliging is de verzamelnaam voor de processen die ingericht worden om de betrouwbaarheid van BSR-processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen misbruik en oneigenlijk gebruik. Hierbij is de Baseline Informatiebeveiliging Overheid (BIO) het belangrijkste kader. Vanaf 1 januari 2020 is deze van kracht. Hiermee ontstaat één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek. De uitwerking van dit kader is vastgelegd in het Strategisch Informatiebeveiligingsbeleid BSR.

## 4 Beheersmaatregelen ter voorkoming M&O

Bepaalde regelingen en processen (of onderdelen daarvan) kunnen het risico van misbruik of oneigenlijk gebruik met zich meedragen. Meer specifiek is dit het geval als er sprake is van afhankelijkheid van gegevens die derden aan BSR verstrekken.

Wettelijke eisen en minimumnormen verbinden aan de meeste regelingen de verplichting om maatregelen ter bestrijding van fraude en misbruik te treffen. Hierbij worden maatregelen ingezet uit landelijke wetgeving en regelgeving van BSR. Daarnaast zijn extra beheersmaatregelen denkbaar die het risico van misbruik en oneigenlijk gebruik verder terugdringen.

Ook beheersmaatregelen die intern zijn gericht zijn relevant. Het gaat dan om zaken zoals functiescheiding, toegangsrechten tot applicaties, regelmatige controle daarvan, het vastleggen van gebeurtenissen in log-ins, en rapportages over deze maatregelen.

Een onderscheid kan worden aangebracht tussen preventieve en repressieve maatregelen (of een mix daarvan).

### 4.1 Preventieve maatregelen

Preventieve maatregelen zijn maatregelen die liggen vóór het moment van beschikken, aanslagoplegging en restitutie. Preventieve maatregelen betreffen regelgeving, voorlichting en controle vooraf. Zij zijn gericht op het voorkomen van misbruik en oneigenlijk gebruik van regelingen.

#### *Regelgeving*

Heldere en eenduidige regelgeving beperkt de ruimte voor misbruik en oneigenlijk gebruik. Onder regelgeving wordt verstaan: verordeningen en beleidsregels.

Adequate en handhaafbare regelgeving is een belangrijke beheersmaatregel in het kader van M&O-beleid en voldoet in dat verband aan de volgende eisen:

- eenvoud, inzichtelijkheid en begrijpelijkheid;
- er gelden eenduidige definities;
- het doel en de doelgroep van de regeling is nauwkeurig bepaald;
- rechten, plichten en voorwaarden zijn opgenomen;
- er zijn geen overbodige en/of met elkaar strijdige bepalingen;
- de afhankelijkheid van gegevens afkomstig van derden is zoveel mogelijk beperkt;
- mogelijke maatregelen of sancties bij geconstateerd misbruik en oneigenlijk gebruik zijn in de regeling opgenomen;
- ingangsdata en overgangsregels zijn in de regeling opgenomen.

#### *Voorlichting*

Wet- en regelgeving wordt door middel van voorlichting onder de aandacht gebracht van belanghebbenden (collega's, inwoners, gemeenten, instellingen en bedrijven).

Er dient informatie te worden verstrekt over het bestaan van een regeling, aard en doel van de regeling, de specifieke doelgroep, geldende voorwaarden en controle- en sanctiebeleid.

Voorlichting draagt in preventieve zin bij aan het voorkomen van misbruik en oneigenlijk gebruik van een regeling, zeker als ook duidelijk wordt gecommuniceerd over mogelijke sancties.

#### *Controle vooraf*

Controle in de uitvoering is een middel om (de kans op) misbruik of oneigenlijk gebruik te signaleren. Mogelijke M&O gevallen kunnen al in een vroegtijdig stadium worden waargenomen.

Controle vooraf van gegevens wordt uitgevoerd tot aan het moment van betaling of beschikkingsverlening en geldt daarmee als preventieve maatregel. Controle vooraf richt zich op de toetsing van de juistheid en volledigheid van gegevens die door derden zijn verstrekt. Door betrokkene(n) aangeleverde gegevens worden indien mogelijk geverifieerd. Uitgangspunt is dat, voordat wordt beschikt, uitbetaald of een uitspraak wordt verstuurd, een andere medewerker controleert of deze werkzaamheden zichtbaar, volledig en juist zijn uitgevoerd (vier-ogen principe).

In beleid wordt bepaald welke controlemethoden worden gebruikt ten aanzien van regelingen. Controles kunnen variëren van integraal (totale controle), steekproefsgewijs tot incidenteel. Hierbij is van belang: de aard en omvang van de doelgroep en hoe misbruikgevoelig een regeling is.

Processen waarbij gevoeligheden spelen, moeten voldoende maatregelen bevatten om de tijdigheid, juistheid, volledigheid en prestatielevering te toetsen van door belanghebbende(n) verstrekte gegevens.

Mechanismen controle vooraf:

- Administratieve organisatie (AO)  
Door middel van stapsgewijze werkprocessen en deels geautomatiseerde processen is gewaarborgd dat vereiste gegevens worden aangeleverd, beoordeeld en gearchiveerd;
- Integriteitsvoorschriften  
Onder andere in het Integriteitsbeleid, de Gedragscode Integriteit voor medewerkers, Tactisch informatie beveiligingsbeleid BSR, Strategisch informatie beveiligingsbeleid BSR en het Operationele informatie beveiligingsbeleid BSR;
- Fraudeprotocol;
- Opstellen Risico analyse & auditplanning;
- Mandaatstructuur  
Deze is ook verankerd in de financiële applicaties en de belastingapplicaties;
- Inkoop- en aanbestedingsbeleid en inkoopvoorwaarden.

## 4.2 Repressieve maatregelen

Repressieve maatregelen zijn maatregelen die na het moment van beschikken of betalen worden genomen. Het gaat om controle achteraf, waarbij M&O kan worden vastgesteld, en sanctionering/maatregelenbeleid.

### *Controle achteraf*

Controle van gegevens achteraf wordt uitgevoerd na het uitkeren/innen van bedragen, dan wel nadat de beschikking is verleend. Daarmee is het een repressieve maatregel.

Controles achteraf kunnen (evenals bij controles vooraf) integraal, steekproefsgewijs of incidenteel worden uitgevoerd. Manieren om te controleren kunnen zijn: verzoeken om inlichtingen, inspecties, waarneming, bevestigingen, herberekeningen, cijferanalyses en het opnieuw uitvoeren van controles.

Interne controles worden periodiek uitgevoerd om te beoordelen of conform de interne procedures is gewerkt en of transacties getrouw en rechtmatig tot stand zijn gekomen. In de uitvoering van de controles is expliciet aandacht voor M&O. Vastlegging van de controleresultaten is verplicht. De resultaten van de controle kunnen bijvoorbeeld leiden tot aanpassing van het controlebeleid en/of de regelgeving.

Periodiek wordt een geactualiseerd intern controleplan bedrijfsvoering door het dagelijks bestuur vastgesteld. Dit vormt de basis voor de audits en de verantwoording daarover in de jaarstukken en vanaf 2025 in de bestuursrapportage.

### *Verbijzonderde interne controle.*

De (V)IC is in feite een check op de toepassing en functionaliteit van de AO. De Interne Controle (IC) wordt uitgevoerd door de afdelingen zelf, door medewerkers die zelf bevoegdheden hebben in de gecontroleerde processen. De werkwijzen, conclusies en aanbevelingen van de IC-medewerkers worden aanvullend getoetst door de auditor van de afdeling Bedrijfsvoering & Innovatie.

## 4.3 Sanctionering/maatregelenbeleid

Sancties worden opgelegd als reactie op een vaststelling van misbruik. Alleen misbruik is immers onrechtmatig en moet worden hersteld en/of passende maatregelen worden genomen.

Maatregelenbeleid is vereist om adequaat te reageren op geconstateerd misbruik en/of oneigenlijk gebruik. Maatregelenbeleid moet voldoen aan de beginselen van behoorlijk bestuur. Dit houdt onder andere in dat maatregelen en sancties proportioneel moeten zijn in relatie tot het vergrijp.

Uitgangspunt is dat het behaalde voordeel wordt teruggevorderd en er indien nodig maatregelen worden getroffen.

Concreet leidt het tot terugvordering van te veel betaalde bedragen, naheffing van ten onrechte gederfde ontvangsten. In bepaalde gevallen kan ook de ontbinding van een overeenkomst of de intrekking van een erkenning als niet-financiële sancties worden opgelegd.

In geval van een misdrijf (fraude of diefstal) wordt aangifte gedaan bij de politie. Van sanctionering gaat een afschrik-effect uit en dit draagt om die reden eveneens bij aan het voorkomen en beperken van misbruik van regelingen.

#### 4.4 Evaluatie

Regelgeving wordt veelal periodiek geëvalueerd. In een evaluatie dient ook plaats te zijn voor de effectiviteit van genomen maatregelen ter voorkoming van misbruik en oneigenlijk gebruik en de toereikendheid van verschillende controlewerkzaamheden. De auditor neemt dit op in het auditplan vanaf 2025 en rapporteert twee keer per jaar de status aan het MT.

Het M&O beleid kan hierop worden aangepast.

## 5 Risicogebieden

M&O-beleid wordt toegepast bij regelingen waar een risico bestaat op misbruik en oneigenlijk gebruik. Afhankelijk van de misbruikgevoeligheid van een regeling wordt de intensiteit van de inzet van beheersmaatregelen bepaald. In dit hoofdstuk worden de risicogebieden beschreven waarop M&O-beleid van toepassing is. Daarbij wordt de intensiteit van de inzet van het M&O-beleid benoemd en onderbouwd.

### 5.1 Intensiteit M&O-beleid

Afhankelijk van de mate van een M&O-risico wordt een streng, een gematigd of een basis beleid gevoerd. De hoogte van een risico is afhankelijk van de kans dat het zich voordoet en de (financiële) impact die het heeft.

#### *Streng M&O-beleid*

Streng M&O-beleid omvat beheersmaatregelen die verder gaan dan de reguliere maatregelen op het gebied van de administratieve organisatie en interne controle (AO/IC). Specifieke en aanvullende (controle)maatregelen zijn noodzakelijk, zowel in voorwaardenscheppende sfeer als voor wat betreft het houden van een actief toezicht daarop.

#### *Gematigd M&O-beleid*

Gematigd M&O-beleid houdt in dat waakzaamheid is geboden. Enkele aanvullende maatregelen worden getroffen, zoals een actieve voorlichting en een kritische beoordeling van de onderbouwing en herkomst van door derden aangeleverde gegevens (b.v. verscherpte controles).

#### *Licht M&O-beleid*

Licht M&O-beleid kan worden toegepast in het geval dat de reguliere AO/IC toereikend is. Er zijn geen aanvullende maatregelen noodzakelijk (te denken valt aan een adequate functiescheiding). Uiteraard moet er wel aandacht zijn voor heldere en eenduidige regelgeving en actieve voorlichting.

#### *Geen specifiek M&O-beleid*

Als de regulier AO/IC toereikend is, zijn geen aanvullende maatregelen noodzakelijk en kan incidentele controle op misbruik en oneigenlijk gebruik plaatsvinden.

### 5.2 Risicovolle processen

Regelingen waarbij de informatie van andere partijen bepalend is voor het verlenen en vaststellen van een indicatie, zijn gevoelig voor misbruik en oneigenlijk gebruik. Ook interne processen kunnen M&O-gevoelig zijn.

De volgende processen worden aangemerkt als risicogebieden omdat derden een aanmerkelijk (financieel) belang hebben en BSR in grote mate afhankelijk is van door die derden verstrekte gegevens:

#### *1. Heffingen en belastinginkomsten (licht M&O-beleid)*

De belastinginkomsten voor deelnemers van BSR worden grotendeels gerealiseerd door watersysteemheffing, zuiveringsheffing, ozb, afvalstoffenheffing en rioolrechten. De hoogte van deze belastingen wordt gebaseerd op redelijk objectieve criteria of op gegevens van niet-betrokken derden.

Er is ook een groep belastingen/heffingen waarbij rechtstreeks toetsbare gegevens ontbreken zoals de Reclamebelasting, Verblijfsbelasting/toeristenbelasting en forensenbelasting.

Bij de verblijfsbelasting/toeristenbelasting gaan we in beginsel uit van de aangifte van de inwoner/ondernemer die de mogelijkheid biedt tot overnachting. Jaarlijks worden deze aangiftes wel steekproefsgewijs gecontroleerd in opdracht van de deelnemers.

De forensenbelasting kan alleen gecontroleerd worden waar dit geldt voor o.a. vakantieparken. Voor het overige wordt uitgegaan van het eerlijk doorgeven door de belastingplichtige.

Tenslotte is er een groep overige belastingen waarbij BSR volledig afhankelijk is van de informatie van derden, zoals de hondenbelasting en de reclamebelasting o.b.v. de oppervlakte van de reclame-uiting. Hier is specifiek M&O-beleid wat minder relevant.

## *2. Kwijtscheldingen (gematigd M&O-beleid)*

Ook de procedure van kwijtschelding is risicogevoelig, omdat deze bij automatische verlening sterk afhankelijk is van de juistheid van inkomensregelingen. Hier zijn aanvullende M&O maatregelen nodig en daarmee een gematigd M&O beleid.

## *3. Inkopen en aanbestedingen (gematigd M&O-beleid)*

Met inkoop en aanbesteding kan een aanmerkelijk financieel belang gemoeid zijn. Wet- en regelgeving en ook het inkoopbeleid van BSR bevatten echter al de nodige waarborgen op het gebied van M&O.

Reeds van toepassing zijnde (verbijzonderde) interne controles op inkopen en aanbestedingen zijn eveneens een waarborg dat deze juist en volledig zijn.

Ook interne budget- en functiescheidingen zijn van toepassing.

Aanvullende M&O-maatregelen kunnen zich beperken tot enkele extra controles van aangeleverde gegevens. Daarom geldt voor inkopen en aanbestedingen een gematigd M&O-beleid.

Voor aanvullende opdrachten (meerwerk) en opdrachten die één-op-één gegund worden is tevens een gematigd beleid noodzakelijk, omdat hierop mogelijk niet alle voorstaande beheersmaatregelen worden toegepast.

Een mogelijke vorm van misbruik is dat iemand zich wil verrijken door een nepfactuur naar BSR te sturen in de hoop dat deze wordt betaald, terwijl de prestatie niet (geheel) is geleverd. Ook kan het voorkomen dat een medewerker zaken bestelt op rekening van BSR maar die ongeoorloofd privé gebruikt (intern).

## *4. Integriteit van relaties (gematigd M&O-beleid)*

Integriteit van medewerkers en directie in de omgang met externe relaties vormt een M&O-risico.

Preventieve maatregelen in de zin van integriteitbeleid en gedragscodes zijn al van kracht.

M&O beleid kan dan ook beperkt zijn tot het treffen van enkele aanvullende maatregelen, waardoor een gematigd beleid volstaat.

## *5. Personeelslasten (licht M&O-beleid)*

De interne controle op personeelslasten is goed georganiseerd. Enkele belangrijke aandachtspunten zijn: kopie identiteitsbewijs, formele aanstelling, controle buiten de personeelsadministratie om en Verklaring Omtrent Gedrag.

Een nuance geldt wellicht voor kostenvergoedingen. Hierbij valt te denken aan het verkrijgen van een vergoeding voor gemaakte reiskosten, terwijl deze kosten door een persoon niet juist opgegeven worden of dat de juiste grondslag ontbreekt. Deze controle vindt plaats in de eerste lijn (manager).

De salarisadministratie wordt uitgevoerd door een externe partij.

Het risico is dat een (fictieve) medewerker wordt opgevoerd in de salarisadministratie of dat het salaris of aantal uren te hoog wordt ingegeven in het salarissysteem. Het financiële belang hiervan is in het algemeen echter beperkt. Hierbij moet wel sprake zijn van een goede functiescheiding.

## 6 Verantwoording

Om inzicht te krijgen in de wijze waarop het M&O-beleid wordt uitgevoerd en nageleefd, moet verantwoording worden afgelegd. Dit wordt gerealiseerd door aan te sluiten bij de reguliere Planning & Control cyclus.

In het kader van de verantwoording worden in ieder geval de volgende stappen ondernomen:

- Vanaf de begroting 2026 wordt in de paragraaf Bedrijfsvoering informatie opgenomen over het M&O-beleid;
- Vanaf de bestuursrapportage 2025 wordt in de paragraaf Bedrijfsvoering gerapporteerd over de voortgang in het M&O;
- Vanaf de jaarrekening 2025 wordt verantwoordingsinformatie over het M&O beleid opgenomen;
- Bij het verrichten van interne controles, audits en onderzoeken wordt aandacht besteed aan het M&O-beleid;
- Bij het opstellen van procesbeschrijvingen, in het kader van de administratieve organisatie, wordt rekening gehouden met M&O-gevoelige aspecten.