Dienst Justis
Ministerie van Veiligheid en Justitie

Evaluatie Wet Controle op Rechtspersonen

Een verslag over doeltreffendheid en effecten van de wet in de praktijk

Inhoud

Samenvatting 4

1. Inleiding 6
   1. Toezicht op rechtspersonen 6
   2. Opbouw 8

2. Output van het toezicht 9
   1. Verstrekte producten 9
   2. Acties naar aanleiding van signalen 12

3. Inrichting van het toezicht 16
   1. Ontwikkeling RADAR 16
   2. Wet bescherming persoonsgegevens 16

4. Samenwerking in het netwerk 19
   1. Samenwerking op het gebied van risicomeldingen 19
   2. Samenwerking op het gebied van netwerkanalyses 23
   3. Uitbreiding van het netwerk 25

5. Slotopmerkingen en aanbevelingen 26

6. Bijlage 29

Samenvatting

De Wet controle op rechtspersonen heeft tot doel om door middel van een doorlopend toezicht op rechtspersonen de aanpak van misbruik van rechtspersonen te verbeteren. Dit toezicht wordt gerealiseerd door samenwerking tussen een groot aantal partijen. Binnen deze samenwerking vervult Justis een centrale rol door op basis van verschillende bronnen producten op te stellen die de afnemers, de handhavende en opsporende instanties, ondersteunen in de uitvoering van hun taken. De Wet controle op rechtspersonen is op 1 juli 2011 in werking getreden. Vanaf dat moment is door Justis het (nieuwe) toezicht op rechtspersonen van de grond af opgebouwd, ingericht en geprofessionaliseerd. In de periode van 1 juli 2011 tot 1 juli 2013 is veel aandacht besteed aan het vormgeven van het toezicht, het opbouwen van relaties met de netwerkpartners en het opdoen van ervaring met het toezicht.

Justis levert in het kader van het toezicht op rechtspersonen een drietal producten: risicomeldingen uit het systeem, risicomeldingen op verzoek en netwerkanalyses. Het doorlopende toezicht op rechtspersonen kenmerkt zich door een zogenaamde 'trechterwerking'. In totaal is toezicht gehouden op ongeveer 1 miljoen rechtspersonen, bij wie in twee jaar tijd circa 1,5 miljoen wijzigingen in het Handelsregister plaatsvonden. Ongeveer 200.000 van die wijzigingen leidden tot een automatische analyse door het systeem, waarbij in 1.368 van de gevallen een systeemmelding werd aangemaakt en in behandeling werd genomen. In 37 van deze gevallen werd naar aanleiding van deze systeemmelding een risicomelding verstrekt aan één of meer afnemers. Daarnaast zijn op verzoek van afnemers nog eens 28 risicomeldingen en 1.158 netwerkanalyses verstrekt.

Uit de terugkoppelingen die van de afnemers zijn ontvangen, is op te maken dat de producten op verschillende wijzen van toegevoegde waarde zijn geweest bij het tegengaan van misbruik van rechtspersonen. Enerzijds zijn door afnemers preventieve vervolgstappen genomen om toekomstige schade te voorkomen en anderzijds zijn onder meer politie en OM betrokken bij het nemen van repressieve vervolgstappen.

Voor een optimale werking van het toezicht op rechtspersonen is het van belang dat het werkproces efficiënt is ingericht en dat bronnen op een juiste manier worden ontsloten. Daartoe zijn op basis van opgedane ervaringen en contact met netwerkpartners aanpassingen doorgevoerd. Zo worden steeds nieuwe risicoprofielen ontwikkeld en worden de bestaande profielen aangescherpt. Daarnaast wordt door het inbouwen van

verschillende waarborgen een juiste omgang met de te verwerken persoonsgegevens gegarandeerd.

Binnen het netwerk waarin het toezicht op rechtspersonen wordt uitgevoerd speelt Justis een centrale rol. Vanuit deze rol onderhoudt Justis op verschillende manieren contact met alle betrokken instanties. Zo wordt op meerdere niveaus overleg gevoerd met de partners binnen het netwerk en wordt afnemers standaard om een terugkoppeling gevraagd. Daarmee wordt ingezet op een zo goed mogelijke aansluiting bij de wensen en behoeften van de verschillende partners wat de doeltreffendheid en effectiviteit van het toezicht ten goede komt. Bovendien biedt deze wijze van overleg de mogelijkheid om de brede aanpak van misbruik van rechtspersonen steeds beter vorm te geven.

In de toekomst zal worden ingezet op borging en verdere uitbreiding van het toezicht zoals dat in eerste twee jaar is opgebouwd. Daartoe is een drietal concrete aanbevelingen gedaan:

1. Versterking van het netwerk
Het is noodzakelijk dat de ingezette weg van plenair en bilateraal overleg op verschillende niveaus met de netwerkpartners wordt geborgd.
Het verdient aanbeveling onderzoek te doen naar de mogelijkheden meer organisaties als afnemer aan te merken opdat het toezicht op rechtspersonen effectiever wordt.

2. Versterking van de informatiepositie
Het verdient aanbeveling de centrale en unieke informatiepositie die Justis inneemt in het netwerk van toezicht op rechtspersonen verder te verbeteren en te versterken om een adequate taakuitvoering door Justis te waarborgen. De informatiepositie kan verder worden versterkt door het wegnemen van belemmeringen in de samenwerking met netwerkpartners, het uitbreiden van de aansluiting op zowel bestaande als toekomstige bronnen.

3. Technische wijziging van regelgeving.
Om onduidelijkheden in de rechtmatige verstrekking van gegevens te voorkomen, wordt aanbevolen
in de tekst van de bepalingen in het Besluit controle op rechtspersonen de namen van diverse netwerkpartners te actualiseren. Dit is nodig omdat de afgelopen twee jaar wijzigingen in de benaming hebben plaatsgehad in verband met de organisatorische wijzigingen bij deze partijen.

1. Inleiding

Op 1 juli 2011 is de Wet controle op rechtspersonen (hierna Wcr)[1] in werking getreden. Daarmee heeft de Verklaring van geen bezwaar (hierna VVGB), die verplicht was bij de oprichting van rechtspersonen, plaatsgemaakt voor een systeem van doorlopend toezicht op rechtspersonen. Artikel 13 van de Wcr stelt dat de minister van Veiligheid en Justitie binnen twee jaar na inwerkingtreding van de wet een verslag aan de Staten-Generaal zendt over de doeltreffendheid en effecten van de wet in de praktijk. Het onderhavige rapport geeft invulling aan die verplichting. Om reden dat de afgelopen periode het (nieuwe) toezicht op rechtspersonen van de grond af is opgebouwd en (inhoudelijk) vormgegeven, wordt in de evaluatie ingezoomd op de output. De doeltreffendheid en (maatschappelijke) effecten van de Wcr zullen eerst op langere termijn kenbaar zijn. Een goede samenwerking van betrokken partijen in het netwerk is essentieel bij het toezicht op rechtspersonen. Dit betreft zowel partijen binnen het domein van Veiligheid en Justitie (zoals politie, OM), als daarbuiten (zoals Belastingdienst, DNB e.a.). Justis heeft in dit netwerk een centrale rol.

1.1. Toezicht op rechtspersonen

De wetgever heeft met invoering van de Wcr beoogd om het voorkomen en bestrijden van misbruik[2] van rechtspersonen te verbeteren en zodoende het vertrouwen in het handelsverkeer te bevorderen. Deze doelstelling moet worden bereikt door een systeem van doorlopend toezicht op rechtspersonen dat zo min mogelijk administratieve lasten voor bedrijven en (georganiseerde) burgers met zich meebrengt.[3] Het voorgestelde systeem van doorlopend toezicht is gebaseerd op het rapport 'Snel en Secuur toetsen; het alternatief voor de verklaring van geen bezwaar' dat op 18 maart 2005 aan de Tweede Kamer is aangeboden.[4]

---

1 De Wet van 7 juli 2010 tot wijziging van onder meer Boek 2 van het Burgerlijk Wetboek en de Wet documentatie vennootschappen (Stb. 2010, 280). De Wet documentatie vennootschappen wordt met ingang van 1 juli 2011 aangehaald als Wet controle op rechtspersonen.

2 Onder 'misbruik' verstaat artikel 2 lid 1 van de Wcr, misbruik van rechtspersonen, waaronder 'het plegen van misdrijven en overtredingen van financieel-economische aard door of door middel van deze rechtspersonen'. Het woord 'waaronder' houdt in dat het misbruik hiertoe niet beperkt hoeft te zijn, ook ander misbruik van een rechtspersoon kan tot een risicomelding leiden.

3 Kamerstukken II 2008/2009, 31 948, nr. 3

4 Kamerstukken II 2004/2005, bijlage bij just050263.

De uitvoering van het toezicht op rechtspersonen komt tot stand door een nauwe samenwerking tussen verschillende (semi)overheidspartijen. Binnen deze samenwerking vervult Justis een centrale rol.
Het toezicht op rechtspersonen omvat het overgrote deel van alle rechtspersonen die in het Nederlandse handelsregister zijn ingeschreven; dat zijn ongeveer 1 miljoen rechtspersonen. In de afgelopen twee jaar is toezicht gehouden op bv's, nv's, stichtingen, verenigingen en buitenlandse rechtspersonen met een onderneming in Nederland.

Bepaalde wijzigingen in het handelsregister, bijvoorbeeld de toetreding van een nieuwe bestuurder tot een bv, leiden ertoe dat RADAR, het ict-systeem dat het toezicht ondersteunt, een 'automatische analyse' uitvoert. RADAR brengt in kaart welke bedrijven en personen betrokken zijn bij deze wijziging in de bedrijfsvoering. Van deze bedrijven en personen gaat RADAR na of zij betrokken zijn geweest bij een faillissement dan wel een strafrechtelijk antecedent op naam hebben via een geavanceerde automatische analyse waarbij alle betrokkenen (natuurlijke en rechtspersonen) en hun antecedenten worden vastgesteld en gewogen. Als deze antecedenten daartoe aanleiding geven, maakt het systeem een zogeheten 'tussentijdse risicomelding'. Dit wil nog niet zeggen dat de betreffende wijziging een risico op misbruik van de rechtspersoon oplevert. Of dat zo is, wordt door een medewerker van Justis handmatig nader onderzocht. Daarbij kunnen extra bronnen worden geraadpleegd, zoals bijvoorbeeld de Belastingdienst en de politie. Als uit dit nadere onderzoek blijkt dat er een risico op misbruik van de rechtspersoon bestaat, wordt een risicomelding gemaakt en verstrekt.

Voor de analyse, zowel de automatische als de handmatige, wordt gebruik gemaakt van risicoprofielen. Deze bestaan uit indicatoren die een verhoogd risico op misbruik kunnen betekenen. De indicatoren die in een bepaald geval worden aangetroffen moeten in samenhang worden bekeken, op basis van de omstandigheden van het specifieke geval, om tot een zorgvuldige afweging te komen of wel of niet sprake lijkt van een risico op misbruik.

Behalve de risicomelding die op basis van een wijziging in het handelsregister tot stand komt, is het ook mogelijk dat één van de afnemers een verzoek doet voor een risicomelding over een specifieke rechtspersoon. Het gaat dan om een rechtspersoon die al in het vizier is van de afnemer en waarover men meer informatie nodig heeft.

Justis verstrekt ook netwerkanalyses of informatieverstrekkingen. Dit betreft een tekening van een rechtspersoon en het netwerk van personen en rechtspersonen om deze rechtspersoon heen. De omvang van de tekening kan variëren van slechts enkele tot vele honderden entiteiten en

hun onderlinge relaties. In het geval van grote netwerken worden de tekeningen vaak gebruikt om overzicht te houden, bijvoorbeeld in grote opsporingsonderzoeken waarbij ingewikkelde structuren van rechtspersonen moeten worden ontrafeld.

In het Besluit controle op rechtspersonen (hierna Bcr)[5], dat strekt tot uitvoering van de Wcr, is vermeld welke partijen gerechtigd zijn risicomeldingen en netwerkanalyses te ontvangen. De partijen die een risicomelding mogen ontvangen, zijn eveneens gerechtigd een verzoek tot verstrekking van een risicomelding bij Justis in te dienen. Ook wordt in het Bcr geregeld aan welke partijen de ontvangers van risicomeldingen gerechtigd zijn gegevens uit de risicomeldingen door te geven. Tot slot wordt in het Bcr geregeld uit welke gegevensverwerkingen Justis gerechtigd is gegevens te putten en is voorzien in een opsomming van de gegevens die door Justis kunnen worden verwerkt. aan welke instanties de afnemers gegevens uit een risicomelding mogen doorgeven.

De invoering van het toezicht op rechtspersonen is gefaseerd verlopen: na een beperkte en beheerste start is RADAR en het daarop volgende handmatige werk geleidelijk uitgebouwd.[6]

1.2. Opbouw

In dit rapport wordt de uitvoering van de Wcr geëvalueerd vanuit drie invalshoeken van het toezicht: de output van het toezicht, de inrichting van het toezicht en de samenwerking in het netwerk. Hierdoor ontstaat één omvattend beeld van de wijze waarop in de periode tussen 1 juli 2011 en 1 juli 2013 uitvoering is gegeven aan het toezicht op rechtspersonen. Aan de hand van cijfers over verstrekte producten en de door de afnemers aan Justis gerapporteerde acties die zij naar aanleiding van deze producten hebben ondernomen, wordt in hoofdstuk 2 de output van het toezicht beschreven. Vervolgens wordt in hoofdstuk 3 weergegeven op welke wijze het toezicht op rechtspersonen is ingericht en met welke waarborgen de uitvoering van het toezicht is omkleed. Tot slot wordt in hoofdstuk 4 uiteengezet op welke wijze de samenwerking in het netwerk is vormgegeven.

---

[5] Besluit van 8 april 2011 tot wijziging van het Besluit documentatie vennootschappen en enige andere besluiten. (Stb, 2011, 180). Het Besluit documentatie vennootschappen wordt met ingang van 1 juli 2011 aangehaald als Besluit controle op rechtspersonen.

[6] Zie voor meer informatie hierover Kamerstukken II 2012/2013, 29 911, nr. 77.

2. Output van het toezicht

In het onderhavige hoofdstuk wordt uiteengezet wat het toezicht op rechtspersonen in de eerste twee jaar na inwerkingtreding van de Wcr heeft opgeleverd. Het toezicht op rechtspersonen, zoals neergelegd in de Wcr, is volledig nieuw. De afgelopen periode is dan ook vooral veel tijd en aandacht besteed aan het inrichten en (inhoudelijk) vormgeven van dit toezicht. Relaties met (keten)partners binnen het netwerk zijn opgebouwd en er is veel ervaring opgedaan zowel bij die (keten)partners als bij Justis. Uiteraard is over de output van het toezicht op rechtspersonen ook veel te melden.

Er wordt in dit hoofdstuk een overzicht gegeven van de aantallen producten (risicomeldingen en netwerkanalyses) die tussen 1 juli 2011 en 1 juli 2013 zijn verstrekt en hoe tot deze producten is gekomen. Tevens wordt inzicht gegeven in de vervolgacties die de verschillende afnemers hebben ondernomen naar aanleiding van de door Justis aan hen verstrekte producten.

2.1. Verstrekte producten

Zoals in hoofdstuk 1 is aangegeven, heeft Justis een signalerende rol in de samenwerking met de netwerkpartners in het toezicht op rechtspersonen. In de uitvoering van deze rol worden signalen verzonden ter ondersteuning van de handhavende of opsporende taken van de afnemers. Enerzijds zijn dat signalen van risico's die zelfstandig door Justis worden vastgesteld, te weten de risicomeldingen uit het systeem, die volgen uit de (deels automatische) analyse van wijzigingen in het handelsregister. Anderzijds zijn dat signalen door Justis verstrekt op verzoek van de afnemers, zoals de risicomelding op verzoek en de netwerkanalyse.

2.1.1. Risicomeldingen uit het systeem

In paragraaf 1.1 is toegelicht op welke wijze een risicomelding uit het systeem tot stand komt. Als de verzamelde informatie wijst op een risico op misbruik van de rechtspersoon, wordt een risicomelding afgegeven aan die afnemers die het misbruik het beste kunnen bestrijden. Concreet betekent dit in ieder geval dat als er aanwijzingen zijn dat er al strafbare feiten zijn gepleegd, de risicomelding naar een opsporende instantie gaat. Het komt in de praktijk vaker voor dat het vermoeden bestaat dat er strafbare feiten zullen worden gepleegd in de nabije toekomst: in die gevallen wordt de risicomelding aan een handhavende instantie (bijvoorbeeld de Belastingdienst of Inspectie SZW) gezonden, die door middel van bijvoorbeeld een controle kan voorkomen dat de strafbare feiten worden gepleegd.

In het eerste half jaar van het toezicht zijn geen risicomeldingen uit het systeem verstrekt. Vanaf 1 januari 2012 is gestart met het verstrekken van deze meldingen. Er zijn met betrekking tot de ongeveer 1 miljoen rechtspersonen waarop toezicht wordt gehouden, circa 1,5 miljoen wijzigingen in het handelsregister geregistreerd in de verslagperiode. Niet alle wijzigingen geven aanleiding tot een automatische analyse: bijvoorbeeld een wijziging van het telefoonnummer geeft daartoe geen aanleiding. Daarnaast maakt Justis gerichte keuzes in het bepalen van de momenten waarop een analyse wordt uitgevoerd en variëren deze momenten in de tijd. Daarbij zijn steeds die keuzes gemaakt, die op dat moment tot zo goed mogelijke resultaten leidden.

In de periode van 1 januari 2012 tot 1 juli 2013 heeft RADAR 205.865 automatische analyses uitgevoerd. In 1.368 van de gevallen werd een systeemmelding aangemaakt en in behandeling genomen. Zeker in de eerste fase werden nog veel systeemmeldingen aangemaakt die na beoordeling van een onderzoeker geen risico op misbruik van een rechtspersoon bleken op te leveren. Uiteindelijk zijn er 37 risicomeldingen op basis van systeemmeldingen verstrekt aan (telkens één of meer) van de afnemers.

Door middel van aanpassing van de instellingen van RADAR wordt de output van de automatische analyse beïnvloed. Deze instellingen worden aangepast aan de ontwikkelingen: als blijkt van nieuwe vormen van fraude, andere prioriteiten bij de afnemers van de risicomeldingen of in de maatschappij, zal hierop de focus worden gelegd. In paragraaf 2.1.3 is nader uitgewerkt welke focus in de verslagperiode is gehanteerd.

2.1.2. Risicomeldingen op verzoek

Naast de risicomeldingen die worden gemaakt op basis van een systeemmelding, kunnen afnemers verzoeken om een risicomelding. Als een dergelijk verzoek Justis bereikt, wordt eenzelfde soort onderzoek verricht als het onderzoek dat verricht wordt naar aanleiding van een systeemmelding. Als in het onderzoek wordt geconstateerd dat een risico op misbruik van de rechtspersoon aanwezig is, wordt de risicomelding op verzoek aan de betreffende afnemer verzonden. Wanneer geen risico wordt aangetroffen, zal uiteraard geen risicomelding verzonden worden. Wel wordt dan het bericht verzonden dat geen risico is geconstateerd. De afnemers van risicomeldingen op verzoek zijn dezelfde organisaties als de afnemers van de risicomeldingen op basis van een systeemmelding.

Risicomeldingen op verzoek zijn vanaf de start van het toezicht in behandeling genomen. In de periode van 1 juli 2011 tot 1 juli 2013 zijn 49

verzoeken voor een risicomelding ingediend, waarvan er 28 zijn verstrekt. In de overige gevallen is het verzoek ingetrokken, is vastgesteld dat er geen risico op misbruik naar voren kwam dan wel is het verzoek nog in behandeling.

2.1.3. Typen misbruik risicomeldingen

Zoals uit de hiervoor genoemde aantallen blijkt, is kenmerkend voor het toezicht op rechtspersonen dat sprake is van een zogenaamde 'trechterwerking': circa 1,5 miljoen wijzigingen bij circa 1 miljoen rechtspersonen leiden tot ruim 200.000 automatische analyses, die in de verslagperiode tot 1.368 tussentijdse risicomeldingen en handmatige analyses hebben geleid, waarna uiteindelijk in totaal 65 risicomeldingen zijn verstrekt in de eerste twee jaar van de Wcr: 37 uit het systeem en 28 op verzoek.

Als wordt gekeken naar de voornaamste risico's op misbruik waarvoor de 65 risicomeldingen zijn verstrekt, ontstaat het volgende beeld. Van de 65 verstrekte meldingen hadden er:

- 29 betrekking op een vermoeden van faillissementsfraude door notoire fraudeurs (ofwel veelplegers);
- 12 betrekking op een vermoeden van faillissementsfraude door (rechts)personen die (nog) niet bekend staan als notoire fraudeurs;
- 5 betrekking op een vermoeden van witwassen;
- 2 betrekking op een vermoeden van beleggingsfraude;
- 5 betrekking op een vermoeden van belastingfraude en
- 12 betrekking op een vermoeden van overige soorten van fraude dan wel ander misbruik van rechtspersonen.

De bovenstaande verdeling vormt een goede afspiegeling van de vormen van misbruik waar het toezicht op rechtspersonen in de eerste twee jaar op gericht was, zowel gelet op de inhoud van de verzoeken om een risicomelding door afnemers als de instellingen van de automatische analyse. De focus lag en ligt op het thema faillissementsfraude. Dit heeft de afgelopen twee jaar en thans nog steeds hoge prioriteit bij een belangrijk deel van de partners in het netwerk van het toezicht op rechtspersonen.

Het verschil in soorten misbruik waarop risicomeldingen uit het systeem en op verzoek zien, is klein. Wel valt op dat 9 van de 12 vermoedens van faillissementsfraude door een (rechts)persoon die (nog) niet bekend stond als notoire fraudeur, een risicomelding uit het systeem betroffen. Dit is een eerste indicatie dat Justis daadwerkelijk bijdraagt aan het in kaart brengen van nog niet bekende fraudeurs.

2.1.4. Netwerkanalyses

Een netwerkanalyse of informatieverstrekking is een product waarbij schematisch een overzicht wordt gegeven van de rechts- en natuurlijke personen waarmee een rechtspersoon in relatie staat[7]. Op basis van gegevens uit het Handelsregister, het Insolventieregister en de Gemeentelijke Basisadministratie, wordt daartoe een zogenaamde netwerktekening opgesteld. Deze netwerktekening maakt zowel actuele als historische verbanden tussen verschillende bedrijven en bestuurders inzichtelijk. Netwerkanalyses worden uitsluitend op verzoek van daartoe bevoegde instanties en personen die bij de uitvoering van hun publiekrechtelijke taak een dergelijk overzicht nodig hebben, zoals bijvoorbeeld faillissementscuratoren, door Justis verstrekt.

In de periode van 1 juli 2011 tot 1 juli 2013 zijn 1.253 verzoeken voor een netwerkanalyse in behandeling genomen. Per 1 juli 2013 zijn 1.158 netwerkanalyses verstrekt.

2.2. Acties naar aanleiding van signalen

Justis geeft door middel van de in paragraaf 2.1 benoemde producten een signaal af aan handhavende en opsporende instanties. Het is vervolgens aan deze instanties om de door Justis verstrekte signalen een vervolg te geven; zie paragraaf 4.1.3 voor de wijze waarop zij daar gedurende de verslagperiode uitvoering aan hebben gegeven. Om de risicomeldingen zo goed mogelijk te laten aansluiten op de behoeften van de afnemers, vraagt Justis bij elk verstrekt product aan de afnemer een terugkoppeling over wat er met het signaal is gedaan. Deze terugkoppelingen dienen om verbeteringen in de producten of de werkwijze door te voeren, maar geven ook inzicht in de doelmatigheid van het toezicht.

2.2.1. Risicomeldingen

Voor het inzichtelijk maken van de opvolging van de risicomeldingen is gebruik gemaakt van terugkoppelingen die Justis van de afnemers heeft ontvangen. Van de 65 in de periode tot 1 juli 2013 verstrekte risicomeldingen is per de datum van dit rapport in 45 gevallen een terugkoppeling ontvangen. In zaken waarbij de risicomelding kort voor 1 juli 2013 is verzonden, of waarin een bestuurs- en strafrechtelijke onderzoek gestart moet worden, kan een terugkoppeling langer op zich laten wachten. Vandaar dat nog niet in alle gevallen een terugkoppeling is

[7] Het product netwerkanalyse is niet een nieuw product, het bestond reeds ten tijde van het voormalige preventieve toezicht op basis van de Wet documentatie vennootschappen.

ontvangen. In zijn algemeenheid kan worden gesteld dat, ondanks de medewerking van de afnemers die Justis op dit moment al ontvangt, de terugkoppeling blijvende aandacht verdient teneinde de doelmatigheid en effecten van het toezicht goed in beeld te kunnen brengen.

Hieronder wordt in een overzicht weergegeven welke acties zijn ondernomen in de 45 gevallen waarin Justis een terugkoppeling heeft ontvangen. Daarbij moet nog worden opgemerkt dat de terugkoppelingen vrij kort na het verstrekken van het signaal zijn ontvangen, waardoor in een flink aantal gevallen de 'eindsituatie' (is tot vervolging overgegaan? Is de vergunning ingetrokken?) nog niet bekend is. De volgende acties zijn ondernomen:

Preventieve acties	- Heroverwegen van een vergunning dan wel onderzoeken of een vergunning kan worden ingetrokken; - Afwijzen vergunning in geval van aanvraag; - Boete opleggen dan wel het onderzoek of er een overtreding is begaan loopt nog; - Plannen of afleggen van een bedrijfsbezoek (in de meeste gevallen inclusief een voornemen om de boekhouding veilig te stellen); - Intrekken van btw-nummers of de status van OB-ondernemerschap; - Verzoek uitzetten naar regiokantoren om niet-actieve ondernemers af te voeren van de lijst van ondernemers; - Onderzoek of monitoring van inkomsten en aangiftes; - Onderzoek naar het mogelijk verhalen van reeds verleende belastingteruggaven; - Onderzoek naar bestuurdersaansprakelijkheid; - Overleg met de curator; - Voordragen van rechtspersonen voor ontbinding, al dan niet in samenwerking met de KvK; - Doorsturen aan andere toezichthouder of regio.
Repressieve acties	- Beslagleggen op geld/ goederen; - Overleg om te beslissen hoe het (strafrechtelijk) onderzoek opgepakt moet worden; - Contact opnemen met politie in verband met een al lopend strafrechtelijk onderzoek; - Voorstel voor vervolging door het OM; - Opnemen van de melding in het (eigen) systeem, in afwachting van eventuele toekomstige extra signalen; - Aanhouden en vervolgen van verdachten.

Geen acties
- Het betrof een testcase;
- Capaciteitsgebrek;
- Project is gestopt;
- Geen reden gegeven;
- Niet bruikbaar wegens het ontbreken van bepaalde informatie.

Toelichting
De meerderheid van de ondernomen acties was preventief van aard; er was nog niet aannemelijk gemaakt dat er al misbruik had plaatsgevonden, maar er bestond risico dat dit in de nabije toekomst zou gebeuren. De meest voorkomende preventieve actie is het afleggen van een bedrijfsbezoek door de Belastingdienst en de Inspectie SZW. Bij een bezoek door de Belastingdienst wordt bij die gelegenheid tevens, indien mogelijk, de boekhouding veiliggesteld om reden dat in de praktijk is gebleken dat dit effectief is: dikwijls is in frauduleuze faillissementen de boekhouding zoek gemaakt of vernietigd. Als de Belastingdienst reeds over een kopie van de boekhouding beschikt, wordt er vervolgens minder gefraudeerd omdat men weet dat de Belastingdienst over bewijzen beschikt om deze fraude aan te tonen, waarmee de kans om "ermee weg te komen" drastisch vermindert.

In een aantal gevallen is de risicomelding door een netwerkpartner voor repressieve doeleinden gebruikt, bijvoorbeeld om een strafrechtelijk onderzoek te starten of daaraan bij te dragen. In één geval is aan Justis terug gemeld dat de risicomelding, samen met andere signalen, de reden was voor een onderzoek, welk onderzoek inmiddels heeft geleid tot het aanhouden en vervolgen van de betrokkenen die ervan verdacht worden voor 9 miljoen euro te hebben gefraudeerd. Dankzij de overzichtelijke opsomming van relevante feiten rondom deze betrokkenen in de risicomelding, kon het Openbaar Ministerie snel beslissen in deze zaak tot vervolging en voorlopige hechtenis over te gaan.

In een beperkt aantal gevallen (circa 10%) is geen actie ondernomen naar aanleiding van de risicomelding. De redenen daarvoor zijn divers: het betrof een testcase, het ging om een project dat inmiddels is gestopt, de risicomelding bevatte onvoldoende informatie voor deze afnemer of capaciteitsgebrek bij de netwerkpartner.

2.2.2. Netwerkanalyses

Op 1 juli 2012 is gestart met het versturen van evaluatieformulieren aan de afnemers van netwerkanalyses. De volgende acties zijn ondernomen naar aanleiding van een netwerkanalyse (NWA):

Preventieve en repressieve acties	-	NWA is 'nuttig voor de boedel' of geeft inzicht in de (bestuurs)verhoudingen;
	-	NWA is gebruikt voor rechtmatigheidsonderzoek door curator;
	-	NWA is gebruikt voor verhaalonderzoek bestuurdersaansprakelijkheid of beslagmogelijkheden of verhoren failliet;
	-	NWA wordt aan proces-verbaal toegevoegd ter verduidelijking voor het OM en de rechter;
	-	Inzichtelijk maken van constructies en rechtsvormen;
	-	Opstarten van een civiele-, fiscale- of strafrechtelijke rechtszaak;
	-	Opstarten van een strafrechtelijk onderzoek;
	-	Gebruik van de informatie in lopend strafrechtelijk onderzoek;
	-	Mogelijk benaderen van curator in betrokken faillissementen.
Geen acties	-	Informatie van Justis te laat aangeleverd;
	-	Geen (nieuwe) rechtspersonen in beeld waarop actie kon of diende te worden ondernomen;
	-	(Nog) geen vervolgstappen;
	-	Niet aangegeven of / welke vervolgstappen worden gezet.

Toelichting
De ondernomen acties naar aanleiding van een netwerkanalyse zijn voornamelijk repressief van aard. Dit ligt ook voor de hand: het merendeel van de analyses wordt aangevraagd ofwel door curatoren (er loopt dus al een faillissement waarin wordt vermoed dat er fraude is gepleegd) ofwel door opsporingsinstanties die al met een onderzoek bezig zijn.

Curatoren geven aan dat de netwerkanalyse hen helpt bij het doen van verhaalonderzoek, het krijgen van inzicht in de verhoudingen en/of het aansprakelijk stellen van de bestuurder(s). Opsporingsinstanties gebruiken de informatie om de structuur van het bedrijvennetwerk te verduidelijken aan het Openbaar Ministerie en de rechter of starten een (strafrechtelijk) onderzoek met behulp van deze informatie.

In enkele gevallen heeft de netwerkanalyse geen opvolging gekregen, bijvoorbeeld omdat het onderzoek geen nieuwe, nog onbekende rechtspersonen opleverde waarop actie moest worden ondernomen. Ook is in sommige gevallen niet aangegeven of en welke vervolgstappen zijn gezet.

3. Inrichting van het toezicht

De centrale rol bij de uitvoering van het toezicht rechtspersonen is belegd bij Justis. Om ervoor te zorgen dat zo goed mogelijk invulling wordt gegeven aan deze rol, is een goede inrichting van het toezicht van groot belang. Daarbij gaat het naast de technische ondersteuning ook over de waarborgen in het kader van de Wet bescherming persoonsgegevens.

3.1. Ontwikkeling RADAR

Zoals beschreven in paragraaf 1.1, wordt het toezicht op rechtspersonen technisch ondersteund door het ict-systeem RADAR. De minister van Veiligheid en Justitie heeft de Tweede Kamer uitvoerig schriftelijk geïnformeerd over de ontwikkelingen van dit ict-systeem.[8] Hieruit is te begrijpen dat het toezicht op rechtspersonen in de eerste periode grotendeels handmatig werd uitgevoerd door Justis, omdat nog geen gebruik kon worden gemaakt van de ondersteuning door RADAR. Op 9 januari 2012 is RADAR in gebruik genomen en zijn, op basis van automatische meldingen, de onderzoeken gestart om te komen tot risicomeldingen uit het systeem.

RADAR is zo ontworpen dat nieuwe gegevensbronnen kunnen worden toegevoegd en dat het toezicht op rechtspersonen steeds "slimmer" kan worden uitgevoerd doordat risicoprofielen flexibel kunnen worden aangepast. Het gebruik van het ict-systeem kan daarmee worden aangepast aan de behoeftes van handhavende en opsporende organisaties en kan inspelen op nieuwe fraudefenomenen. In de verslagperiode is op basis van praktijkervaringen dan ook reeds ingezet op het ontwikkelen en verfijnen van het systeem. Nieuwe profielen, die inspelen op nieuwe kennis en ontwikkelingen, en de soorten en omvang van het misbruik van rechtspersonen inzichtelijk maken, zullen in de komende periode worden toegevoegd aan RADAR. Om aan de behoeften van afnemers te kunnen blijven voldoen, zal zowel in de bestaande versie als in toekomstige versies van RADAR worden gezocht naar mogelijkheden om de effectiviteit van het toezicht te verbeteren.

3.2. Wet bescherming persoonsgegevens

De Wcr omvat de verwerking van persoonsgegevens en andere gegevens. Op grond van de toenmalige Wet documentatie vennootschappen was het

[8] Kamerstukken II 2011/2012, 29 911, nr. 74 en Kamerstukken 2012/2013, 29 911, nr. 77

al mogelijk om gegevens te registeren om misbruik van vennootschappen te voorkomen en te bestrijden. De Wcr breidt de controle uit tot een bredere kring van rechtspersonen en natuurlijke personen. Tevens wordt het instrument risicomelding geïntroduceerd. Bij de totstandkoming van de Wcr[9] is dan ook veel aandacht besteed aan de verhouding van de Wcr tot de privacy in het algemeen en de Wet bescherming persoonsgegevens (hierna Wbp) in het bijzonder. Aandacht ging met name uit naar de volgende punten:

1. Voorkomen moet worden dat:
   - onjuiste of gedateerde gegevens worden gebruikt;
   - er meer gegevens worden verwerkt dan nodig is om de toezichtstaak te vervullen en bij het opvragen en verwerken van de persoonsgegevens moet voldaan zijn aan de eisen van proportionaliteit.
2. Het betrekken van familieleden en adresgenoten van bij de rechtspersoon betrokken natuurlijke personen moet zorgvuldig en proportioneel worden ingezet.
3. De gegevensstromen dienen afdoende te zijn beveiligd opdat voorkomen wordt dat gevoelige informatie in verkeerde handen valt.

Door de minister van Veiligheid en Justitie is in dat kader een aantal toezeggingen gedaan dan wel acties in het vooruitzicht gesteld.

Ten eerste is de verwerking van persoonsgegevens in het kader van de Wcr aangemeld bij de Functionaris voor de Gegevensbescherming van het ministerie van Veiligheid en Justitie[10].

Ten tweede zijn de te verwerken gegevens veelal afkomstig uit het stelsel van basisregistraties, waardoor authenticiteit en actualiteit gewaarborgd zijn. Bovendien is een correct beleid voor verwijdering van gegevens een belangrijk onderdeel van de omgang met persoonsgegevens. Om te voorkomen dat de verkeerde gegevens gebruikt worden voor risicomeldingen, moeten verouderde gegevens en gegevens van personen die voor het onderzoek niet relevant zijn bevonden, zo snel mogelijk worden verwijderd. In RADAR is een functionaliteit ingebouwd die automatische analysegegevens verwijdert, wanneer de voorgeschreven

---

[9] Zie onder meer Kamerstukken II 2008/2009, 31 948, nr. 3 (blz. 9-14), nr. 6 (blz. 14-18), en Kamerstukken I 31 948, nr. C (blz. 11-15).

[10] http://www.rijksoverheid.nl/ministeries/venj/documenten-en-publicaties/formulieren/2011/06/29/formulier-herziening-toezicht-rechtspersonen.html (Formulier Meldingenregister, nummer: MVenJ/Wbp/0028-05/29-06-2011)

bewaartermijnen[11] zijn verstreken. Beide maatregelen dragen bij aan het voorkomen van het gebruik van onjuiste of gedateerde gegevens.

Ten derde voldoet Justis aan de wet met betrekking tot de verplichting neergelegd in artikel 34 van de Wbp. Omdat het hier verwerking van gegevens krachtens wettelijk voorschrift betreft, worden alle betrokkenen (naast de gebruikelijke publicatie van wetgeving) door de notaris of via de website van de Kamer van Koophandel op de hoogte gesteld van het bestaan van de Wcr en de implicaties daarvan voor de ondernemer en zijn naaste omgeving. Hiermee wordt invulling gegeven aan de werkwijze zoals verwoord in de Memorie van Toelichting bij de Wcr. [12]

Ten vierde kan over de beveiliging van gegevens worden opgemerkt dat gewerkt is en wordt aan het beveiligd (versleuteld) verzenden van informatie binnen het netwerk van het toezicht op rechtspersonen. Onder andere wordt gebruik gemaakt van een encryptie-programma. Hiermee kan worden voorkomen dat gevoelige gegevens 'zomaar' op straat terecht komen.

[11] De bedoelde termijnen zijn: een analyse die niet tot een tussentijdse risicomelding leidt wordt na een dag verwijderd; een tussentijdse risicomelding die niet tot een risicomelding leidt wordt binnen een maand na deze constatering verwijderd en een verstrekte risicomelding wordt na twee jaar verwijderd.

[12] Kamerstukken II, 2008/2009, 31 948, nr. 3 (blz. 12).

4. Samenwerking in het netwerk

Het doel van de Wcr is het voorkomen en bestrijden van het misbruik van rechtspersonen. De uitvoering van de controle op rechtspersonen vindt plaats in een netwerk, waarbij Justis een centrale rol vervult. Om aan deze centrale rol zo effectief en efficiënt mogelijk invulling te geven voert Justis op regelmatige basis overleg met zowel de partijen die informatie leveren, de informatieleveranciers, als de partijen die met behulp van de producten van Justis actie ondernemen, de afnemers. Een grafische weergave van het netwerk is als bijlage bij dit rapport gevoegd. In zijn algemeenheid kan worden gesteld dat de samenwerking in de verslagperiode heeft geleid tot een betere afstemming van de werkzaamheden van de netwerkpartners, zowel op inhoud als op proces.

4.1. Samenwerking op het gebied van risicomeldingen

Bij het toezicht op rechtspersonen is het van belang dat de informatie op basis waarvan mogelijk misbruik kan worden geconstateerd, beoordeeld en gemeld op de juiste wijze beschikbaar wordt gesteld. Daarnaast moeten de risicomeldingen de afnemers in het netwerk in staat stellen om acties te ondernemen tegen het misbruik van rechtspersonen. Daarom wordt tussen informatieleveranciers, Justis en de afnemers actief samengewerkt en structureel overlegd. Dat overleg heeft diverse vormen waarbij wordt uitgegaan van de modus die voor de betreffende partijen het beste werkt.

De informatieleveranciers en afnemers zijn in de Wcr en het Bcr aangewezen. Door diverse organisatorische wijzigingen bij enkele van deze informatieleveranciers en afnemers in de afgelopen twee jaren, is de benaming van deze organisaties in het Bcr in een aantal gevallen achterhaald. Dit heeft aanleiding gegeven tot vragen van informatieleveranciers en afnemers over de legitimiteit van de gegevensverstrekking. In het onderhavige hoofdstuk wordt de benaming aangehouden zoals die thans in het Bcr is opgenomen.

4.1.1. Informatieleveranciers - Justis

Een risicomelding mag uitsluitend gegevens bevatten van de volgende partijen: Handelsregister, Politie, Justitiële Informatiedienst, UWV, Belastingdienst, GBA, Algemene inspectiedienst, Autoriteit Financiële Markten, Arbeidsinspectie en andere SZW toezichthouders, milieudiensten, bijzondere opsporingsdiensten, DNB, Dienst Wegverkeer, OM, Autoriteit consument en markt, Voedsel- en Warenautoriteit en de VROM-inspectie. Daarnaast mag informatie uit openbare bronnen worden gebruikt.

Gezien het grote aantal en grote diversiteit van de informatieleveranciers worden tussen de informatieleveranciers en Justis bilaterale overleggen gevoerd. Tussen Justis en de beheerders van het Handelsregister, het Centraal Insolventieregister en de Justitiële Informatiedienst wordt structureel overleg gevoerd. Eventuele wijzigingen in de systemen van deze informatieleveranciers hebben gevolgen voor de koppeling met RADAR, waardoor blijvend overleg nodig is. Andere leveranciers, zoals de Belastingdienst, kennen een veelheid van registraties, waardoor het overleg met deze partijen zich vooral richt op welke gegevens relevant zijn om te leveren. Met beheerders van openbare informatie wordt geen overleg gevoerd.

Over het algemeen genomen verloopt de samenwerking tussen de leveranciers van informatie en Justis goed. De informatie die nodig is, wordt doorgaans binnen de gevraagde termijnen (in beginsel twee weken) geleverd. Het ontbreken van een leveringsverplichting voor informatieleveranciers in de Wcr (uitzonderingen zijn de Belastingdienst en het UWV) leidt geregeld tot de vraag vanuit de informatieleverancier of deze voor het toezicht op rechtspersonen wel verplicht is tot levering en hoe deze plicht zich verhoudt tot de op de informatieleverancier rustende geheimhoudingsplicht. Daarbij komt het voor dat om die reden niet wordt geleverd, wat de volledigheid en bruikbaarheid van de risicomeldingen negatief kan beïnvloeden.

4.1.2. Justis – Afnemers

De afnemers van risicomeldingen zijn: AFM, DNB, OM, Belastingdienst, FIOD, VROM-inspectie, Algemene inspectiedienst, Arbeidsinspectie en andere SZW toezichthouders, SIOD, politie en de Koninklijke Marechaussee.

In de praktijk zit er veel verschil tussen de hoeveelheden risicomeldingen die aan een afnemer worden verstrekt. Aan sommige afnemers zijn nog geen of is slechts één risicomelding verstrekt, aan andere afnemers (zoals de Belastingdienst) zijn vele risicomeldingen verstrekt. Dit is onder meer afhankelijk van het aantal verzoeken om een risicomelding dat een afnemer heeft gedaan en de afspraken die met de verschillende afnemers zijn gemaakt over aantallen en soorten risicomeldingen. Verder speelt mee dat in het kader van handhaving sneller actie kan worden ondernomen dan in het kader van opsporing, ook als nog geen strafbaar feit is gepleegd maar slechts het risico daarop dreigt. In die gevallen is een korte doorlooptijd tussen gebeurtenis in het handelsregister en verzending van de risicomelding van belang: hoe sneller de afnemer op kan treden, des te meer effect deze doorgaans kan bereiken.

'We hebben vanaf de inwerkingtreding van de Wet cor in drie gevallen gebruik gemaakt van deze mogelijkheid. De doorlooptijd van deze verzoeken varieerde van 3 maanden tot 12 maanden. De lange doorlooptijd had tot gevolg dat de risicomelding uiteindelijk weinig nut meer had voor ons toezicht. We zijn ons er van bewust dat de doorlooptijd van een risicomelding op verzoek inmiddels is verlaagd tot circa 8 weken. Een verdere verlaging van de doorlooptijd zou de effectiviteit van het toezicht op rechtspersonen echter nog verder kunnen verhogen.' - De Nederlandsche Bank

De doorlooptijd is thans circa acht weken. Het realiseren van een koppeling met verschillende informatiebronnen die in de nadere analyse vaak worden geraadpleegd, kan de analyse verder versnellen. Daarnaast moet voortdurende monitoring en bijsturing van het werkproces leiden tot verdere aanscherping van de doorlooptijden.

Het plenaire overleg tussen Justis en de afnemers is ondergebracht in drie gremia: het Handhavingsgremium, de Gebruikersraad en het afnemersoverleg. In de genoemde overleggen wordt gezorgd dat er zo min mogelijk hiaten in het toezicht op rechtspersonen ontstaan; wat de ene afnemer niet op kan pakken, kan de andere wellicht wel op zich nemen. Daarnaast wordt er door Justis ook bilateraal met de afnemers overlegd.

Door structureel overleg op verschillende niveaus zijn de deelnemende partijen op de hoogte van elkaars wensen en prioriteiten en kunnen knelpunten snel worden verholpen. Deze overlegconstructie zorgt ervoor dat de samenwerking en afstemming op alle uitvoeringsniveaus in het netwerk is geborgd. De inrichting stemt daarmee overeen met de omschrijving zoals verwoord in de Memorie van Toelichting bij de Wcr.[13]

Handhavingsgremium
Het handhavingsgremium is een adviesorgaan waarin zitting wordt genomen door de partijen die als afnemer van risicomeldingen zijn aangemerkt. Het handhavingsgremium adviseert over uitvoeringsbeleid, producten en over de wijze waarop de screening kan worden ingezet en welke kwaliteitseisen hierin van belang worden geacht. Op een hoger abstractieniveau worden hier handhavings- en opsporingsprioriteiten van de leden besproken, met elkaar verbonden en als richting meegegeven aan Justis.

Gebruikersraad

[13] Kamerstukken II 2008/2009, 31 948, nr. 3

De gebruikersraad overlegt over profielen en indicatoren. De gebruikersraad kent leden, de zgn. (inhoudelijke) specialisten, afkomstig uit de toezichthoudende en handhavende instanties en uit de wetenschap. Afhankelijk van het te bespreken onderwerp voor een (beoogde) profiel worden de deskundigen uitgenodigd die ten aanzien van dit onderwerp over de benodigde kennis en expertise beschikken, alsmede de overige afnemers die hier een belang bij hebben.

Afnemersoverleg
In dit overleg van 'praktijkmensen' worden tactische en operationele vraagstukken rond de risicomeldingen en de samenwerking tussen de netwerkpartners behandeld. Dit overleg vormt een aanvulling op de met deze partners op reguliere basis gevoerde bilaterale overleggen. Het afnemersoverleg is ooit ingericht als voorloper op de in de parlementaire geschiedenis van de Wcr genoemde gremia. Het afnemersoverleg fungeert als een voorportaal voor het handhavingsgremium en de gebruikersraad. Mede dankzij de overleggen op verschillende niveaus verloopt de samenwerking tussen Justis en de afnemers goed.

'De huidige samenwerking wordt als prettig en constructief ervaren. In het kader van de toezichtstaak van de Belastingdienst en de beperkte toezichtscapaciteit is het van groot belang dat de risicomeldingen zeer actueel zijn en voldoende informatie bevatten, waardoor het toezicht zoveel mogelijk aan de voorkant van het proces kan plaatsvinden. Hierbij geldt: Less is more!' - De Belastingdienst

Vanuit de overleggen met netwerkpartners komen ook voorstellen voor aanpassing van de producten of nieuwe producten om misbruik van rechtspersonen nog beter te kunnen voorkomen en bestrijden. Denk hierbij bijvoorbeeld aan de mogelijkheid om de systeemmeldingen zonder verdere bewerking door te sturen aan de afnemer, of aan het monitoren van (netwerken van) rechtspersonen voor langere tijd. In overleg wordt gekeken naar de mogelijkheden: van belang is dat de risicomelding effectief is voor het beoogde doel én binnen de wettelijke regels van de betrokken netwerkpartners en de Wcr valt.

Vanuit De Nederlandsche Bank komt het voorstel om enige vorm van 'toestemming vooraf', vergelijkbaar met de VVGB te herintroduceren:

'Door het wegvallen van de VVGB kunnen ook personen met antecedenten een rechtspersoon oprichten. Hoewel de oprichting van een rechtspersoon door een persoon met antecedenten een automatische risicomelding van de Dienst Justis tot gevolg zal hebben, neemt dit niet weg dat de rechtspersoon is opgericht en er mogelijk aanzienlijke inspanning vereist is om de schade te beperken die door misbruik van de rechtspersoon

ontstaat en de betrokkenen bestuurs- of strafrechtelijk aan te pakken. De terugkeer van een vorm van preventief toezicht, in aanvulling op het doorlopende toezicht op rechtspersonen, zou dit kunnen voorkomen.'

Dit preventieve toezicht is met de komst van de Wcr juist afgeschaft, omdat het voor bedrijven de nodige administratieve lasten met zich meebracht en het voor criminelen eenvoudig te omzeilen was.

4.1.3. Uitgevoerde vervolgacties afnemers

Zoals eerder aangegeven moet, om het misbruik van rechtspersonen daadwerkelijk te voorkomen of te bestrijden, de risicomelding gebruikt worden voor een actie. Welke actie dat kan zijn, zal afhangen van de mogelijkheden van de afnemer. In paragraaf 2.2.1 is aangegeven welke acties zijn ondernomen door de verschillende netwerkpartners. Daarbij geldt dat waar al sprake lijkt te zijn van een vermoeden van een strafbaar feit, een strafrechtelijk traject wordt gestart. En daar waar dat vermoeden er (nog) niet is, wordt een bestuursrechtelijke, civiele of fiscale actie verricht (bijvoorbeeld: vergunning intrekken, bedrijfsbezoek afleggen, BTW-nummer intrekken, onderzoek naar bestuurdersaansprakelijkheid) of het signaal wordt door de afnemer toegevoegd aan andere signalen die hij uit andere hoofde heeft ontvangen.

Ten behoeve van het optimaliseren van de kwaliteit van het toezicht op rechtspersonen houden de afnemers bij wat zij met de informatie uit de risicomelding doen en koppelen hierover terug aan de dienst Justis. De resultaten van deze terugkoppeling zijn eerder in deze evaluatie vermeld.

Niet alle afnemers koppelen in dezelfde mate terug wat zij met de risicomelding hebben gedaan. Het is verklaarbaar in die gevallen dat pas na afronding van het opsporingsonderzoek, melding wordt gedaan over al dan niet ingestelde vervolging en dat pas na afloop van de rechtszaak bekend is of een veroordeling heeft plaatsgevonden. In alle andere gevallen is (directe) terugkoppeling echter van groot belang om inzicht te krijgen in de effecten van het toezicht en om de uitvoering van het toezicht te (kunnen) verbeteren. Op dit moment voorziet de Wcr niet in een verplichting tot terugkoppeling. Het komt geregeld voor dat afnemers niet terugkoppelen vanwege het ontbreken van een verplichting daartoe. In dit verband wordt door afnemers de vraag gesteld hoe de terugkoppeling zich verhoudt tot de op de afnemer rustende geheimhoudingsplicht.

4.2. Samenwerking op het gebied van netwerkanalyses

Voor de partners bij netwerkanalyses geldt in beginsel hetzelfde als voor de netwerkpartners van risicomeldingen. Met deze afwijkingen:

4.2.1. Informatieleveranciers – Justis

Voor netwerkanalyses worden minder informatiebronnen gebruikt dan voor risicomeldingen: netwerkanalyses worden opgesteld op basis van informatie van de Kamers van Koophandel (Handelsregister), GSR-dossiers, GBA-gegevens en het Centraal Insolventie Register. De levering van informatie voor netwerkanalyses door deze partijen "loopt mee" met de levering voor risicomeldingen; er is geen apart overleg voor het product netwerkanalyses.

4.2.2. Justis – Afnemers

Voor netwerkanalyses is in de regelgeving geen limitatieve lijst met afnemers opgenomen zoals dat voor risicomeldingen het geval is, wel zijn volgens het Bcr enkele voorwaarden van toepassing. Afnemers van netwerkanalyses moeten zijn belast met een publiekrechtelijke taak en de gevraagde gegevens nodig hebben voor de uitvoering van die taak. Dat de groep afnemers van netwerkanalyses groter is dan de groep afnemers van risicomeldingen ligt voor de hand: een netwerkanalyse bevat geen gevoelige persoonsgegevens zoals bijvoorbeeld strafrechtelijke gegevens, een risicomelding wel.

Het overleg met de afnemers van de netwerkanalyses is op een andere manier ingericht, omdat hierbij een (veel) groter aantal partijen betrokken is die bovendien heterogener van aard is dan de groep afnemers van risicomeldingen. Vandaar dat bilaterale overleggen zijn ingericht met verschillende belangrijke beroepsgroepen, die veel afnemers vertegenwoordigen.

Een voorbeeld van dergelijk overleg is het periodieke overleg met INSOLAD, de beroepsvereniging van curatoren in Nederland. Het overleg over netwerkanalyses met afnemers die ook recht hebben op risicomeldingen wordt doorgaans met dat overleg 'meegenomen'. Per geval of soort gevallen kan worden besproken welk product het beste aansluit bij de behoefte / benodigde informatie. In de voorfase van een strafrechtelijk onderzoek zal een bijzondere opsporingsinstantie bijvoorbeeld meer baat hebben bij een netwerkanalyse, om het hele netwerk in kaart te brengen. Als met behulp van deze netwerkanalyse bepaald is op welk deel van het netwerk het onderzoek zich zal richten, kan deze opsporingsinstantie daarover nog een risicomelding aanvragen. Op die wijze worden alleen over de daadwerkelijk onderzochte (rechts)personen gevoelige gegevens verwerkt.

4.3. Uitbreiding van het netwerk

Hierboven is al aangegeven dat het netwerk bestaat uit een vast aantal partijen; met name het netwerk van het toezicht op rechtspersonen rond de afnemers van risicomeldingen kent een beperkt aantal (keten-)partners. Meerdere (publieke en private) partijen hebben in de afgelopen jaren aangegeven dat zij ook deel willen uitmaken van dit netwerk. Ook is uitbreiding van bestaande informatiebronnen en aansluiting op nieuwe bronnen denkbaar.

5. Slotopmerkingen en aanbevelingen

De Wet controle op rechtspersonen is erop gericht om het misbruik van rechtspersonen te voorkomen en te bestrijden. Dit doel wordt nagestreefd door middel van een doorlopend toezicht op rechtspersonen, waarin een groot aantal partijen, informatieleveranciers en afnemers, in een netwerk samenwerkt. Justis neemt hierin een centrale rol. Dit gebeurt door in de samenwerking binnen het netwerk van toezicht op rechtspersonen op basis van verschillende bronnen producten op te stellen die de afnemers, de handhavende en opsporende instanties, ondersteunen in de uitvoering van hun taken. De afgelopen periode is het (nieuwe) toezicht op rechtspersonen van de grond af opgebouwd, ingericht en geprofessionaliseerd. Dit heeft geleid tot betere aansluiting op elkaars mogelijkheden binnen het netwerk en tot een stijgende productie.

Op basis van de vervolgstappen die de afnemers hebben ondernomen kan worden gesteld dat de producten van toegevoegde waarde zijn voor het toezicht op rechtspersonen. De verwachting is dat de (maatschappelijke) effecten en de doeltreffendheid van het toezicht op rechtspersonen zich in de toekomst duidelijk(er) zullen manifesteren. Daarmee wordt mogelijk misbruik en fraude nog beter voorkomen en bestreden. Justis richt zich bij het toezicht op rechtspersonen op een optimale invulling van de behoeften en wensen van afnemers en zal in de toekomst waar mogelijk nog meer rekening houden met het belang van afnemers om deze op zo kort mogelijke termijn te voorzien van waardevolle informatie en signalen. Met de combinatie van de unieke informatiepositie die Justis heeft in het netwerk en de beschikbare kennis en ervaring binnen de organisatie, wordt voorzien in de behoefte van afnemers aan kwalitatief hoogwaardige producten. Voorts zal Justis zich nog meer toeleggen op advisering van afnemers over ontwikkelingen die zij ziet op het gebied van misbruik van rechtspersonen en mogelijke (nieuwe) producten die voor afnemers interessant kunnen zijn.

De ingeslagen weg van verdere verbreding en verdieping van het toezicht, wordt ook in de toekomst gevolgd. Hiervoor dienen bestaande informatiebronnen maximaal te worden benut. Een adequate aansluiting van Justis op nieuwe informatiebronnen, zoals het centraal aandeelhoudersregister, zal bijdragen aan de verdere ontwikkeling van het toezicht. Daarnaast zullen ervaringen met het toezicht worden benut om de toegepaste risicoprofielen verder aan te scherpen en nieuwe profielen te ontwikkelen. Dit zal helpen bij het inzichtelijk maken van de soort en omvang van het misbruik van rechtspersonen die zich voordoen. Hiermee kunnen toezichthouders en handhavende diensten de door hen gewenste acties ondernemen.

Om te komen tot een goede en bestendige inrichting van het toezicht op rechtspersonen worden op grond van de gehouden evaluatie de volgende concrete aanbevelingen gedaan.

Aanbeveling 1: Versterk het netwerk

Om een optimale effectiviteit van toezicht op rechtspersonen te realiseren, is het noodzakelijk de samenwerking in het netwerk verder te verstevigen. Structureel overleg met netwerkpartners en het leveren van maatwerk is hierbij van cruciaal belang. Hiervoor is het noodzakelijk dat de ingezette weg van plenair en bilateraal overleg op verschillende niveaus met de netwerkpartners wordt geborgd.

Het toezicht op rechtspersonen wordt effectiever als meer organisaties als afnemer kunnen worden aangemerkt, mogelijk ook private partijen. Het verdient aanbeveling onderzoek te doen naar de mogelijkheden hiertoe.

Aanbeveling 2: Versterk de informatiepositie

Justis neemt in het netwerk van toezicht op rechtspersonen een centrale en unieke informatiepositie in. Het verdient aanbeveling deze positie verder te verbeteren en te versterken om een adequate taakuitvoering door Justis te waarborgen. In de eerste plaats zal dit gebeuren door het gebruik van bestaande informatiebronnen te optimaliseren. Daarnaast is het wenselijk dat een uitbreiding van bestaande informatiebronnen en een aansluiting op toekomstige informatiebronnen plaatsvindt. In dit verband is de instelling van het centraal aandeelhoudersregister en de registratie van bestuursverboden relevant. Dit zal eraan bijdragen dat het toezicht op rechtspersonen nog verder kan worden verbeterd.
Voorts is de informatie die Justis van haar partners (terug-)ontvangt, onontbeerlijk om inzicht te krijgen in de effecten van het toezicht en om de uitvoering van het toezicht te (kunnen) verbeteren, onder meer in het aanscherpen van de risicoprofielen en de risicomeldingen op verzoek.

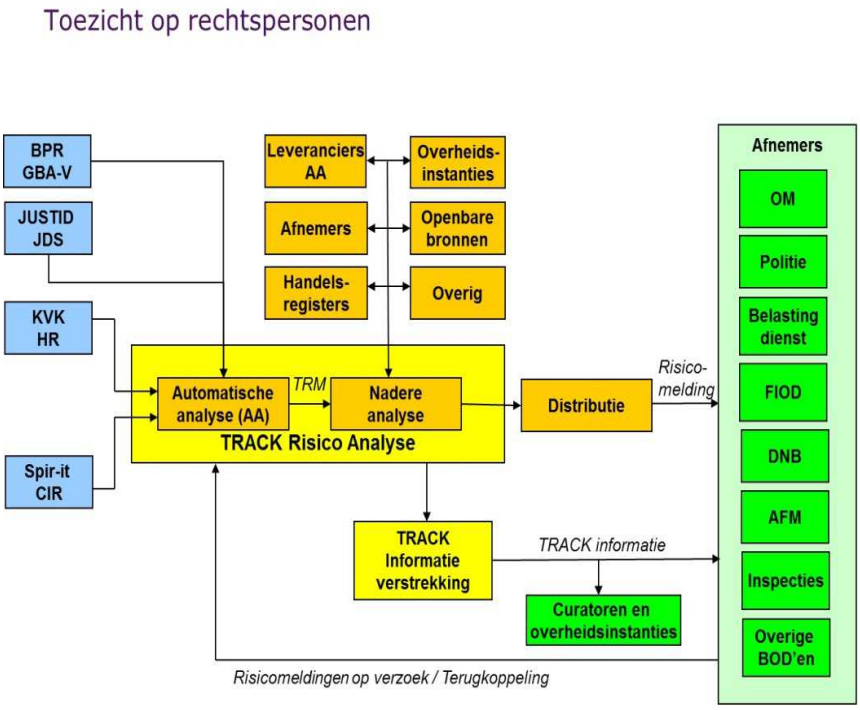
De informatiepositie van Justis wordt versterkt als de door Justis ervaren belemmeringen in de samenwerking met netwerkpartners kunnen worden weggenomen. In dit verband wordt gewezen op het ontbreken van een leverings- en terugmeldingsplicht van de netwerkpartners aan Justis en de vraag die in dat verband opkomt hoe de genoemde verplichtingen zich verhouden tot de op de (keten-)partners rustende geheimhoudingsplicht.

Aanbeveling 3: Technische wijziging van regelgeving

Het verdient aanbeveling om in de tekst van de bepalingen in het Bcr de namen van diverse netwerkpartners te actualiseren. Dit is nodig omdat de

afgelopen twee jaar wijzigingen in de benaming hebben plaatsgehad in verband met de organisatorische wijzigingen bij deze partijen. Onduidelijkheid over de rechtmatige verstrekking van gegevens wordt daarmee voorkomen.

Bijlage


Toezicht op rechtspersonen
BPR GBA-V
JUSTID JDS
KVK HR
Spir-it CIR
Leveranciers AA
Afnemers
Handels-registers
Overheids-instanties
Openbare bronnen
Overig
Automatische analyse (AA)
TRM
Nadere analyse
TRACK Risico Analyse
Distributie
Risico-melding
TRACK Informatie verstrekking
TRACK informatie
Curatoren en overheidsinstanties
Risicomeldingen op verzoek / Terugkoppeling
Afnemers
OM
Politie
Belasting dienst
FIOD
DNB
AFM
Inspecties
Overige BOD'en
1