

Kennis delen geeft kracht

*Naar een betere en zorgvuldigere gegevensuitwisseling
in samenwerkingsverbanden*

Rapport van de Werkgroep Verkenning kaderwet
gegevensuitwisseling

Den Haag, 5 december 2014

Inhoudsopgave

Samenvatting	5
1. Inleiding	11
2. Contexte verkenning	13
2.1 Namending verkenning	13
2.2 Dilemma's bij streven naar betere gegevensuitwisseling	13
2.3 Samenwerkingsverbanden	15
2.4 Verschillende wettelijke kaders en categoriële gegevens	17
2.5 Verschillende typen gegevensuitwisseling	18
2.6 Beang van zorgvuldigheid bij gegevensuitwisseling	20
2.7 Betere gegevensuitwisseling: taak van meer dan wetgeving alleen	21
2.8 Reserveer andere omstandigheden	23
3. Knelpunten	27
3.1 Inleiding	27
3.2 Verschillende wettelijke kaders	27
3.3 Rechtvaardigingen	28
3.4 Verenigbaarheidstoets	29
3.5 Geheimhoudingsplicht	31
3.6 Gegevensverklingsdoor opsporingsdiensten en OM	34
3.7 Verstrekking van strafrechtelijke gegevens	36
3.8 Typen van verwerking	36
3.9 Kwaliteit gegevens en zorgvuldigheid bij verwerking	37
3.10 Verantwoordelijke	38
3.11 Informatieplicht	38
3.12 Vertrouwen in het gebruik van gegevens door andere partijen	39
4. Concluderen kaderwet	40
4.1 Inleiding	40
4.2 Reikwijdte kaderwet	41
4.3 Regeling samenwerkingsverband in ruime zin	43
4.4 Verplichte uitwisseling van gegevens	45
4.5 Specifieke vastlegging van soorten gegevens	47
4.6 Legmatie typen van gegevensverwerking	48
4.7 Zorgvuldigheid bij verwerking	49

4.3 Verantwoordelijke.....	51
4.9 Informatieplicht.....	57
4.10 Informatieprotocol.....	52
4.11 Rechtsbescherming en toezicht.....	53
4.12 Verhouding tot bestaande wetgeving.....	55
4.13 Betekenis voor bestaande samenwerkingsverbanden.....	57
4.14 Toetsing aan het EVRM.....	57
4.15 Toetsing aan regelgeving van de EU.....	58
5. Sletbeschrijving.....	60
<i>Bijlage 2</i> Overzicht: samenwerkingsverband.....	61

Samenvatting

1. Aanleiding

Het kabinet heeft in een brief van 20 december 2013 aan de Tweede Kamer over de aanpak van fraude een verkenning aangekondigd naar een kaderwet voor de gegevensuitwisseling op het terrein van fraudebestrijding. De vraag die moet worden beantwoord, is of zo'n kaderwet grondwettelijk juist is en tot welke uitwerking in bestaande wetgeving kan worden toegevoegd.

2. Analyse van de problematiek

De behoefte aan een verkenning naar een kaderwet voor de gegevensuitwisseling op het terrein van fraudebestrijding vloeit voort uit de opvatting van het kabinet dat fraudebestrijding een brede en integrale benadering vergt, waarbij de relatieverhouding samenwerkt met gemeenten en private partijen. Om tot een efficiënte en doeltreffende samenwerking te komen is uitwisseling van informatie essentieel. Alleen dan kunnen partijen tot zo effectief mogelijk en op elkaar afgestemde interventies komen. Partijen vormen echter knelpunten bij de door hen gewenste gegevensuitwisseling.

Een belangrijke oorzaak van deze knelpunten is gelegen in het feit dat de huidige wetgeving met betrekking tot verwerking van gegevens door overheidsinstaties wordt gedomineerd door regelingen met een sectoraal karakter. Denk hierbij aan de Wet politiegegevens, de Wet Justitie en Strafrechtelijke gegevens en de bepalingen over gegevensverwerking in bijvoorbeeld de Algemene wet inzake rijbewijzen. Deze sectorale regelingen hebben deels eenzijdige uitwerking met het bestaan van samenwerkingsovereenkomsten. Dit impert, zoals hierna zal blijken, knelpunten voor de gegevensuitwisseling in de verbanden op.

Deze knelpunten bestaan voor een deel uit wettelijke belemmeringen. Ze vloeien voort uit het feit dat de bestaande regelingen daar hun sectorale karakter onvoldoende duidelijk maken wat bij de gegevensverwerking in een samenwerkingsverband wel en niet mag. Ook worden die bestaande bepalingen niet altijd in gewenste vormen van gegevensuitwisseling waardedoor sprake is van knelpunten. Deze onduidelijkheden en het ontbreken van wettelijke bepalingen die een grondslag bieden voor gegevensuitwisseling zetten een overbodige rem op de uitwisseling en verdere verwerking van gegevens. Dat belemmert op haar beurt een adequate aanpak van de problemen waarvoor een samenwerkingsverband staat. Voor deze wettelijke belemmeringen kan de vraag worden gesteld of die belemmeringen kunnen worden weggenomen met een kaderwet. Voor een ander deel hangen de bekende wettelijke belemmeringen samen met het spanningsveld dat nu eenmaal ontstaat bij een breder gebruik van gegevensuitwisseling en de wettelijke bepalingen die uit een oogpunt van bescherming van privacybelangen van betrokkenen voortvloeien. Deze laatste soort "belemmeringen" zijn van een andere orde dan de eerder genoemde belemmeringen. Beiden worden in deze verkenning in hoeverre een kaderwet belemmeringen van met name de eerste bedoelde categorie kan wegnemen.

Bij het streven naar verbetering van de mogelijkheden van gegevensuitwisseling tussen kabinet en kamer nadrukkelijk aandacht moeten schenken aan de vraag waar de grenzen liggen bij gegevensuitwisseling. Er dient een afweging te worden gemaakt tussen de belangen die worden getuigd met een breder gebruik van gegevensuitwisseling en de in (internationale) regelgeving vastgelegde kaders ter bescherming van de privacybelangen van de burger. In de politieke discussie over de verbetering van de mogelijkheden van gegevensuitwisseling door een kaderwet zullen de relevante belangen scherp in kaart moeten worden gebracht ten behoeve van een verantwoorde belangenafweging en besluitvorming. De Verkenning bevat ten behoeve van deze belangenafweging al de eerste bouwstenen.

3. Aard van de verkenning

De verkenning spint zich toe op gegevensuitwisseling in samenwerkingsverbanden. Gebleken is dat zich vooral in dergelijke verbanden knelpunten voordoen. Het gekozen uitgangspunt steelt ook op de bedoelte dat gestructureerde vormen van gegevensuitwisseling die niet al in een wettelijke regeling zijn uitgewerkt, meestal anken en daartoe openbiedt samenwerkingsverband plaatsvinden, waarbij de regeling van de gegevensuitwisseling is neergelegd in een convenant en eventueel een protocol.

De verkenning heeft betrekking op gegevensuitwisseling op een breder terrein dan fraudebestrijding. Dat heeft twee redenen. De eerste is dat bestaande samenwerkingsverbanden zich maar zeer ten dele met uitwisseling van gegevens bezig houden. De tweede reden is dat een eventueel kaderwet eveneens van belang kan zijn met het ring en knelpunten bij gegevensuitwisseling ten behoeve van andere doeleinden. Gekozen zou dan kunnen worden voor een kaderwet op het brede terrein van de voorkoming van onrechtmatig gebruik van overheidsgegevens en overheidsvoorzieningen, de uitoefening van toezicht op de naleving van wettelijke voorschriften en de handhaving van de openbare orde en veiligheid ("bestuursrechtelijke preventie en handhaving"), alsmede de voorkoming, opsporing en vervolging van strafbare feiten ("strafrechtelijke preventie en handhaving"). Het is immers dit brede terrein waarop zich allerlei samenwerkingsverbanden manifesteren die gegevens binnen en tussen het bestuursrechtelijke en strafrechtelijke domein willen uitwisselen.

Bij een verkenning naar een kaderwet gegevensuitwisseling kon het niet alleen gaan om het verkennen van mogelijkheden om knelpunten weg te nemen die op dit moment met betrekking tot het uitwisselen van gegevens bestaan. Ingeendielt, een verbetering van de mogelijkheden tot gegevensuitwisseling die uit hun opnamen van deze knelpunten voortvloeit, schipt een ruwvram grote verenhoudelijkheid voor een toepastelijke indeling van het proces van gegevensuitwisseling. Het begrip "zorgvuldigheid", uitgewerkt in een aantal waarborgen, zou het centrale (kijkt bij iedere vorm en fase van gegevensverwerking in samenwerkingsverbanden moeten zijn.

Verbetering van de gegevensuitwisseling in samenwerkingverbanden is een ambitie die niet alleen met een eventueel kaderwet kan worden gerealiseerd. Daarvoor is ook nodig dat partijen bereid zijn tot samenwerking en het delen van gegevens, doordat de nodige organisatorische voorzieningen treffen en een adequate (technische) infrastructuur bouwen.

4. Karakter van een kaderwet

Een kaderwet (of maatwet) is een wet die de algemene principes, verantwoordelijkheden en procedures regelt, maar geen gedetailleerde regels bevat. Een belangrijke eigenschap van kaderwetten lijkt dan ook dat zij doorgaans niet zelf beleidsinhoudelijke regulatieve keuzes vastleggen, maar vooral randvoorwaarden scheppen waaraan bijvoorbeeld lagere regelgevers, beleidsmakers of uitvoerders dienen te opereren. Een kaderwet voor de gegevensuitwisseling in samenwerkingsverbanden zal in dat licht bezien niet voor ieder samenwerkingsverband in detail behoeven te regelen waaraan dat verband zich heeft te houden. Wel zal een kaderwet een raamwerk bieden waarbinnen de deelnemers aan een samenwerkingsverband hun samenwerking nadrukkelijk in een convenant en in een informatieprotocol, dat de nodige waarborgen voor de bescherming van persoonsgegevens bevat. Een kaderwet kan daarbij de knelpunten wegnemen die nu in de praktijk bij het opstellen van zo'n convenant en protocol worden ervaren.

Het uitgangspunt voor een eventuele kaderwet zou zijn dat zij de bestaande regelgeving met betrekking tot gegevensverwerking op enkele uitzonderingen na in stand zou laten. Dat geldt met name ook voor de daarin vastgelegde waarborgen voor de bescherming van persoonsgegevens, zoals het principe van doelbinding en de rechten van burgers van wie gegevens wordt verwerkt.

(fachs op inzage, correctie en verzet). Een kaderwet voor gegevensuitwisseling in samenwerkingsverbanden zou naast een aantal noodzakelijke afwijkingen of wijzigingen van bestaande wetgeving vooral bestaan uit bepalingen die duidelijkheid moet brengen over wat bij gegevensuitwisseling wel en niet mag, waar de bestaande sectorale wetgeving op de desbetreffende punten onvolgende helderheid bieden.

Een kaderwet voor gegevensuitwisseling zou een algemene aanvulling vormen op wettelijke regelingen die in specifieke gevallen samenwerking voorschrijven en daarbij regels over gegevensuitwisseling geven, zoals de samenwerking die artikel 9 van de Wet structuur uitvoeringsorganisatie werk en inkomen voorschrijft voor het UWV, de SVB en de gemeenter bij de uitvoering van die wet en enige andere wetten. De aanvullende bateskens van een kaderwet zal zijn gelegen in het feit dat, als partijen tot samenwerking besluiten en de uitwisseling van gegevens onder de werkdag van de kaderwet willen laten vallen, deze kaderwet die uitwisseling van gegevens in zo'n samenwerkingsverband legitimeert, faciliteert en normeert. Hiermee is ook gezegd dat de kaderwet niet tot doel heeft een exclusief regime voor gegevensuitwisseling in samenwerkingsverbanden te creëren. Het staat huidige en toekomstige samenwerkingsverbanden vrij ervoor te kiezen hun gegevensverwerking in te richten op grond van de thans al geldende wetgeving.

5. Knelpunten, oplossingen en contexten van een kaderwet

5.1. Van "nec, tenzij" naar "ja, tenzij"

De geheimhoudingsbepalingen in de verschillende wetten zetten een rem op de gegevensuitwisseling in samenwerkingsverbanden. Door in een kaderwet deze geheimhoudingsbepalingen in relatie tot gegevensuitwisseling in samenwerkingsverbanden buiten toepassing te verklaren, ontstaat ruimte om het huidige uitgangspunt bij de verdelkens van gegevens hier oorden, voor samenwerkingsverbanden te transformeren van "nec, tenzij" naar "ja, tenzij".

5.2. Voor gegevensverstrekking aan samenwerkingsverbanden zijn geen afzonderlijke wetswijzigingen meer nodig ...

De ruimte die door het buiten toepassing verklaren van geheimhoudingsbepalingen ontstaat, kan in een kaderwet worden benut door eerste een algemene grondslag op te nemen voor verstrekking van gegevens door de deelnemende partijen aan een samenwerkingsverband. Nu is het voor verstrekking van gegevens aan een samenwerkingsverband vaak nog nodig een specifieke grondslag op te nemen in de desbetreffende wetten en/of daarop gebaseerde uitvoeringsbesluiten. Met zo'n algemene grondslag in de kaderwet is dat niet meer nodig. Op basis van deze algemene grondslag zullen de deelnemers aan een samenwerkingsverband hun samenwerking naar een aantal regels in een convenant. Daarin zullen zij ingevolge de kaderwet onder meer dienen vast te leggen voor welk doel zij gegevens uitwisselen en hoe zij sturing aan het samenwerkingsverband zullen geven. Uit een oogpunt van "accountability" zou een kaderwet verder moeten voorschrijven dat de deelnemers aan het samenwerkingsverband in een informatieprotocol een aantal in deze wet te noemen elementen vastleggen die bij de gegevensverwerking in een samenwerkingsverband het belang van gegevensbescherming dienen.

5.3. ... maar nog wel een verwijsbaarheidstoets

Persoonsgegevens mogen niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verzameld (principe van doelbinding). Dit brengt mee dat voor de gegevensuitwisseling in een samenwerkingsverband moet worden getoetst of zij al dan niet verenigbaar is met de doeleinden waarvoor de gegevens oorspronkelijk zijn verzameld. De uitvoering van deze toets blijft in de praktijk bij tijd en wijle aan rem te zetten op de bereidheid om gegevens uit te wisselen. Aan het beginsel van doelbinding en daarmee aan de

verenigbaarheidstoets kan echter in het licht van de Europese privacyregulering geen afbreuk worden gedaan. Overigens lijkt men in de praktijk soms ten te bremschijde houding, bij de uitvoering van de verenigbaarheidstoets in te nemen. Niet kar toet het achterwege laten van gegevensuitwisseling leiden, waarvoor een goed uitgevoerde verenigbaarheidstoets wel ruimte zou kunnen geven. Waar op dit punt weigering geen uitkomst kan bieden, zou voortlicht nog dat wel kunnen. Overigens lijkt de Nederlandse Afstemming van de Verenigbaarheid van de Europese Unie meer ruimte te geven om in de toekomst ook ingeval van onverenigbaarheid van doelen in een samenwerkingsverband toch gegevens te kunnen verwerven.

5.4. Geen twijfel maar over rechtmatigheid van verstrekking aan alle deelnemers tegelijk en aan een eventueel ondersteunend bureau

De huidige wetgeving gaat bij verstrekking van gegevens aan derden Journaals uit van vormen van bilaterale verstrekking. Er bestaat twijfel of deze wetgeving daarom ook een voldoende grondslag biedt voor gegevensverstrekking aan alle deelnemers van een samenwerkingsverband tegelijk of aan een eventueel ondersteunend bureau, als het voor een effectieve functionering van het verband als geheel ten goede zou komen. De kadernwet kan een bepaling bevatten die deze twijfel wegneemt.

5.5. Ruimte voor deelname van private partijen

Publiek-private samenwerking bij fraudebestrijding en de aanpak van andere vormen van wetsovertreding levert beide kanten voordeel op. De bestaande wetgeving geeft echter betrekkelijk weinig ruimte voor gegevensuitwisseling met private partijen. Tenzij een sectorspecifieke wet voor dat geval gegevensverstrekking mogelijk maakt, zal de verstrekking aan een private partij uitsluitend kunnen worden gebaseerd op een bepaling uit de Wet Bescherming Persoonsgegevens (Wet 6, onder f) die een individuele afwijking vergt van het grondwettelijke belang van de verdragsluitende of ontvangende partij tegen het belang van de betrokken burger op bescherming van zijn persoonlijke levenssfeer. Dit betekent een structurele uitwisseling van gegevens met private partijen. Een eventuele kadernwet zou, onder het stellen van voorwaarden, deze beperking kunnen wegnemen.

5.6. Verplichte verstrekking van noodzakelijke gegevens, tenzij ...

De deelname aan een samenwerkingsverband kan niet vrijblijvend zijn. De kadernwet zou dan ook moeten voorschrijven dat de deelnemers in beginsel verplicht zijn de voor het samenwerkingsverband noodzakelijke gegevens aan de andere deelnemers te verstrekken. Op deze verplichting zou voorafgaand een uitzondering moeten worden gemaakt, voor zover het om de volgende gaat: bijzondere persoonsgegevens zou gaan: gegevens met betrekking tot aanpak profielerend of levensvervalsing, ras, politieke gezindheid, gezondheid, seksuele leven en lidmaatschap van een vakbond. Onder twee overige categorieën van bijzondere gegevens - strafrechtelijke gegevens en persoonsgegevens over onrechtmatig of onrechtmatig gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag - bij uitstek relevant kunnen zijn voor samenwerkingsverband op het brede terrein dat hiervoor onder 3 is beschreven, zouden deze categorieën niet onder voornoemde uitzondering moeten vallen. De verplichting tot gegevensverstrekking zou ook anderszins niet absoluut zijn. Partijen zouden in het informatieprotocol uitzonderingen hierop moeten kunnen opnemen.

5.7. Verstrekking aan opsporingsinstanties en OM wordt eenvoudiger, ...

De samenwerking tussen bestuurlijke en strafrechtelijke instanties kan bij uitstek meerwaarde hebben bij fraudebestrijding en andere activiteiten op het terrein van de rechtspraak en strafrechtbestrijding. Het Wetboek van Strafvordering kent evenwel een systeem voor het vorderen van informatie door opsporingsinstanties en OM, dat een barrière voor een efficiënte vorm van gegevensuitwisseling in samenwerkingsverbanden opwerpt. Het College van procureurs-

gegevens heeft in het verleden al op dit probleem gewezen. Door de desbetreffende bepalingen ingeval van gegevensuitwisseling in samenwerkingverbanden buiten toepassing te verklaren, zal een vordering voortaan niet meer nodig zijn.

5.8 ... verstrekking van strafrechtelijke gegevens ook

In de praktijk bestaat behoefte aan betere mogelijkheden om strafrechtelijke gegevens door politie, bijzondere opsporingsdiensten en OM aan andere partijen binnen het samenwerkingsverband te verstrekken. Op basis van de mogelijkheden op dit punt zijn niet optimaal. Zo moest voor verstrekking van politiegegevens aan de Regionale Informatie- en Expertisecentra (RIEC's) eerst een machtigingsbesluit op grond van de Wet politiegegevens worden afgegeven, volgde later een wijziging van het Besluit politiegegevens en is er in ander onderzoek verspreid te zien convergent en protocol. Op basis van de kadernet zal worden kunnen worden met vastlegging van de verstrekking van politiegegevens, strafrechtelijke gegevens en justitiegegevens bij convenant en nadere uitwerking daarvan in een informatieprotocol.

5.9 Betere legitimatie van het gebruik van moderne analyse-technieken

Samenwerkingsverbanden worstelen met de vraag of en, zo ja, in hoeverre de huidige mogelijkheid allerlei typen van gegevensverwerking bestaan. Dat geldt vooral voor het gebruik van geavanceerde analysemethoden. Het bijvoorbeeld de Infobox Criminaliteit en Omverkeerdbaar Vermogen (ICOV) een door haar te ontwikkelen profiel van bijvoorbeeld de organisatie van matches met alle data waarover zij rechtmatig de beschikking heeft, om een lijst vast te stellen van personen aan wie de grootste risico's zijn verbonden dat zij fraude plegen? Het thans bestaande kaderlijstheid op dit punt belemmert de ontwikkeling en het gebruik van diensten en producten die met moderne analysemethoden geleverd kunnen worden. Om de bestaande onduidelijkheid op dit punt weg te nemen, zou een kadernet kunnen expliciteren dat de door deze kadernet gereuleerde gegevensuitwisseling binnen samenwerkingsverbanden het gebruik kan hebben op alle in dit wet kaderreken typen van gegevensverwerking.

5.10 Vereenvoudiging informatieverstrekking aan burgers

In de praktijk blijkt dat samenwerkingsverbanden zich de vraag stellen of en, zo ja, in hoeverre zij moeten voldoen aan de informatieplicht van artikel 34 Wet bescherming persoonsgegevens. De vraag speelt vooral in het geval van geautomatiseerde bestaansvergelijkingen in een fase die voor het overgrote deel van de betrokkenen niet tot gevolgen leidt. Belangrijk is ook dat het in samenwerkingsverbanden op het terrein van de fraudebestrijding al gewoonte is om gegevensverwerking die, als zij bij betrokkenen bekend wordt, tot calculerend gedrag bij hen kan leiden. De informatieplicht geldt niet in het geval dat de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven, in dat geval dient het samenwerkingsverband de betrokkenen op diens verzoek te informeren over het wettelijk voorschrift dat tot vastlegging of verstrekking van de hem betreffende gegevens heeft geleid. Ter compensatie van het wegvallen van de verplichting de burger individueel te informeren, zou een kadernet kunnen voorschrijven dat bij de oprichting van een samenwerkingsverband ervoor wordt gezorgd dat de algemene informatie wordt gegeven over de gegevensverwerking door het desbetreffende samenwerkingsverband. Deze informatie zou dan bijvoorbeeld op een website van het samenwerkingsverband kunnen worden geplaatst.

5.11 Extra waarborgen voor een zorgvuldige gegevensverwerking

Wilt een kadernet gegevensuitwisseling een integrale verbetering van de gegevensuitwisseling in samenwerkingsverbanden opleveren, dan zal deze kadernet niet alleen een verbetering van de mogelijkheden van gegevensuitwisseling moeten bieden, maar ook vereisten en moeten bevatten die bijdragen aan de kwaliteit van de gegevens en de zorgvuldigheid bij de verwerking daarvan. Daarbij kan onder meer worden gedacht aan explicitering in de kadernet van het vereiste van

noezakelijkheid en de daaruit voortvloeiende beginselen van proportionaliteit en subsidiariteit, waarborgen met betrekking tot het koppelen van gegevensbestanden, de deling van de kwaliteit van de gegevens en de transparantie van de gegevensverwerking en het uitvoeren van een Privacy Impact Assessment.

Uit een begrip van "accountability" is het wenselijk dat de code-wet de deelnemers aan het samenwerkingsverband voorschrijft in een informatieplanterd een aantal elementen vast te leggen die voor de bescherming van gegevens in een samenwerkingsverband van belang zijn. Daarbij kan worden gedacht aan onder meer de volgende elementen: de inrichting van het proces van gegevensverwerking en de waarborgen die hierin zijn opgenomen met het oog op de bescherming van persoonsgegevens, alsmede de informatieverstrekking over de gegevensuitwisseling aan het publiek en aan betrokkenen.

6. Slot

De werkgroep die deze verkenning heeft opgesteld, heeft niet de pretentie met deze verkenning alles tot in detail te hebben doordacht. Zij heeft wel de overtuiging dat de verkenning een voldoende basis geeft om een positieve beslissing over het opstellen van een voorstel voor een federwet te kunnen nemen.

1. Inleiding

Op 20 december 2013 heeft het kabinet de Tweede Kamer een brief gezonden over de aanpak van fraude met publieke middelen. In die brief kondigt het kabinet onder meer een verkenning aan naar een kaderwet voor de gegevensuitwisseling op het terrein van fraudebestrijding. Je vraag die voorligt, is of een kadernet een aantal knelpunten met betrekking tot de gegevensuitwisseling in de bestaande wetgeving kan oplossen in plaats van het aanbrengen van afzonderlijke wettelijke in specifieke wetten.¹

In § 2 van deze verkenning wordt eerst de context geschetst waarbinnen zij heeft plaatsgevonden. In § 3 wordt een aantal knelpunten in de huidige praktijk van gegevensuitwisseling op een rijtje gezet die tijdens de verkenning naar voren zijn gekomen. Vervolgens worden in § 4 de contouren van een mogelijke kadernet geschetst waarmee deze knelpunten zouden kunnen worden opgelost. De notitie eindigt met een slotsbeschouwing (§ 5).

De verkenning is opgesteld door een werkgroep, bestaande uit vertegenwoordigers van de ministeries van Veiligheid en Justitie, Sociale Zaken en Werkgelegenheid en Financiën, van het openbaar ministerie en van de gemeente Tilburg. De werkgroep heeft daarbij in de eerste plaats gebruik gemaakt van ervaringen die zijn opgedaan bij de ontwikkeling van samenwerkingsverbanden waarin partijen gegevens uitwisselen. Verder heeft de werkgroep in april 2014 een brainstormsessie met verschillende genodigden gehouden over knelpunten in de gegevensuitwisseling en de mogelijkheden die een kadernet zou kunnen bieden om deze op te lossen. Ook heeft de werkgroep voor haar verkenning gebruik gemaakt van de in aangegevende kabinetsbrief aangekondigde inventarisatie van de behoefte aan gegevensuitwisseling in een aantal gevallen: vijf jaar geleden over banken, kredietinstellingen, levensverzekering, fraudebestrijding en fraudebestrijding, bij deze inventarisatie is ook naar eventuele knelpunten bij de gegevensuitwisseling gekeken. Voor de verkenning heeft uitbreidend ook raadpleging plaatsgevonden van relevante literatuur, officiële publicaties en websites. Concepten van de verkenning zijn gepresenteerd aan verschillende partijen² om te toetsen of een eventuele kadernet uitkomst zou kunnen bieden. De reacties in die gesprekken waren in het algemeen positief.

In deze verkenning wordt ervan uitgegaan dat de gegevensuitwisseling in een enkel vorm van samenwerkingsverband plaatsvindt. Daarmee wordt gescheidt op de situatie dat twee of meer partijen voor een bepaald doel in een georganiseerd verband samenwerken om om dat doel te bereiken gegevens uitwisselen. Het is vooral in dergelijke samenwerkingsverbanden dat zich knelpunten laten gevoelen als in § 3 zijn beschreven. Het gekozen uitgangspunt staat ook op de gedachte dat gestructureerde vormen van gegevensuitwisseling die niet al in een wettelijke regeling zijn uitgewerkt, meestal binnen een daartoe opgericht samenwerkingsverband plaatsvinden, waarbij de regeling van de gegevensuitwisseling is meegenomen in een convenant en eventueel een protocol. De gerichtheid op samenwerkingsverbanden sluit overigens niet uit dat een eventuele kadernet ook betekenis kan hebben voor gegevensuitwisseling in "reguliere processen". Gegevensuitwisseling in dergelijke processen kan immers zeer wel vorm krijgen in samenwerkingsverbanden. De gerichtheid op samenwerkingsverbanden brengt wel mee dat verstrekking van gegevens met een lichte karakter buiten de reikwijdte van deze notitie vallen. Daar komt bij dat een kadernet althans minder goed leent voor de oplossing van een eventuele knelpunt bij dat type verstrekking. Zo is kadernet althans niet althans een aantal randvoorwaarden voor gegevensuitwisseling waarvan die niet bij randvoorwaarden-verstrekkingen passen, zoals de verplichting om een convenant en een informatieprotocol op te stellen (zie nadar § 4).

¹ Kamerstukken II 2013-2014, 17090, nr. 490, blz. 7-8.

² Presentaties zijn gegeven aan o.a. het Landelijk Platform Geïntegreerde aanpak Ondermijrende Criminaliteit en aan het RIEC-hoofden-overleg.

Een cadewet zou het voordeel hebben dat zij voor allerlei vormen van gegevensuitwisseling één aanvullend kader zou bieden. Het zou dan niet nodig zijn om voor een specifieke vorm van gegevensuitwisseling door middel van een afzonderlijke wet of een afzonderlijk besluit de noodzakelijke wijzigingen in de diverse relevante regelgeving aan te brengen. Als een kadewet, zoals hierna wordt besproken, betrekking zou hebben op gegevensuitwisseling in samenwerkingsverbanden, zou bovendien de situatie ontstaan dat een samenwerkingsverband al als bedoeld in de cadewet een aangrijpingspunt zou kunnen vormen voor bepalingen in de sectorale wetten die de verstrekking van gegevens aan het samenwerkingsverband regelen. Overigens zou het niet per se noodzakelijk zijn dergelijke bepalingen in de sectorale wetten op te nemen; de cadewet zelf zou ook kunnen volstaan als basis voor de verstrekking van gegevens aan samenwerkingsverbanden.

Tot slot is van belang dat de verontking betrekking heeft op gegevensuitwisseling op een breder terrein dan fraudebestrijding. Dit heeft twee redenen. De eerste is dat bestaande samenwerkingsverbanden zich maar zeer ten dele met uitsluitend fraudebestrijding bezighouden (zie § 2.3). De tweede reden is dat een eventuele kaderwet, eventueel van belang kan zijn met het oog op knelpunten bij gegevensuitwisseling ten behoeve van andere doeleinden (zie nader § 4.2).

2. Context verkenning

2.1 Aanleiding verkenning

Fraude met overheidsvoorzieningen is een groeiend probleem. De effecten daarvan reiken verder dan alleen de directe financiële schade voor de overheid. Fraude ondermijnt de integriteit van het economisch stelsel, het vertrouwen in de financiële instellingen, tast de betaalbaarheid van voorzieningen aan en kan leiden tot een vermindering van het maatschappelijke draagvlak voor sociale voorzieningen en tot aantasting van het rechtsgerechtigd. Tegen die achtergrond wil het kabinet fraude zoveel mogelijk voorkomen en waar fraude ondanks alle maatregelen toch nog heeft plaatsgevonden, zo effectief mogelijk bestrijden. Dat vraagt volgens het kabinet om een brede en integrale benadering waarbij de risicovrijheid ook zal samenwerken met gemeenter en private partijen, zoals banken en autoriteiten.³

In de praktijk wordt in het kader van fraudeaanpak al veelvuldig samengewerkt door verschillende partijen. Om tot een efficiënte en doeltreffende samenwerking te komen is uitwisseling van informatie essentieel. Alleen dan kunnen partijen tot zo effectief mogelijk en op elkaar afgestemd de inbrenging komen. Daarbij valt in de praktijk een toenemende inzet op 'intelligentie' en een risico-gestuurde benadering waar te nemen. Dat draait bij aan de identificatie van personen en organisaties die achter de schermen de regio over zware vormen van fraude voeren, en aan een effectieve inzet van de beschikbare capaciteit om fraude te voorkomen en bestrijden.

Bij de uitwisseling van informatie worden ook persoonsgegevens gedeeld. Het delen daarvan moet uiteraard voldoen aan de wettelijke bepalingen ter bescherming van persoonsgegevens. Hetzelfde geldt voor andere gegevens die wettelijk bescherming krijgen. Waar onze wetgeving in algemene zin belangrijke waarborgen voor de bescherming van dergelijke gegevens bevat, blijven zij echter in de specifieke situatie waarin partijen in samenwerkingsverbanden gegevens willen uitwisselen, de nodige knelpunten op te leveren.

Deze knelpunten belemmeren het optreden van een overheid als een georganiseerd geheel, dat maatschappelijke vraagstukken als de aanpak van fraude integraal, effectief en efficiënt moet op te pakken. De samenleving verwacht echter van een overheid dat zij wel als een georganiseerd geheel optreedt. Z'n overheid neemt het oplossen van een maatschappelijk probleem als uitgangspunt, kijkt welke overheidsorganisaties en eventueel private partijen nodig zijn om het probleem te kunnen aanpakken, deelt welke informatie-uitwisseling daarvoor noodzakelijk is en maakt goede afspraken over privacybescherming. De verwachting in de samenleving dat een overheid als een georganiseerd geheel optreedt, neemt ook toe. De ontwikkelingen op het terrein van ICT bieden partijen binnen de overheid immers steeds meer mogelijkheden om tot een snelle, accurate en volledige uitwisseling van informatie te komen en op grond van deze informatie analyses te maken die tot een integraal en effectief optreden leiden. Een verkenning van de mogelijkheden om met een continuïteit tot een betere gegevensuitwisseling te komen, moet dan ook een overheid die langs deze lijnen opereert, als uitgangspunt nemen.

2.2 Dilemma's bij streven naar betere gegevensuitwisseling

Hiervoor is te zeggen dat deze verkenning erop is gericht knelpunten bij de gegevensuitwisseling ten behoeve van de fraudebestrijding in kaart te brengen en te bepalen in hoeverre een kaderwet kan worden genomen. Het is niet de bedoeling bij gegevensuitwisseling niet beperkt is tot het domein van fraudebestrijding. In het bijzonder de genoemde knelpunten zijn even goed voor te doen op andere terreinen waar behoefte bestaat aan een nimmer gebruik van gegevensuitwisseling. Dit is namelijk een eerste dilemma: welk bereik dient een kaderwet gegevensuitwisseling te hebben?

³ Kamerstukken II 2013-2014, 17050, nr. 450, blz. 2

Bij de behoefte aan een breder gebruik van gegevens speelt voorts als dilemma dat de bestaande regelgeving op het gebied van overheeriging van privacybelangen van burgers door grenzen stelt. Waar die grenzen precies liggen is overigens vatbaar voor interpretatie. In de mate waarin een ruimer gebruik van gegevensuitwisseling wordt gezocht, is duidelijk dat in beginsel eerder tegen grenzen wordt aangelopen en dat meer gefundeerde afwegingen dienen te worden gemaakt. Dat deze afwegingsvraag noodzakelijk is, is recent nog gebleken bij de vraag die voortvloeit uit de eerste Kamer en Tweede Kamer zijn gesteld over het verzamelen van gegevens door de Belastingdienst en het uitwisselen van die gegevens met andere overheidsorganisaties¹ en over het gebruik van SyR².

Als voorbeeld van de hier bedoelde dilemma's en belangenafweging kan worden gewezen op de geheimhoudingsplicht van, bij voorbeeld de Belastingdienst. Deze geheimhoudingsplicht strekt zich uit tot het gebruik van de belastingplichtige niet wordt bekendgemaakt zijn van de goede bestelling van relevante gegevens aan de Belastingdienst te verstrekken in de wetenschap dat de Belastingdienst deze gegevens in beginsel niet aan derden verstrekkt. Naast het belang van het heffen van de juiste belasting is hiermee het privacybelang van de burger gedaan. Wat leidt tot het aanleveren van gegevens door ondernemingen is dit privacybelang hierin gelegen dat hun fiscale gegevens veelal bedrijfsgeheimen omvatten, zoals productieprocessen, winstmarges, enzozetten en dergelijke. Met zorgvuldige verwerking van dergelijke gegevens door de Belastingdienst is uiteindelijk het belang van Nederland als gunstig vestigingsland voor het land het nationale bedrijfsleven gemoeid. Dit voorbeeld geeft aan dat naast de belangen die kunnen zijn gemoeid met een breder gebruik van gegevens andere eveneens gerechtvaardigde belangen zich daartegen kunnen verzetten.

Andere dilemma's die bij deze discussie spelen, zijn bij voorbeeld de rol van het voorzorgsrecht van het OM en de bijzondere vraagstelling die zich voordoet bij de overgang van gegevens uit het bestuursrechtelijk naar het strafrechtelijke circuit. Beide stromen kunnen veelal naar eigen zijde reguleren. Het strafrechtelijke circuit kent vooral aparte waarborgen in verband met het feit dat in het algemeen bij vermoeden van het OM sprake is van een verdachte en een vermoeden van een strafbaar feit. Verdachten stellen dan voorwaarden voor het optreden van het OM. Samenwerkingsverbanden die gericht zijn op fraudebestrijding, opereren op het snijvlak tussen het bestuursrecht en het strafrecht. Dit levert nieuwe vragen op, bij voorbeeld de vraag of de gegevensverwerking in zo'n samenwerkingsverband zich onder het regime van de Wet bescherming persoonsgegevens uitstrekt dan wel het regime van Wet politie gegevens en de Wet justitie en strafvorderlijke gegevens.

In dit verband doet zich voorts de problematiek voor dat met intensivering van samenwerkingsvormen waarin het OM deelneemt, het OM zich actiever dan voorheen bezig gaat houden met dat deel van zijn taak dat is gelegen op het gebied van het voortzetten van overnames. In het verleden was de gegevensuitwisseling in het kader van het samenwerkingsverband is veelal nog niet sprake van de klassieke verdachte en een concreet vermoeden van een strafbaar feit. Dat een dergelijke ontwikkeling de behoefte aan een vermenigvuldiging van een dergelijke verschuiving van taken van het OM met zich brengt, kan ook als een dilemma worden aangemerkt.

Een ander imploort dat in een discussie over eventuele uitbreiding van de mogelijkheden van gegevensuitwisseling door een kostenwet of andere relevante belangen en een voorlopende dilemma's scherp in beeld dienen te worden gebracht en goed moeten worden afgevoerd. Zonder een gedegen afweging van een evenwichtige basis onder een eventuele kostenwet geen sprake zijn. Het streven moet er daarbij op zijn gericht dat in zo'n kostenwet een optimale balans tussen de verschillende belangen wordt gezocht. Het is ook om die reden dat een kostenwet de nodige

¹ Zie Kamerstukken II 2014-2015, 32761, nr. 71.

² Zie Kamerstukken II 2014-2015, 2014Z37931 en 2014Z37440.

weezorgen voor een zorgvuldige gegevensverwerking dient te bevatten. Dat kan eren bijdragen dat ook bij de inrichting van een samenwerkingsverband zelf de optimale balans tussen de verschillende relevante belangen wordt verkregen.

2.3 Samenwerkingsverbanden

Om de effectiviteit van het overheidshandelen te vergroten, richten overheidsonderdelen in toenemende mate samenwerkingsverbanden op. We zien dat niet alleen gebieden bij de aanpak van fraude, maar ook op andere beleidsterreinen. Wat daarbij opvalt, is dat er ook samenwerkingsverbanden zijn in het bijzonder met de aanpak van fraude bezighouden en andere samenwerkingsverbanden een bredere scope hebben, die causaal ook in enigszins vorm mede de aanpak van fraude omvat. Dat mege blijkt, als we blieden in vogelvlucht een aantal samenwerkingsverbanden de revue laten passeren.⁹

De Belastingdienst, de Inspectie GZW, het UWV, de gemeenten, het OM, de SVB, de ministeries van Financien en van Sociale Zaken en Werkgelegenheid en de politie werken samen in een interveniëstructuur met het oog op het voorkomen en bestrijden van fraude. Het gaat daarbij om belasting- en premiefraude, uitkeringfraude, illegale tewerkstelling en de daarmee samenhangende misstanden. Deze partijen hebben daartoe in 2003 een samenwerkingsovereenkomst gesloten (de politie is later toegetreden). De interveniëstructuur bestaat uit een landelijke stuurgroep, een analysefunctie, regionale platformen en interventiecellen. In deze structuur werken de partners niet alleen op strategisch, tactisch en operationeel niveau samen, maar delen ze ook gegevens met elkaar. Het betreft niet alleen gegevensuitwisselingen die wettelijk geboden zijn, maar ook geïntercedeerd bestandskoppelingen op basis waarvan niet de inzet van het instrument Systeem Riden Informatie (SYRI) risico-analyses worden uitgevoerd en eventuele interventies worden voorbereid.¹⁰

Om de integriteit van de financiële sector te versterken is in 1999 het Samenwerkingsverband Financieel Expertise Centrum (FEC) opgericht. Aan dit samenwerkingsverband nemen de volgende partijen deel: de AIVD, de AFM, de Belastingdienst, EBN, de FIOD, de politie en het OM. Het FEC heeft tot taak een structurele informatie-uitwisseling tussen de partners te creëren, een kennisbestuur te realiseren en projecten uit te voeren. Het FEC richt zich als bewaker van de financiële integriteit op onder meer de volgende schadelijke gebieden: misbruik van de vastgoedmarkt, identiteitsfraude, hypotheekfraude, beleggingsfraude en cybercrime.¹¹ De manier waarop de FEC-partners samenwerken en met elkaar informatie uitwisselen is vastgelegd in een convenant, respectievelijk informatieprotocol.¹²

In 2013 hebben verschillende partijen de Infobox Crimineel en Overneembaar Vermogen (ICOV) opgericht. Het betreft het OM, de politie, de Belastingdienst, de Douane, de FIOD en de Financieel Intelligence Unit Nederland. Doel van ICOV is het in kaart brengen van overneembaar of crimineel vermogen, het blootleggen van witwas- of fraudeconstructies en het kunnen innemen van overheidsoverdrachten ter ondersteuning van de publiekrechtelijke toezichtvoering van de strafrechtelijke organisatie. Het doel staat voor ogen: houdt ICOV zich onder meer bezig met het opstellen van rapportages, criminaliteitsbeoordelingen, risico-indicatoren en procesprotocollen. Een en ander is vastgelegd in een convenant en protocollen.¹³

⁹ Voor een uitgebreider overzicht van samenwerkingsverbanden wordt verwezen naar bijlage 1.

¹⁰ Zie:

http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/nieuwsvernieuwend/bescherming_rubriecatie/infocentrum_interventiecellen

¹¹ Eénheidsakten II 2013-2013, 21579, nr. 1, blz. 3.

¹² Zie: <http://www.fec-ssd.nl/nl/nl/overeenkomst>

¹³ Zie Convenant FEC 2009, Stort 2009, 71, en informatieprotocol FEC 2011, Stort. 2011, 21708.

¹⁴ Zie Convenant ICOV 2013, Stort 2013, 24607, Protocol gegevensverwerking ICOV Productie 2013, Stort 2013, 24608, en Protocol gegevensverwerking ICOV Research and Development 2013, Stort. 2013, 24610.

Met het oog op de versterking van de bestuurlijke aanpak en de ondersteuning van de integrale aanpak van de georganiseerde criminaliteit zijn in de afgelopen jaren de Regionale Informatie- en Expertisecentres (RIEC's) en het Landelijk Informatie- en Expertisecentrum (LIEC) opgericht. Binnen de RIEC's en het LIEC werken de volgende partijen samen: de gemeenten, het OM, de politie, de Belastingdienst, de Douane, de FIOD, de Inspectie SZW, de provincies, de Koninklijke Marechaussee en de IND. De samenwerking heeft tot doel gezamenlijk invaag te geven aan:

1. een bestuurlijke en geïntegreerde aanpak van de georganiseerde criminaliteit door naast strafrechtelijke ook bestuursrechtelijke en fiscale maatregelen te treffen;
2. de integratie van veiligheidsstructuren binnen de economische sectoren en publieke voorzieningen die vatbaar zijn voor bedreiving door de georganiseerde criminaliteit;
3. de bestrijding van zijn hindernisposten en
4. de bevordering en ondersteuning van integratievoorzieningen door het openbaar bestuur op grond van de Wet Bibob.

De samenwerking richt zich voor de eerste twee doelen op ondernemen als mensenhandel, georganiseerde hennepcultuur en fraude in vastgoedsector. De samenwerking is vastgelegd in een bestuurlijk akkoord en een convenant.¹² In de loop van 2014 zal de verwerking van persoonsgegevens binnen de RIEC's nader worden geregeld in een privacyprotocol.

Naast samenwerkingsverbanden waaraan uitsluitend overheidspartijen deelnemen, ontstaan in toenemende mate samenwerkingsverbanden waar ook private partijen participeren. Publiek-private samenwerking levert beide kanten voordelen op. De overheid leert van de private sector. Zo zit er veel kennis bij het bedrijfsleven over nieuwe ontwikkelingen, risico's en technologieën. Omgekeerd steelt de private sector ook veel op van de overheid. De samenwerking levert niet in de laatste plaats voordeel op door gebruik te maken van elkaars informatie. Ook private partijen beschikken over informatie die voor het voorkomen en bestrijden van fraude en andere vormen van criminaliteit van belang is. Zowel de private partij als de publieke partij kan op basis van uitgewisselde informatie aan ondernemen of een interventie plannen die bijdraagt aan het voorkomen en bestrijden van criminaliteit. Over welk soort verbanden te noemen: energielevering bij de aanpak van illegale elektriciteitsrijen, caravans bij het voorkomen van valhuusfraude, financiële dienstverleners bij het tegengaan van witwassen en transportondernemingen bij de handel in verboden goederen.

Ook publieke en private partijen werken vaak met elkaar samen op basis van convenanten. Enkele voorbeelden van dergelijke convenanten zijn:

1. Convenant verbetering bestrijding zorgfraude tussen de Nederlandse Zorgautoriteit, de Inspectie voor de Gezondheidszorg, Zorgverzekeraars Nederland, de Inspectie SZW, de FIOD, de Belastingdienst, het OM, het Centrum Indicatiestelling Zorg en het Ministerie van VWS;¹³
2. Convenant hermetiteit Zeeland - West-Brabant 2013 tussen gemeenten, politie, GMP, woningcorporaties, notarisvereniging, UWV en SVB;¹⁴
3. Convenant aanpak verzekeringsfraude tussen Verbond van Verzekeraars, zorgverzekeraars, het GMP en de politie;¹⁵

¹² Zie het Bestuurlijk Akkoord Samenwerking Des Centrale Aanpak Georganiseerde Criminaliteit van september 2008 (kadersstukken II, 29-9-11, nr. 27) en het Convenanten benoemen van bestuurlijke en geïntegreerde aanpak georganiseerde criminaliteit, handhaving hindernisposten en bevordering integratievoorzieningen

¹³ <https://zoek.officielebekendmakingen.nl/bsk-2013-1121.html>

¹⁴ Zie <http://www.rijksrechtspraak.nl/documenten/rijksrechtspraak/2013/09/12/convenant-verbetering-van-besluiting-zorgfraude.html>

¹⁵ Zie <http://www.hetcc.nl/binaries/content/assets/cc/cosiers/hermetiteit13-09-0679-samenwerk-hermetiteit-zeeland-west-brabant-2013.pdf>. Omdat het inspecteren van hennepkwekerijen vrijwel altijd gepaard gaat met andere strafbare feiten zoals diefstal van elektriciteit, belastingontduiking en uitbreiding fraude, richt de samenwerking zich ook op deze vormen van criminaliteit.

¹⁶ Zie: <https://www.verzekeraars.nl/over-het-verband-elf-regulerings/Documenten/Convenanten/Convenant-aanpak-verzekersfraude.pdf>

Het delen van informatie tussen publieke en private partijen ligt gevoelig. Immers, burgers mogen ervan uitgaan dat informatie die zij aan de overheid verstrekken niet zo maar bij private partijen terecht komt. Anderszins geldt dat verstrekking van gegevens door private partijen naar de overheid het gevoel kan oproepen van "big brother is watching you". Een (wettelijke) grenslijn voor het uitwisselen van gegevens tussen publieke en private partijen ontbreekt vaak.¹⁶ Indien een kaderwet gegevensuitwisseling mede betrekking zou moeten hebben op gegevensuitwisseling tussen publieke en private partijen, kan ligt het voor de hand dat deze wet de nodige waarborgen tegen onwettelijke misbruik van gegevensverwerking bevat. Welke dat zouden kunnen zijn, komt in § 4.2 aan bod.

Van de hier genoemde samenwerkingverbanden houdt een inderdaad zich uitsluitend met fraudebestrijding bezig. De meeste samenwerkingsverbanden hebben een taak die zich niet beperkt tot het onderzoek van de aanpak van fraude, maar ook tot andere te nemen maatregelen. Het dat aspect zal rekening moeten worden gehouden bij de aanpak van fraude, maar de reikwijdte van een eventuele kaderwet. Een kaderwet die zich beperkt tot gegevensuitwisseling ten behoeve van de fraudebestrijding zal tot gevolg hebben dat verschillende samenwerkingsverbanden ten dele wel en ten dele niet onder de werking van de kaderwet vallen. Op de vraag welke consequentie daaraan verbonden zou kunnen worden, wordt hierin ingegaan in § 4.2.

Tot slot is van belang te onderkennen dat deelnemers aan samenwerkingverbanden weliswaar gegevens uitwisselen ten behoeve van bijvoorbeeld het formuleren van een gezamenlijke interventiestrategie of het opstellen van bepaalde informatieproducten waaraan gezamenlijk behoefte bestaat, maar vervolgens op basis daarvan niet eigen verantwoordelijkheid en niet gebruikmaking van de eigen bevoegdheden eventueel acties ondernemen. Anders gezegd: een samenwerkingsverband laat de bestaande verantwoordelijkheden en bevoegdheden van de deelnemers op dit punt in stand.

2.4 Verschillende wettelijke kaders en categorieën gegevens

Overheidsinstanties en eventueel private partijen werken in samenwerkingsverbanden verschillende categorieën gegevens. De categorie die daarbij doorgaans de meeste aandacht krijgt, betreft *persoonsgegevens*. Dit standpunt maakt voort uit het feit dat het bij persoonsgegevens om gegevens gaat die grondrechtelijke bescherming genieten op basis van internationale verdragen, regelingen van de Europese Unie en onze eigen Grondwet.¹⁷ De bescherming van persoonsgegevens is verder geregeld in de Wet Bescherming Persoonsgegevens (Wbp) als algemeen kader voor de verwerking van persoonsgegevens en daarnaast in sector specifieke regelingen als de Wet politiegegevens (Wvp)¹⁸ en de Wet Justitie en Strafvordering (Wjs).

¹⁶ Zo mag de Belastingdienst op grond van artikel 43c, eerste lid, van de Uitvoeringsregeling Algemeen wet rijksbewaarden alleen gegevens verstrekken aan bestuursorganen. Een uitzondering op het beginsel dat geen gegevens aan private partijen mogen worden verstrekt, is te vinden in de Aanwijzing Wet justitie en strafrecht (Wjst) van het College van procureurs-generaal. Zo kunnen ten behoeve van het voorkomen en opsporen van strafbare feiten strafrechtelijke gegevens worden verstrekt aan bepaalde "gevoelige" bedrijven of instellingen op het gebied van bijvoorbeeld vervoer en transport, telecommunicatie en internet, beveiliging, financiën, onderwijs, kinderactiviteiten, energie, vervoersvoorziening, kunst en onderdelen.

¹⁷ Zie artikel 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele vrijheden (EVRM), het Dataovereenkomstverdrag uit 1981 (E.O. 108), nr. 7) de Europese Privacyrichtlijn uit 1995 (Richtlijn 95/46/EG, Pb L 281), artikel 8 van het Handvest van de grondrechten van de Europese Unie (Pb EG 18 december 2000, C 364/3) en artikel 10 van de Grondwet.

¹⁸ De Wvp is niet alleen van toepassing op politiegegevens. Op grond van artikel 46 Wvp is deze wet van overeenkomstige toepassing op de verwerking van persoonsgegevens door bijzondere opsporingsrechter.

In de Wbo wordt een persoonsgegeven aangemerkt als elk gegeven betreffende een geïdentificeerde of identificeerbare persoon. Het gegeven dient dus informatie over een persoon te bevatten. De feitelijke of wettelijke gegevens over eigenschappen, opvattingen of gedragingen zal dat uit de aard van de gegevens voortvloeien. Maar ook telefoonnummers, kentekens van auto's en postcodes met huisnummers dienen onder omstandigheden als persoonsgegevens te worden aangemerkt.¹⁹

De Wbo definieert bepaalde gegevens als *bijzondere persoonsgegevens*. Voor dergelijke persoonsgegevens geldt een apart regime. Het gaat om gegevens met betrekking tot (zware) misdrijven of levensvervalsing, ras, politieke gezindheid, gezondheid, seksuele leven, levenswijze van een vrouw, strafrechtelijke gegevens en persoonsgegevens over anamnese of hinderlijk gedrag in verband met een uitsluitend verbod naar aanleiding van het gedrag. De verwerking van dergelijke gegevens is verboden, tenzij de wet een uitzondering schept. Zo'n uitzondering bestaat bijvoorbeeld voor strafrechtelijke persoonsgegevens, indien de verantwoordelijke de gegevens heeft verkregen krachtens de Wvjo of de Wvsg (artikel 22, derde lid, Wbo).

Politiegegevens zijn persoonsgegevens die in het kader van de uitoefening van de politietak worden verwerkt. Strafvorderlijke gegevens zijn gegevens die zijn verkregen in het kader van een strafrechtelijk onderzoek en die het OM in een strafdossier of langs geautomatiseerde weg verwerkt. Bij justitie gegevens gaat het om bepaalde beslissingen van de rechter of het OM ten aanzien van bepaalde personen. Bij zowel strafrechtelijke als justitie gegevens gaat het om gegevens van personen, maar ook om gegevens over een rechtspersoon. Van belang is verder dat, wanneer gegevens op grond van de Wvjo of de Wvsg aan partners in een samenwerkingsverband zijn verstrekt en vervolgens binnen dat verband worden doorverstrekt, die twee wetten niet meer van toepassing zijn en de Wbo geldt.²⁰

Samenwerkingsverbanden verwerken immers niet alleen persoonsgegevens. Een andere categorie gegevens waaraan gedacht kan worden, betreft *bedrijfs- of beheersgegevens*. Het gaat hier om gegevens die bijvoorbeeld in het kader van de uitoefening van toezicht zijn verzameld.²¹ Deze gegevens hebben vaak een vertrouwelijk karakter. Verder valt zo verstaan op gegevens die uitsluitend voor werpen aanstoden, bijvoorbeeld gestolen goederen of hertrouwingswijzer. Dergelijke gegevens zijn geen persoonsgegevens, indien deze geen informatie bevatten met betrekking tot personen in hun maatschappelijke positie kunnen worden geraakt. Het gaat dan om zuivere beheersgegevens. Hetzelfde geldt voor gegevens die oorzaken van of andere registratiegegevens identificeren. Het feit dat deze zaken via een openbaar register zoals de kadaster, registratie tot een individuele natuurlijke persoon kunnen worden herleid, doet hieraan op zichzelf niet af.²²

2.5 Verschuilde bron gegevensverwerking

Bij het inventariseren van locipersonen in de gegevensuitwisseling en de verkenning van de mogelijkheden om deze met een knifknip op te lossen, is het van belang vooral te onderkennen

¹⁹ Kamerstukken II 1997-1998, 25992, nr. 3, blz. 46-47.

²⁰ Dit is bijvoorbeeld het geval wanneer de politie op grond van artikel 20 Wvjo gegevens verstrekt aan de reclassering en de reclassering in het kader van een publiekrechtelijk samenwerkingsverband deze gegevens wil doorverstreken aan de gemeente. Met het oog op een dergelijke situatie bijwilt artikel 22, derde lid, Wbo dat het verbod om strafrechtelijke persoonsgegevens te verwerken, niet van toepassing is op verwerkingen door of ten behoeve van publiekrechtelijke samenwerkingsverbanden van verantwoordelijke of groepen van verantwoordelijke, indien de verwerking noodzakelijk is voor de uitvoering van de taak van deze verantwoordelijke of groepen van verantwoordelijke en zij de uitvoering is voorzien in zodanige maatregelen dat de persoonlijke levenssfeer van de betrokkene niet onaanvaardig wordt geschaad (Kamerstukken II 2008-2009, 31 841, nr. 3, blz. 5).

²¹ Zie bijvoorbeeld artikel 19.3 Wet milieubeheer en artikel 1.93 Wet op het financieel toezicht.

²² Kamerstukken II 1997-1998, 25992, nr. 3, blz. 47.

de gegevensuitwisseling²³ verschillende verschijningsvormen kan hebben. Deze vormen laten zich categoriseren naar niveau en doel van uitwisseling, naar vorm van verwerking, naar de aard en frequentie van de uitwisseling, naar de vraag of van: unilaterale, bilaterale dan wel multilaterale verstreking sprake is, naar herkomst en – tot slot – naar de adresant van de gegevens.

Als het gaat om het niveau en doel van gegevensuitwisseling, kan onderscheid worden gemaakt tussen de volgende niveaus:

1. **Strategisch.** Het gaat hierbij om verwerking van gegevens, veelal van statistische aard, met het oog op het signaleren van trends en ontwikkelingen. Hiervoor worden in beginsel geen persoonsgegevens gebruikt.
2. **Tactisch.** Het gaat hierbij om verwerking van gegevens om tactische analyses te maken die uitmonden in mogelijke interventiestrategieën. Voorbeelden hiervan op het bredere terrein van criminaliteitsbestrijding en handhaving zijn de Bestuurlijke Criminaliteitsbeoordelingen (BCBA's) die de RIEC opstellen²⁴, en de beleidsaanbevelingen die de Opleidingsinstituten uitvoeren. Voor het opstellen van dergelijke analyses kan het noodzakelijk zijn ook persoonsgegevens te gebruiken. Daarbij kunnen zo mogelijk vormen van pseudonimisering of anonimisering worden toegepast.²⁵
3. **Operationeel/zaakgericht.** Het gaat hierbij om gegevensuitwisseling in een concrete casus met als doel het verkrijgen van een goede informatiepositie op basis waarvan gezamenlijk kan worden beslist welke aanpak het meest effectief is. Voorbeelden hiervan zijn de gegevensuitwisseling binnen het FEC voor het opstellen van adviezen aan de RIEC-partners voor het uitvoeren van bepaalde interventies²⁶ en de inkomens- en vermogensrapporten van de ICOPV²⁷. Het opstellen van dergelijke casusanalyses brengt uit de aard der zaak mee dat persoonsgegevens worden verwerkt.

De vorm van verwerking kan op de volgende aspecten betrekking hebben:

1. **Wettelijk.** Te denken valt aan schriftelijke en mondelinge gegevensuitwisseling tijdens zgn. informatietoets of -pleinen in samenwerkingsverbanden. Er wordt hierbij geen gebruik gemaakt van ICT-voorzieningen.
2. **Geautomatiseerd.** Binnen samenwerkingsverbanden wordt op zeer verschillende manieren gebruik gemaakt van ICT-voorzieningen. In sommige gevallen is het gebruik van ICT slechts ondergeschikt aan het primaire proces. Denk aan (beveiligde) systemen om de gegevensuitwisseling zorgvuldig te ontvangen en door te zenden en eventueel op maat vorm te kunnen geven. Dergelijke systemen zijn het 'Colleges Collaboration Tool' (CoCoTo) van het FEC en het RIEC IS van de RIECs²⁸. Bij deze systemen vervult het secretariaat van de samenwerking nog een belangrijke informatieve rol bij het verdelen en uitzetten van de gegevens. Dat is al weer anders bij geautomatiseerde, ter beschikking staande waarbij verspreiden op basis van een informatie- en autorisatiemethode geheel automatisch van bronhouder naar eindgebruiker gaat. Voorbeelden hiervan zijn Inspectieweb Bedrijven en Inspectieweb Milieu van de Inspectie Transport en Leefomgeving²⁹ en Suwi-Inkijk. Tot slot zijn er samenwerkingsverbanden waar ICT-toepassingen centraal staan en voor een groot deel het

²³ Onder gegevensuitwisseling wordt hier in termen van de Wbo verstaan de verstreking van gegevens aan het samenwerkingsverband en de verdere verwerking van die gegevens binnen het samenwerkingsverband.

²⁴ Zie <http://www.fec.nl/instrumenten/advies>.

²⁵ Bij pseudonimisering wordt een geïdentificeerd gegeven vervangen door een ander identificerend gegeven. Bij anonimisering worden gegevens omgemaakt naar een vorm die niet meer met iemand kan worden geassocieerd.

²⁶ Zie het FEC-jaarverslag 2012-2014, voor het jaar 2014, blz. 9 (http://www.fec-partners.nl/media/76/45/795533/123/fec-jaarverslag_2012-2014_voor_het_jaar_2014.pdf).

²⁷ Zie Convenant ICOPV 2013, Start 2013, 24607 (<http://zoet.officiëlebelangden.nl/text-2013-24607.html>).

²⁸ Zie het jaarverslag 2012 van het IEC, blz. 28 (http://www.lic.nl/doc/130156_RIEC-IEC-jaarverslag_web.pdf).

²⁹ Zie <http://www.informatieuitwisselingsmilieu.nl/page.php?id=8>. Inmiddels is bij Inspectieweb Milieu en Inspectieweb Bedrijven voorzien in de mogelijkheid van een bulkvraag. Analisten kunnen grote hoeveelheden gegevens opvragen om risico-analyses op te stellen.

primaire proces beslezen. Hierbij kan worden gedacht aan gegevensuitwisseling door koppeling van bestanden van verschillende partners om met behulp van geavanceerde software bepaalde patronen te ontdekken ("data mining")¹⁹, gericht(e) bevragingen in databestanden van verschillende partners om bepaalde profielen vast te stellen ("profiling"). Voorbeelden van dergelijke verwerkingen zijn verwerkingen met behulp van het Systeem Risico Indicatie (SyRI)²⁰ en verwerkingen door COV.

Aus het gaat om de *zand en frequentie* van de uitwisseling, kan zowel worden gedacht aan verstrekking op *ad-hoc-basis* ten behoeve van een bepaalde casus als aan gegevensuitwisseling van structurele aard. Bij het laatste valt te denken aan het maandelijks aan elkaar rapporteren van controles in een bepaald gebied en aan bepaalde producten die periodiek kunnen worden geleverd, zoals de COV-rapportage inkomsten en Vermogen.

Bij gegevensuitwisseling kan het gaan om zowel *unilaterale, bilaterale als multilaterale* verstrekking van gegevens. Bij *unilaterale* verstrekking is sprake van verstrekking door één partij aan één andere partij, bij *bilaterale* verstrekking van verstrekking door twee partijen over en weer en bij *multilaterale* verstrekking van verstrekking door en aan meer dan twee partijen.

De herkomst van de gegevens kan divers zijn. Een belangrijke, zo niet belangrijkste bron van de gegevens zal bij *samenwerkingsverbanden* uiteraard gelegen zijn in verstrekking door de deelnemers zelf. De samenwerking zal immers mede gestuurd zijn op de gedachte dat de deelnemers over gegevens beschikken die voor de andere deelnemers met het oog op het doel van het samenwerkingsverband van belang zijn. De gegevens kunnen echter ook een andere herkomst hebben. Daarbij kan worden gedacht aan gegevens uit openbare registers, gegevens uit andere openbare bronnen, gegevens uit registraties met authentieke gegevens, zoals de Basisregistratie personen, en gegevens die van bedrijfsinformatiebureaus als Dun & Bradstreet afkomstig zijn.²¹

Tot slot de *afbreken* van de gegevens. Bij samenwerkingsverbanden kan de gegevensuitwisseling in de eerste plaats bestaan uit directe verstrekking van gegevens aan één of meer andere partners in het verband, zonder dat deze gegevens in een apart bestand worden opgeslagen.²² Voor deze vorm van gegevensuitwisseling zijn alleen de wettelijke regelingen van belang die voor de betrokken partijen gelden voor het verstrekken van gegevens aan het samenwerkingsverband, voor de politie de Wvpo, voor het CM de Wvfga van voor de overige betrokken partners de Wop (nietig voor hen nak een bijzondere wet geldt). De gegevensuitwisseling kan ook bestaan uit verstrekking aan het samenwerkingsverband zelf, waarbij een organisatie die het verband ondersteunt, de verstrekte gegevens verwerkt tot specifieke informatieproducten als een *dataanalyse*, een *profiel* of een *profiel* van bepaalde personen of bedrijven. Deze informatieproducten worden dan vervolgens weer ter beschikking gesteld aan de deelnemers aan het samenwerkingsverband. De verwerking van gegevens tot dergelijke informatieproducten valt onder de Wvpo. Zo'n verwerking zal in beginsel moeten worden aangemeld bij het College bescherming persoonsgegevens (art. 27 Wvpo e.v.).

2.6 Belang van *proportionaliteit* bij gegevensuitwisseling

Bij een verkenning naar een kadervoor gegevensuitwisseling kan het niet zelden gaan om het vaststellen van mogelijkheden om knelpunt op weg te nemen die op dit moment met betrekking tot

¹⁹ Bij deze vorm van gegevensverwerking wordt de computer in feite zelf het werk. Mits de te verwerken data voldoende gestructureerd worden aangeboden, kunnen bepaalde computercode zelf uit grote data mogelijk relevante patronen halen. Daarmee kunnen modellen worden gemaakt waarmee niet alleen actuele risico's in beeld kunnen worden gebracht, maar ook voorspellingen doen omtrent risico's die zich mogelijk in de toekomst gaan voordoen ("predictive modeling").

²⁰ Zie artikel 65 van de Wet structureel uitvoeren organisatie werk en inkomens (Wet Sumi).

²¹ Vgl. artikel 7 Protocol gegevensverwerking (COV Productie 2013, Sect. 2013, 2460).

²² Zo worden in het Maritiem Informatie Knooppunt van de kustwacht, waarin o.a. de politie, de Koninklijke marechaussee en de douane samenwerken, wel gegevens uitgewisseld, maar is er geen eigen bestand.

Het uitwisselen van gegevens bestaan, integendeel, een verbetering van de mogelijkheden tot gegevensuitwisseling die uit het wegnemen van deze knelpunten voortvloeit, schept een eveneens, grote verantwoordelijkheid voor een zorgvuldige inrichting van het proces van gegevensuitwisseling. Anders gezegd: er zal een goede balans moeten worden gevonden tussen enerzijds de met een kadernet bedoelde verbetering van de mogelijkheden van gegevensuitwisseling en anderzijds de behoefte aan zorgvuldigheid bij de uitwisseling. Beide kunnen hand in hand gaan, als een kadernet niet alleen knelpunten wegneemt, maar ook de nodige waarborgen voor een zorgvuldige gegevensverwerking bevat. Zó'n kadernet kan een uit een nieuwe impuls geven aan een zorgvuldige omgang met gegevens in de al bestaande praktijk van gegevensuitwisseling.

Dat bij iedere vorm van gegevensverwerking zorgvuldigheid voorop dient te staan, is op zich niets nieuws. De Wip schrijft in artikel 5 nu al voor dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt. Weer liet hij een vervulling van mogelijkheden van gegevensuitwisseling in samenwerkingverbanden evenwel om gaat, is dat het principe van een zorgvuldige omgang met persoonsgegevens nog meer dan nu, een algemeen erkende en aanvaardde praktische toetssteen bij de inrichting van deze gegevensuitwisseling zou kunnen vormen.

Zó'n toetssteen zou uiteraard in de eerste plaats gebaseerd kunnen worden op een aantal bestaande waarborgen, maar het principe van dualiteit, het noodzakelijkheidsvereiste en de beginselen van proportionaliteit en subsidiariteit. Dergelijke waarborgen vloeien voort uit internationale verdragen, EU richtlijnen en de daarop gebaseerde nationale wetten ter bescherming van persoonsgegevens voort. Wil het principe van een zorgvuldige omgang met persoonsgegevens in samenwerkingverbanden een voldoende praktische toetssteen kunnen vormen, dan is het wenselijk dat een eventueel kadernet een aantal aanvullende, meer specifieke waarborgen bevat. Te denken valt aan waarborgen met betrekking tot onder meer het koppelen van gegevensbestanden, de duiding van de kwaliteit van de gegevens en het uitvoeren van een "Privacy Impact Assessment". Een uitgebreidere uiteenzetting van mogelijke waarborgen is hierna in § 4.7 te vinden.

Het begrip "zorgvuldigheid", uitgedrukt in een aantal waarborgen, zou aldus het centrale criterium bij iedere vorm en fase van gegevensverwerking in samenwerkingverbanden moeten zijn. Dit impliceert dat bij de afweging wat bij gegevensverwerking wel en niet kan, dit begrip "zorgvuldigheid" telkens een leidende rol dient te vervullen. De eis van zorgvuldigheid brengt ook mee dat de uitkomsten van deze afwegingen en de daarbij gebruikte argumenten zo transparant mogelijk zijn.

Het vastleggen van een aantal waarborgen met betrekking tot een zorgvuldige gegevensuitwisseling in een kadernet biedt niet alleen houvast voor partijen bij de inrichting van de processen waarin zij gegevens uitwisselen. Dergelijke waarborgen geven ook een houvast voor degenen van wie persoonsgegevens worden afgewisseld. Met een verwijzing naar deze waarborgen kunnen zij immers, zo nodig, betwisten dat van een zorgvuldige gegevensuitwisseling sprake is. Het vastleggen van deze waarborgen in een kadernet vergroot aldus de transparantie en daarmee de verantwoordelijkheid en aansprakelijkheid ("accountability") van de partijen in het samenwerkingsverband voor een zorgvuldige gegevensuitwisseling.

2.7 Betere gegevensuitwisseling: zaak van meer dan wetgeving alleen

Verbetering van de gegevensuitwisseling in samenwerkingverbanden is een ambitie die niet alleen met een eventueel kadernet kan worden gerealiseerd. Daarvoor is ook nodig dat partijen bereid zijn tot samenwerking en het delen van gegevens, daartoe de nodige organisatorische voorzieningen treffen en een adequate (technische) infrastructuur bouwen.

De bereidheid tot samenwerking hangt in de praktijk meestal af van de vraag of betrokken partijen belang in samenwerking zien. Vaak is het belang daarvan evident en soms is de samenwerking zelfs verankerd in wetgeving.³⁴ Intussen drukt wat steeds meer het besef is: overheidsorganisaties door dat het belang van samenwerking niet uitsluitend gelegen hoeft te zijn in een specifiek belang dat een individuele organisatie bij een eigen goede taakuitvoering heeft, maar dat samenwerking ook een breder, overkoepelend publiek belang kan meebrengen. Als organisaties dat niet al te zichzelf zijn gaan beseffen, is het wel de publieke zaak die de stap tot samenwerking geeft. Zoals ook al in § 2.1 naar voren kwam, verwachten burgers en bedrijven immers in toenemende mate dat de overheid als één georganiseerd geheel optreedt.

Een ander neemt niet weg dat samenwerking waar dat mogelijk en zelfs nodig zou zijn, niet steeds wettelijk verplicht is. Het komt nog voor dat cultuurverschillen en verkolend denken samenwerking in de weg staan.³⁵ Hier ligt vooral een bestuurlijke opgave om deze drempels tot samenwerking te slechten. Een kaderwet gegevensuitwisseling kan in dit verband helpen, omdat het niet langer mogelijk is zich te verschillen achter het argument dat bepaalde wettelijke voorschriften het uitwisselen van gegevens belemmeren en daarmee de mogelijkheden tot samenwerking beperken.

De bereidheid tot het uitwisselen van gegevens zal ook zijn ingegeven door het belang dat men daarbij heeft. Het directe belang bij de verstrekking van gegevens zal doorgaans bij de ontvangende partij liggen. Daar zal immers mede op basis van de ontvangen informatie een analyse kunnen uitvoeren, een interventie kunnen plannen dan wel daarop een andere handeling kunnen baseren. Doch ook de verstrekkende partij kan indirect belang bij de verstrekking hebben. Zo kan verstrekking van gegevens door de politie aan een gemeente er toe leiden dat de gemeente een maatregel neemt die een bepaalde vorm van criminaliteit voorkomt, zodat de politie niet zelf hoeft op te treden. In dit licht gezien hoeft samenwerking niet te betekenen dat er a tijd van een bilaterale of multilaterale verstrekking van gegevens sprake moet zijn, ook een unilaterale verstrekking van gegevens kan de belangen van beide betrokken partijen dienen.

In het geval dat er bij een partij geen taken of belangen zijn aan te wijzen die tot verstrekking van gegevens van een andere partij roepen, kan een goede taakuitvoering door die andere partij juist waardevol tot verstrekking zijn. Uitgaande van een kaderwet is in zo'n geval verstrekking mogelijk, maar is ook dan vooral sprake van een vrijwillige opgave. Dit doet mogelijkheid te benutten door samenwerkingsafspraken te maken. Als deze opgave niet wordt opgepakt, realiseert slechts het middel van een wettelijke verplichting tot verstrekking.

Om de gegevensuitwisseling in een samenwerkingsverband goed te laten verlopen, dient ook een weloverwogen juridische voorziening te worden getroffen. Van essentiële belang is dat de eigen informatiebeschouwing op orde is: weten de verschillende organisaties welke gegevens zij in huis hebben en hebben zij de verwerking van deze gegevens in goede procesbeschrijvingen vastgelegd, waaruit helder naar voren komt op welke wettelijke grondslagen een verwerking plaatsvindt en wie geautoriseerd is om toegang tot welke (categorieën van) gegevens te hebben? Slechts vanuit een adequaat beeld van de eigen informatiebeschouwing kunnen organisaties vervolgens de vraag onder ogen zien welke (categorieën van) gegevens noodzakelijk zijn voor een samen op te richten samenwerkingsverband en zij om die reden willen gaan uitwisselen.

Voordat tot gegevensuitwisseling wordt overgegaan, dienen het maken partijen daarover goede afspraken te maken. Afspraken over het doel van de samenwerking, de aansturing van het samenwerkingsverband en de hoofdlijnen van de gegevensuitwisseling worden vaak – zie ook § 2.

³⁴ Een voorbeeld daarvan is de samenwerking tussen het UWV, de SVB en de gemeenten bij de uitvoering van de Wet structuur uitbreidingsorganisatie werk en inkomens (Wet Suwi) enige andere wetten. Zie daarvoor art. 9 Wet Suwi.

³⁵ Zie in dit verband ook: A.J.C. de Moor-van Vugt, Gegevensuitwisseling door Toezichtbureaus: hoe vaak uitgevoerd in opdracht van het WODC, 2012, blz. 56.

2 - in een convenant vastgelegd. Afspraken over de gegevensuitwisseling worden dan meestal uitgewerkt in een informatie- of privacyprotocol. Daarbij is van belang een heldere beschrijving te geven van de inrichting van de gegevensuitwisseling: welke partijen wisselen welke gegevens in welk proces uit om tot welk resultaat of product te komen? Bij de inrichting daarvan moet uiteraard acht worden geslagen op de vorm en mate waarin hiervoor relevante regelgeving de gegevensuitwisseling toelaten.

Ten ondersteuning van het samenwerkingsverband wordt vaak een bureau in het overnemen van de feitelijke gegevensuitwisseling (registratie, analyse en rapportage) opgesteld of overgenomen. Afhankelijk van de gemaakte afspraken behoeft zijn organisatie vaak ook een informatiesysteem waarin de uitgewisselde gegevens worden verwerkt. Een heldere beschrijving van de inrichting van de gegevensuitwisseling is niet alleen nodig om die uitwisseling goed te laten verlopen, maar ook een randvoorwaarde voor het opzetten van een dergelijk informatiesysteem. Daarnaast wordt voorkomen dat een systeem wordt ontwikkeld dat nadat hand gegevens blijkt te verwerken op een wijze die niet strookt met de geldende regelgeving, en dat tegen wellicht hoge kosten moet worden aangepast.

2.6 Relevante andere ontwikkelingen

Bij deze verkenning is mede acht geslagen op verschillende ontwikkelingen die betrekking hebben op gegevensverwerking in het algemeen.

Een eerste ontwikkeling die hier wordt genoemd, betreft het onderzoek dat in het verleden naar gegevensuitwisseling door toezichhouders is verricht. In 2008 heeft een interdepartementale werkgroep herijking toezichtbevoegdheid onderzoekt wat de mogelijke juridische belemmeringen zijn voor de voortzetting en intensivering van de samenwerking tussen de rijksregering en welke mogelijkheden er zijn deze belemmeringen weg te nemen. De werkgroep kwam tot de conclusie dat een algemene wettelijke regeling voor de informatie-uitwisseling tussen inspecties rife en gelijk reguleer voor alle inspecties zou creëren, niet goed mogelijk en niet wenselijk is. De werkgroep voerde daartoe aan dat er immers sprake is van nogal uiteenlopende toezichthoudende organen, die gegevens van allerlei aard uitwisselen waarvoor diverse regimes gelden. Het zou volgens de werkgroep zeer de vraag zijn of het zou lukken deze regime in een uniforme, eenduidige regeling onder te brengen. Bovendien zou een algemeen geldende doelmotivering voor de overdracht van gegevens voor inspectiedoeleinden op problemen kunnen stuiten in relatie tot de eis uit artikel 6 van de Europese privacyrichtlijn dat het doel van de verwerking van persoonsgegevens welbepaald moet zijn.²⁶ Het toenmalige kabinet nam deze conclusie over.²⁷ Bij de behandeling van het kabinetsstandpunt maakte het advies van de Commissie Brouwer-Kort en de evaluatie van de Wbp is op aandringen van de Tweede Kamer toegevoegd de mogelijkheid van een dergelijke algemene regeling toch te bezien.²⁸ Het toenmalige kabinet heeft in dat verband gewezen op de mogelijkheid van een algemene wettelijke bepaling die inhoudt dat gegevens in het kader van een structurele samenwerking kunnen worden uitgewisseld, mits de afspraken tot samenwerking op een wettelijk voor te schrijven wijze zijn bekans gemaakt.²⁹ De toerekening van het kabinet heeft geleid tot een onderzoek in opdracht van het WODC naar gegevensuitwisseling door toezichthouders. Dat onderzoek heeft geleid tot een rapport waarin wordt aanbevolen om – mede ten behoeve van een vereenvoudiging en vereenvoudiging van de eis van doelbinding – de huidige Wbp om te vormen tot een brede kaderwet, eventueel met nadere uitwerking in externe regelgeving. Ook bevat het rapport aanbevelingen voor het gebruik van convenanten ten behoeve van structurele gegevensuitwisseling in publiekrechtelijke samenwerkingsverbanden.³⁰ Het kabinet heeft in reactie op dat rapport zich op het standpunt gesteld dat de herziening van de Europese regelgeving inzake de verwerking en bescherming van persoonsgegevens (de hierna

²⁶ Rapport van de werkgroep herijking toezichtbevoegdheid, 2008, § 4.2.2.

²⁷ Kamerstukken II 2008-2009, 31700 VI, nr. 70.

²⁸ Kamerstukken II 2009-2010, 31051, nr. 2, blz. 19.

²⁹ Kamerstukken II 2008-2009, 31700 VI, nr. 118, blz. 9.

³⁰ De Moor van Vugt, a.w., blz. xiv.

verkenning, voor zover zij al op een breder terrein dan fraudebestrijding betrekking heeft, in ieder geval niet het sociaal domein omvat waarop de drie decentralisaties zich afspelen.

Deze verkenning vertoont ook samenhang met het rapport "Dienstbaar en transparant" van het project 500-3. In dat rapport adviseert de stuurgroep SCO-3 een programma te starten voor het ontwikkelen van een kaderwet die de haantekenaarheid van de huidige privacywet- en regelgeving verbetert. De stuurgroep adviseert om dit traject af te stemmen met de ondernemende verkenning naar de mogelijkheden van een kaderwet voor de gegevensuitwisseling ten behoeve van de fraudebestrijding.¹⁷

Voor deze verkenning is ook relevant dat op dit moment in Brussel onderhandelingen plaatsvinden over voorstellen van de Europese Commissie voor een Algemene verordening gegevensbescherming¹⁸ en een Richtlijn gegevensbescherming opsporing en vervolging¹⁹. De beoogde verordening moet de Europese privacykultuur uit 1995²⁰ vervangen. Als verordening zal zij directe werking in Nederland hebben en tot gevolg hebben dat de Wet bescherming persoonsgegevens en bepalingen ter bescherming van persoonsgegevens in specifieke wetten overbodig worden dan wel aanpassing behoeven. De beoogde Richtlijn gegevensbescherming opsporing en vervolging zal geen directe werking hebben en moeten worden omgezet in nationale wetgeving. Als gevolg daarvan zullen de wet politiegereguleert en de Wet Justitiële en strafvorderlijke gegevens aanpassing behoeven. Beide voorstellen van de Europese Commissie hebben geen betrekking tot specifiek op gegevensuitwisseling in samenwerkingsverbanden betrekking hebben. Dat neemt niet weg dat bij de verdere voorbereiding van een evolutie kaderwet met de eindhandelingen over de komende verandering en richtlijn rekening moet worden gehouden. In § 4.15 wordt daaraan al een eerste beschouwing gewijd.

Een andere ontwikkeling waarop de deze verkenning wordt gebaseerd, is de evaluatie van de Wet op de persoonsgegevens (Wopg) en de wet Justitiële en strafvorderlijke gegevens (Jstvg). Deze evaluatie heeft geleid tot een brief van de Minister van Veiligheid en Justitie van 23 juni 2014 aan de Tweede Kamer, waarin hij een perspectief schetst op de toekomstige omgang met politieke, justitiële en strafvorderlijke gegevens. In de brief wordt de conclusie getrokken dat deze wetten moeten worden gemoderniseerd, waarbij de verschillende regimes die van toepassing zijn op politieke, justitiële en strafvorderlijke gegevens, moeten worden gelykwaardigend, het gebruik van gegevens en niet de benaamelijkheid het uitgangspunt van de nieuwe regeling moet zijn en het toezicht op het gebruik en de verstreking van gegevens moet worden versterkt. Deze modernisering van de regelgeving en de uitvoering is volgens de Minister ambitieus en zal de nodige tijd kosten.²¹ Met betrekking tot samenwerkingverbanden merkt hij in de brief op dat in verschillende verbanden, waarin ook politieke, justitiële en strafvorderlijke gegevens worden uitgewisseld, in toenemende mate met convenanten en privacyprotocollen wordt gewerkt. Hij zegt daarbij dat hij deze werkwijze krachtig verder zal bevorderen.²² Bij de voorbereiding van een eventuele kaderwet gegevensuitwisseling zal met dit moderniseringstraject rekening moeten worden gehouden en zal ook het belang van convenanten en privacyprotocollen moeten worden meegenomen.

Tot slot valt nog te wijzen op de verkenning naar een aantal scenario's om de informatiepositie van bestuursorganen bij de toepassing van de Wet bevordering integriteitsbeoordelingen openbaar

¹⁷ Eindrapport project 500-3 "Versterkte effectieve inzet van bestuursorganisaties", mei 2014, blz. 63.

¹⁸ <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2014/05/27/de-badkegels-voor-de-gedecentraliseerde-overheid-dienstbaar-en-transparant.html>.

¹⁹ Zie voorstel van de Europese Commissie van 25 januari 2012, COM(2012)11.

²⁰ Zie voorstel van de Europese Commissie van 25 januari 2012, COM(2012)10.

²¹ Rijkswijs 35/46/EG over het Europese performant en de Raad van 24 oktober 1995, betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van de gegevens, Pb L 281.

²² Kamerstukken II 2013-2014, 33842, nr. 2, blz. 1-2.

²³ Icm. blz. 8.

bestuur (Wet Bibob) te verbeteren. Deze verkenning is toegevoegd tijdens de behandeling van het voorstel van de Flexibilisatie- en uitbreidingswet Bibob in de Eerste Kamer.⁵³ Een van deze scenario's gaat uit van een versterking van de rol van de RIECs bij de uitvoering van de Wet Bibob. Dit scenario kan relevant zijn bij de verdere uitwerking van een eventuele kadewet. Uiteraard hangt de relevantie daarvan ook af van het kabinetstandpunt dat naar aanleiding van de verkenning zal worden uitgebracht.

⁵³ Kamerstukken I 2012-2013, 33676 H, blz. 3.

3. Knooppunten

3.1 Inleiding

In § 1 van deze verlening is naar voren gebracht dat de werkgroep haar verkenning van knooppunten bij de gegevensuitwisseling in samenwerkingsverbanden gebaseerd heeft op bestaande ervaringen, een brainstormsessie met experts, de bestudering van een aantal casussen en van literatuur, officiële publicaties en websites. De werkgroep merkt in dit verband op dat zij weliswaar primair aandacht heeft besteed aan gegevensuitwisseling ten behoeve van de fraudebestrijding, maar zich niet tot de tevoren heeft beperkt. Dat heeft twee redenen. De eerste is dat bestaande samenwerkingsverbanden zich maar zeer ten dele met uiteenlopende fraudebestrijding bezighouden (zie § 2.3). De tweede reden is dat knooppunten bij gegevensuitwisseling ten behoeve van andere doeleinden evenzeer van belang kunnen zijn, zeker in het geval voor een kadernet met een bredere reikwijdte dan alleen fraudebestrijding zou worden gekozen (zie nader § 4.2).

3.2 Verschillende wettelijke kaders

Gegevensverwerking heeft altijd een centrale plaats gehad bij de interne werkprocessen van veel overheidsorganisaties en in de verhouding overheid-burger. Gegevensverwerking is immers een belangrijk onderdeel van en afleesbaar aan de opgedragen taak van praktisch iedere overheidsinstelling. Iedere overheidsinstelling heeft zijn eigen taak en omdert een eigen gegevenshuishouding uit bij de uitvoering van die taak. Zolang de gegevensverwerking plaats vindt binnen het kader van de eigen taak, wordt de bevoegdheid tot dergelijke gegevensverwerking gevast op te gaan in de algemene taakomschrijving nu die dienstig is aan die taakinvulling en daarvoor noodzakelijk is. In deze situatie is het opnemen van bepalingen rond gegevensverwerking bij het opnemen van informatieverplichtingen voor burgers die met de betrokken overheidsinstelling te maken hebben. Ook is meestal sprake van een gehoudingsbepaling voor de betrokken overheidsdienst met de burger of het bedrijf erop kan voortvallen dat zijn gegevens in veilige handen zijn (zie ook § 3.5). (Barmoe is sprake van geïsoleerde, gesloten gegevenshuishoudingen per domein of zelfs per overheidsdienst.

Van wanneer sprake is van een behoefte bij de ene overheidsdienst aan gegevens waarover een andere overheidsdienst beschikt en dus aan het uitwisselen van gegevens tussen overheidsdiensten, ontstaat de noodzaak aan dergelijke uitwisseling van gegevens juridisch in te kaderen wat van een adequate juridische grondslag te voorzien. De bevoegdheid gegevens uit te wisselen met een ander valt in beginsel buiten de taakomschrijving van de betrokken overheidsdienst, zoals die daar de wetgever in de vorm van taken en bevoegdheden aan die dienst is gegeven. De leenverval van gegevens te deken met een andere overheidsdienst dient derhalve expliciet in het leven te worden geroepen. Inmiddels is er dan ook een groot aantal bepalingen tot stand gekomen op grond waarvan de ene overheidsdienst gegevens verstrekt aan de andere overheidsdienst. Voor ieder rechtsgebied dan wel iedere overheidsinstelling is dit overigens op eigen wijze geregeld, passend binnen de regelgeving die geldt voor dat rechtsgebied of die instelling.

Anders gezegd: regelingen met betrekking tot verwerking van gegevens hebben uit hun aard prima een "verticaal" karakter: zij regelen de gegevensverwerking binnen de desbetreffende sector. Gegevensuitwisseling in samenwerkingsverbanden heeft echter een "horizontaal" karakter: zij heeft betrekking op gegevensverwerking tussen verschillende sectoren. Voor zover sectorstapsgewijze, regelgeving, bepalingen betreffen over verstrekking van de dien, hebben deze bovendien meestal betrekking op bilaterale verstrekking en niet op verstrekking aan meerdere partijen tegelijk die in een samenwerkingsverband opereren.¹⁴

¹⁴ Uitzonderingen hierop zijn o.a. te vinden in de artikel 30 Wet politiegegevens, artikel 38, tweede lid, onder d, Wet Sibob en artikel 64 Wet Sawi. Verder bevat ook de Wbo in artikel 22, derde lid, een specifieke bepaling met betrekking tot verstrekking van strafrechtelijke gegevens door en ten behoeve van samenwerkingsverbanden.

Gelet op de specifieke context waarin overheidsorganisaties moeten opereren, is de systematiek van de bestaande wetgeving voor iedere individuele organisatie wellicht nog te begrijpen en te begrijpen. Deze systematiek van de wetgeving is voor samenwerkingsverbanden echter wel erg complex. Zo complex dat het ook voor deskundigen lastig is door de bomen het bos te zien. Het gaat dan nog niet eens zozeer om het grote aantal normen dat in acht moet worden genomen, maar meer nog om het feit dat die normen in relatie tot samenwerkingsverbanden in bepaalde gevallen niet goed te duiden zijn. Het kan dan bijvoorbeeld gaan om de vraag of en, zo ja, in hoeverre bepalingen die bilaterale verstrekking mogelijk maken, ook kunnen worden nuttig voor gegevensuitwisseling binnen het samenwerkingsverband.³⁵ De slagkracht van de samenwerking kan, zodoende, tevergeefs gaan door de veelheid aan interpretaties van de bestaande, veelal sectorale regels en door wettelijke samenkomsten. Er bestaat onduidelijkheid over essentieel vragen als die of gegevensuitwisseling wel is geoorloofd in een concrete situatie en wat daarbij precieze randvoorwaarden zijn. Daardoor is in de praktijk gegevensuitwisseling niet steeds vanzelfsprekend, waar zij dat wel zou kunnen of zelfs moeten zijn. En dit belemmert een adequate aanpak.

De introductie van modelbepalingen over gegevensverstrekking (zie § 2.8) heeft in deze situatie opvoerende verandering kunnen brengen. Deze modelbepalingen zijn bestemd voor situaties waarin sprake is van bilaterale dan wel multilaterale gegevensuitwisseling door in de wet bij naam te noemen partijen. Dit impliceert dat voor elk samenwerkingsverband een afzonderlijke wettelijke regel nu moet worden gemaakt. De praktijk heeft evenwel behoefte aan een wettelijk kader waarbinnen meerdere samenwerkingsverbanden voor verschillende specifieke doelen kunnen worden opgezet. Zo in kader zou voldoende ruimte moeten bieden voor maatwerk voor ieder afzonderlijk samenwerkingsverband. Aldus zou op een snellere wijze kunnen worden ingespeeld op de behoefte aan samenwerkingsverbanden dan met de modelbepalingen mogelijk is. Daar komt bij dat deze modelbepalingen niet een oplossing bieden voor alle knelpunten die hierna nog aan de orde komen.

Meer in het bijzonder bij verstrekking van strektrechtelijke gegevens aan samenwerkingsverbanden is bij de evaluatie van de Wpg en de Wvsg gebleken dat elk jaarlijks verschillende knelpunten voortvloeien. De belangrijkste knelpunten die in dit verband bij de evaluatie van de Wpg zijn genoemd, zijn onduidelijkheid over wettelijke verstrekking begrip, wat je mag verstrekken, de soms tegenstrijdige wettelijke kader, de positie en positie van overeenkomsten en hoe het staat met de informatieprivacy nadat verstrekt is.³⁶ De evaluatie van de Wvsg laat zien dat het bij samenwerkingsverbanden zelfs voor goed geïnformeerde betrokkenen vaak niet duidelijk is of gegevens nu via de Wpg, de Wvsg of zelfs via de Wbp moeten worden verwerkt. Daar komt bij dat, als gegevens onder de werking van zowel de Wvsg als de Wpg (lijken te) vallen, men voor verstrekking van gegevens aan samenwerkingsverbanden voor het ruimere regime van de Wpg kiest boven dat van de Wvsg.³⁷

3.2 Rechvaardigingsgronden

Uit de inventarisatie van de werkgroep volgt dat een knelpunt voor de gegevensuitwisseling binnen samenwerkingsverbanden onder meer is gelegen in de rechtvaardigingsgronden die de Wbp voor de verwerking van persoonsgegevens bevat.

³⁵ Zo merkte de Raad van State in zijn advies over het voorstel tot wijziging van de Wet op het financieel toezicht en enige andere wetten (Wetwijziging financieel toezicht 2014) op het toezicht houden toezichtvertrouwelijke informatie slechts mogen verstrekken in één-op-één relatie met in de wet genoemde partijen. Dit eis stond volgens de Raad in de weg aan haakgen met het voorstel wordt beoogd, namelijk het mogelijk maken van informatie-uitwisseling binnen het REC. De regering heeft de desbetreffende bepaling vervolgens aangepast dat die informatie slechts mag worden verstrekt als dat voor de ontvangende partij dienstig is voor de uitvoering van haar wettelijke taak (Staten-Generaal 2013-2014, 33621, nr. 4, 15-19).

³⁶ WODC, Glazen privacy, Knelpuntenonderzoek uitvoering Wet politiegegevens (Wvpg), 2013, blz. 49.

³⁷ WODC, Onderzoekrapport Evaluatie Wet justitie en strafrechtelijke gegevens, 2013, blz. 84, 91.

Persoonsgegevens mogen ingevolge artikel 7 Wvbp alleen worden verzameld voor een bepaalde uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Wanneer sprake is van "gerechtvaardigde doeleinden", valt af te leiden uit artikel 8 Wvbp. Dit artikel bepaalt in een limitatieve opsomming van gevallen wanneer de verwerking – dus ook het verzamelen – van persoonsgegevens gerechtvaardigd is. Dat is het geval wanneer de betrokkene tevens de volgende toestemming heeft verleend (a) of wanneer de verwerking noodzakelijk is ter uitvoering van een overeenkomst (b), ter nakoming van een wettelijke verplichting (c), ter wijfening van een vitiaal belang van de betrokkene (d), voor de goede vervulling van een publiekrechtelijke taak door een overheidsorgaan (e) of ter bescherming van het gerechtvaardigde belang van de verantwoordelijke, tenzij het belang of de fundamentele vrijheid en vrijheid van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleren (f).

Voor gegevensuitwisseling in samenwerkingsverbanden op het terrein van de fraudebestrijding geldt dat deze uiteraard niet afhankelijk kan zijn van toestemming van betrokkenen. Fraudeurs hebben er eerder belang bij dat hun gegevens niet worden uitgewisseld, als daardoor de kans groter wordt dat zij gepakt worden. Dat de gegevensuitwisseling noodzakelijk is ter uitvoering van een overeenkomst, zal zich bij dergelijke samenwerkingsverbanden ook niet voordoen. Op een wettelijke verplichting tot gegevensverstrekking kan veelal ook geen beroep worden gedaan.²⁶ Daarbij moet worden bedacht dat een eventuele lovenswaardigheid van gegevensverstrekking nog geen wettelijke verplichting impliceert. Ook van een vitiaal belang van betrokkenen zal geen sprake zijn. Zo resteren de gronden e en f.

Van deze twee gronden is voor samenwerkingsverbanden de grond, genoemd onder e, het meest relevant. Zij legitimeert de verstrekking van persoonsgegevens door een bestuursorgaan aan een ander bestuursorgaan, als deze noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het verstrekkende orgaan dan wel het orgaan waaraan de gegevens worden verstrekt. Zo'n verstrekking kan ook plaatsvinden in het kader van een samenwerkingsverband, die moet een multilaterale verstrekking in zo'n verband voor ieder van de afzonderlijke deelnemers kunnen worden gerechtvaardigd. Dat vindt u oorspronkelijk uit de formulering van deze rechtvaardigingsgrond voort, waarin een samenwerkingsverband als zodanig immers niet voorkomt. Hetzelfde geldt voor bepalingen uit sectorale wetten die bilaterale verstandingen mogelijk maken (de noot § 3.4). Een ander impliciet dat voor gegevensverstrekking aan alle deelnemers van een samenwerkingsverband tegelijk of aan een ondersteunend bureau, als dat voor een effectief functioneren van het verband als geheel ten goede zou kunnen vaak zeer adequate grondslag bestaat. Een kaderwet zou deze belemmering kunnen wegnemen.

Ken er dus het vinden van een rechtvaardigingsgrond voor gegevensuitwisseling tussen bestuursorganen in een samenwerkingsverband al problemen opleveren, het ligt nog een slag lastiger, als aan een samenwerkingsverband ook private partijen – zie § 2.3 – deelnemen. Tenzij een sectorale wet voor dat geval gegevensverstrekking mogelijk maakt, zal de verstrekking uitlopend kunnen worden gebaseerd op onderaanmerking grond f. Een beroep op die grond brengt echter mee dat steeds een afwijking voor het individuele geval moet worden gemaakt. Dit belemmert een structurele uitwisseling van gegevens. Als een eventuele kaderwet voor gegevensuitwisseling bij fraudebestrijding ook op uitwisseling met private partijen betrekking zou hebben, zou deze kaderwet de belemmering kunnen wegnemen.

3.4. Verenigbaarheidstoets

Aan de rechtvaardigingsgronden van artikel 6 wordt artikel 9 Wvbp de algemene eis toe dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de

²⁶ Een uitzondering hierop wordt onder meer gevormd door artikel 61, derde lid, Wet Suwi, waarin de deelnemers aan een samenwerkingsverband worden verplicht elkaar te noodzakelijke gegevens te verstrekken. Andere voorbeelden zijn te vinden in artikel 29a Arbeidsonderzoekswet, artikel 8:2 Arbeidstijdenwet en artikel 18a Wet minimumloon en minimumvakantiebijslag.

doeleinden waarvoor ze zijn verkregen (principe van doelbinding). Het doel van de gegevensuitwisseling in een samenwerkingsverband is in het algemeen een ander dan het doel waarvoor een deelnemer aan het verband de gegevens oorspronkelijk heeft verkregen. Dit brengt mee dat voor deze gegevensuitwisseling moet worden geconstateerd dat niet verkeerbaar is met de doeleinden waarvoor de gegevens oorspronkelijk zijn verkregen.⁴⁰

De uitvoering van de verenigbaarheidsstoets wordt in de praktijk als een lastige hindernis ervaren en zet om die reden bij tijd en wijle een juridische rem op de bereidheid om gegevens uit te wisselen.⁴¹ Weliswaar geeft artikel 44 Wvbo voor bepaalde doeleinden de mogelijkheid om af te wijken van het principe van doelbinding, maar uit de zeer casuïstische jurisprudentie over dit artikel kan worden afgeleid dat toepassing slechts is weggelegd voor uitzonderlijke gevallen en niet gebruikt kan worden als een grondslag voor permanente of anderszins structurele overdracht van gegevens.⁴² Artikel 43 biedt daarom voor samenwerkingverbanden geen uitkomst.

Lus van deze overweging dient aan het beginsel van doelbinding en daarmee aan de verenigbaarheidsstoets ook grote waarde te worden toegekend. Aan beide kan ook in het licht van de Europese privacyregulering en de Nederlandse wetgeving geen afbreuk worden gedaan. Het is dan ook ondenkbaar dat een eventuele kadewet de verenigbaarheidsstoets terzijde zou kunnen schuiven. Overigens lijkt men in de praktijk soms een te kranachtige houding bij de uitvoering van de verenigbaarheidsstoets in te nemen. Dat kan tot het achterwege laten van gegevensuitwisseling leiden, waar een goed uitgevoerde verenigbaarheidsstoets wel ruimte voor zou kunnen geven. Waar op dit punt wetgeving geen uitkomst kan bieden, zou voorlichting dat wel kunnen.

Niet zonder belang is dat er mogelijk voorondering komt in de omstandigheid dat de Europese privacyregulering weinig tot geen ruimte laat voor verdere verwerking van persoonsgegevens voor een doel dat niet verenigbaar is met het doel waarvoor zij zijn verzameld. Ingevolge artikel 6, vierde lid, van het voorstel voor een Algemene verordening gegevensbescherming is ingeval van onverenigbare doelen verdere verwerking niet mogelijk, mits deze verwerking haar rechtsgrondslag heeft in ten minste één van de gronden die dat artikel in het eerste lid, onder a tot en met e, noemt. De gronden die in relatie tot samenwerkingsverbanden relevant zijn, zijn de gronden c en e. Het gaat om het geval dat de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting van de voor de verwerking verantwoordelijke (grond c) en het geval dat de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang (grond e). Indien een verenigbaarheidsstoets tot de conclusie leidt dat van onverenigbare doelen sprake is, zal verdere verwerking onder de Algemene verordening gegevensbescherming toch mogelijk zijn, als daarvoor één van genoemde gronden kan worden aangevoerd.⁴³

3.5 Geheimhoudingsplicht

De mate waarin gegevens binnen samenwerkingsverbanden kunnen worden uitgewisseld, wordt thans ook sterk bepaald door de bestaande geheimhoudingsplichten. Deze plichten zijn ingegeven met het oog op verschillende belangen. Daarbij kan het erde meer gaan om bescherming van

⁴⁰ Voor het toetsen of er sprake is van verenigbaar gebruik draagt het tweede lid van artikel 9 Wvbo de volgende vijf criteria aan:

1. de veruingschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen;
2. de aard van de gegevens;
3. de gevolgen van de beoogde verwerking voor de betrokkene;
4. de wijze waarop de gegevens zijn verkregen; en
5. de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

⁴¹ Zie in dit verband ook: De Meuw van Zagt, i.w., blz. 35-39.

⁴² Vgl. kametsluden II 2008-2009, 29911, nr. 73, blz. 8. Zie ook HR 31 januari 2012 (JWB: BT1216, pag. 19) en de leidraad afstemmen van wetgeving op de Wet Bescherming persoonsgegevens, 2000, Nr. 60.

⁴³ Zie over de verhouding tot de regelgeving van de EU ook § 4.15.

private belangen (persoonlijke levenssfeer, bedrijfsgeheimen), bescherming van publieke belangen (veiligheid van de staat), bescherming van de bijzondere positie van bepaalde instellingen (onerschendbaarheid Koning) en de zorg voor de goede werking van het openbaar bestuur (mogelijkheid van intern advies, geheimhouding van een bepaalde werkwijze, het belang van inspectie, toezicht en controle door bestuursorganen).¹³

Bij gegevensuitwisseling in samenwerkingsverbanden zijn de bescherming van private belangen en de zorg voor de goede werking van het openbaar bestuur het belang i.k.a. de bescherming van publieke belangen is overigens niet alleen aan belang van burgers en bedrijven, maar eveneens van de overheid zelf. De belangen lopen parallel, daar waar bescherming bijdraagt aan het beeld van de betrouwbare overheid. Burgers en bedrijven zullen immers eerder geneigd zijn gegevens af te staan aan de overheid als zij erop kunnen vertrouwen dat deze goed worden bewaakt en niet zomaar aan de openbaarheid of aan derden worden prijsgegeven. In die zin dient de bescherming van private belangen tevens het organisatiebelang en de goede werking van het openbaar bestuur. Anderzijds kan de bescherming van private belangen juist de goede werking van het openbaar bestuur belemmeren, als overheidsinstellingen zich onterfing beroepen op de geheimhoudingsplicht en om die reden niet tot uitwisseling van gegevens overgaan. Daarbij moet worden bedacht dat geheimhoudingsplichten in de regel in het leven zijn geroepen met het oog op een bepaald deelbelang binnen het openbaar bestuur, zoals de correcte belastingheffing of de bewaking van de soliditeit van banken. De geheimhoudingsplicht heeft aldus meer varianten.¹⁴

Een algemene geheimhoudingsplicht is opgenomen in de Algemene wet bestuursrecht (Awb). Artikel 2:5 Awb bepaalt dat een loder die betrokken is bij de uitvoering van de taak van een bestuursorgaan en daarbij de beschikking krijgt over gegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden, verplicht is tot geheimhouding van die gegevens. Deze geheimhoudingsplicht is aanvullend: zij geldt niet voor wie reeds uit hoofde van aard, beroep of wettelijk voorschrift ter zake van die gegevens een geheimhoudingsplicht geldt. Verder wijkt deze plicht voor een wettelijk voorschrift dat tot mededeling verplicht, tenzij ook uit de taakuitoefening een noodzaak tot mededeling kan voortvloeien. Tot de gegevens met een vertrouwelijk karakter kunnen nuar meer bedrijfs- en fabricagegegevens en gegevens die betrekking hebben op de persoonlijke levenssfeer, worden gerekend.¹⁵

Een algemene geheimhoudingsbepaling voor ambtenaren is opgenomen in artikel 125a, derde lid, van de Ambtenarenwet. Daarin is bepaald dat de ambtenaar verplicht is tot geheimhouding van hetgeen hem in verband met zijn functie ter kennis is gekomen, voor zover die verplichting uit de aard der zaak volgt.

Een algemene geheimhoudingsplicht met betrekking tot persoonsgegevens is vastgelegd in artikel 9, vierde lid, Wv. Daarin wordt bepaald dat de verwerking van persoonsgegevens achterwege blijft voor zover een geheimhoudingsplicht uit hoofde van aard, beroep of wettelijk voorschrift daaraan in de weg staat.

Naast deze algemene geheimhoudingsplichten bestaan ook tal van bijzondere geheimhoudingsbepalingen. Voor samenwerkingsverbanden op het terrein van de fraudebestrijding zijn vooral de geheimhoudingsbepalingen in de volgende wetten relevant: de Wvfg (art. 52), de Wvfg (art. 7), de Algemene wet inzake rijksbelastingen (Aw, art. 67), de Wet op het financieel toezicht (Wft, art. 1:89 e.v.), de Wet centrale en rechtspersonen (Wv, art. 5, derde lid), de Wet bevordering integratievoorzieningen door het openbaar bestuur (Wet B-bol, art. 28) en de Wet Surin (art. 74). Deze wetten bevatten ook bepalingen die het mogelijk maken de

¹³ J.A.M. Klagenberg, A. Logemann en S.A.J. Munnike "Geheimhouding als juridische kwaliteitsbeoordeling van primaire besluitvorming" in: M. Herweijer, A.T. Marstolle, F.M. Noordam, H.B. Winter (red.), Alles in één keer goed. Juridische kwaliteit van bestuurlijke besluitvorming, 2005, blz. 178-179.

¹⁴ De Moor-van Vugt, a.v.o. blz. 31.

¹⁵ Kamerstukken II 1988-1989, 21221, nr. 3 blz. 57.

geheimhoudingsplicht te doorbreken, maar daaraan zijn dan vaak wel de nodige voorwaarden verbonden.

Zo kent de Wvg in de artikelen 6a en 29f het College van procureurs-generaal de mogelijkheid om OM, voor zover dat nodig is met het oog op een zwaarwegend algemeen belang, justitiële, repressieve of strafrechtelijke gegevens aan derden te verstrekken ten behoeve van specifiek omschreven doeleinden. Artikel 6a ziet daarbij op de justitiële documentatie waarover het OM de beschikking heeft gekregen in het kader van de behandeling van een strafzaak.⁴⁶ Het biedt dus geen grondslag om het OM justitiële gegevens te vragen voorover het OM zelf niet beschikt. Daarvoor zal, zo nodig, op grond van artikel 9 Wvg een voorziening kunnen worden getroffen in het Besluit justitie en strafrechtelijke gegevens (Bjsg). Voor zover het OM wel over justitiële en strafrechtelijke gegevens beschikt, heeft het OM in zijn beleidsregels bepaald dat, als aan bepaalde voorwaarden is voldaan, verstrekking ten behoeve van samenwerkingsverbanden mogelijk is.⁴⁷

Ook de Apg biedt de mogelijkheid om politiegegevens aan derden te verstrekken. Op grond van artikel 18 Wvg kan in het besluit politiegegevens (Bpg) worden verspreid aan welke instelling voor welke doeleinden politiegegevens kunnen worden verstrekt. Artikel 18 kent daarnaast aan de Minister van Veiligheid en Justitie de bevoegdheid toe in bijzondere gevallen toewijzing of opdracht te geven tot het verstrekken van daarbij door hem te omschrijven politiegegevens, voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang.⁴⁸ Verder biedt artikel 20 Wvg de kans dat de mogelijkheid in overeenstemming met het bevoegd gezag bepaalde politiegegevens aan samenwerkingsverbanden te verstrekken, voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang en voor bepaald doeleinden, zoals is het voorkomen of opsporen van strafbare feiten.

Een algemeen mogelijkheid om de geheimhoudingsplicht van artikel 6v Awv te doorbreken ten behoeve van de gegevenswisseling in samenwerkingsverbanden, ligt opgesloten in artikel 43c, eerste lid, onder m, van de Uitvoeringsregeling Awv. Ingevolge die bepaling kunnen gegevens worden verstrekt aan bepaalde bestuursorganen, voor zover deze gegevens nodig zijn om de samenwerking in het kader van de integrale aanpak van handhaving van overheidsregelingen efficiënt en effectief te laten verlopen en een covenant is gesloten met deze bestuursorganen.

De geheimhoudingsplicht die op grond van de Wv voor DNB en de AFM geldt, kan op grond van artikel 1:93 van die wet worden doorbroken ten behoeve van onder meer de Belastingdienst, de FIOD, de politie, het Bureau Financieel toezicht, de Financiële instellingen behoud en het OM, voor zover de gegevens of inlichtingen dienstig zijn voor de uitvoering van hun wettelijke taken. Dat zou in beginsel ook kunnen gelden voor samenwerkingsverbanden waarin één of meer van deze partijen deelnemen.

Op grond van artikel 5, derde lid, Wv kan de daarin vastgelegde geheimhoudingsplicht worden doorbroken door het AMvB toe te staan dat een organisatie die krachtens die wet de beschikking krijgt over gegevens een bevoegdheid tot een derde die zijn toegeleid in een melding van een verhoogd risico van misbruik van een rechtspersoon, mededeling van dergelijke gegevens aan een andere organisatie doet. Op basis daarvan bepaalt artikel 5b van het Besluit controle rechtspersonen (Ber) dat mededeling van dergelijke gegevens in een aantal casus genoemde gevallen is toegestaan. Het gaat onder meer om verstrekking voor de politie aan het openbaar

⁴⁶ Aanwijzing wet justitiële en strafrechtelijke gegevens, blz. 15-16.

⁴⁷ Het is ang van het samenwerkingsverband of of aan het samenwerkingsverband of (welke) partij aan de afzonderlijke deelnemers wordt verstrekt. Het samenwerkingsverband wordt dan aangemerkt als overige ontvanger als bedoeld in de Aanwijzing wet justitiële en strafrechtelijke gegevens.

⁴⁸ Van deze mogelijkheid is gebruik gemaakt om politiegeregten te verstrekken aan de RIEG ten behoeve van de aan integrale casusanalyse. Zie Wpg-mechanischbesluit, RIEG's werkproces integrale OM-analyse (Ber, 2013, nr. 67:1).

in historische, de RIJL's, de Koninklijke marechaussee, de Belastingdienst, de bijzondere opsporingsdiensten en de AIVD.

Ingevolge artikel 26, tweede lid, Wet Bibob mag het bestuursorgaan dat of de rechtspersoon met een overheidstaak die ten Bibob advies ontvangt, de daarin opgenomen gegevens desgevraagd aan een partij in die toelating gevraagd de partijen en organisaties. Daartoe behoren onder meer ook andere deelnemers aan een RIEC, voorzover de gegevens noodzakelijk zijn voor het ondersteunen van het bestuursorgaan of de rechtspersoon met een overheidstaak bij het toepassen van de Wet Bibob.

De Wet Suwi kent naast de verschillende mogelijkheden tot bilaterale verstrekking in het Besluit Suwi, in artikel 64 de mogelijkheid gegevens te verstrekken aan samenwerkingsverbanden op een aantal terreinen van fraudebestrijding. Zodra partijen tot deelname aan een samenwerkingsverband hebben besloten, zijn zij ingevolge het derde lid van artikel 64 verplicht de noodzakelijke gegevens aan de andere partijen van het samenwerkingsverband te verstrekken.

Wat al deze mogelijkheden gemeen hebben, is dat zij weliswaar voor gegevensverstrekking aan samenwerkingsverbanden in verschillende mate enige ruimte geven, maar in de praktijk toch nog wel de nodige drempels opleveren. Zo geeft artikel 8a Wvgb toegang tot maar een deel van de justitiële gegevens. Verder lijkt de toelating aan het criterium "zwaarwegend algemeen belang" bij de politie tot een zekere schroom te leiden om de mogelijkheden van artikel 20 Wvg te benutten. Het alternatief is gebruik maken van de mogelijkheid die artikel 9 Wvg en 18 Wvg bieden om de verstrekking van gegevens aan samenwerkingsverbanden te regelen in het Bijg, respectievelijk Epg. De aard van die mogelijkheden brengt evenwel mee dat dit een regeling vergt voor ieder afzonderlijk samenwerkingsverband. Artikel 43c, eerste lid, onder m, van de Uitvoeringsregeling Part lid, op het eerste gezicht veel ruimte voor verstrekking van belastingsgegevens aan bepaalde bestuursorganen, maar staat in de praktijk op haar eende terughoudendheid om deze ruimte te benutten, met name in gevallen waarin de doelestelling van een samenwerkingsverband wel om algemeen is geformuleerd. Met de invoering van het huidige artikel 67 AWR in 2008 is als zijn neergezet dat nieuwe gevallen die in de uitvoeringsregeling werden opgenomen zoveel mogelijk worden beperkt en dat er maar wordt gestreeft om gegevensverstrekking zoveel mogelijk zij wetmatig, voor advies te gaan regelen.⁶⁹ Ingeval van samenwerkingsverbanden zou dit overwel kunnen betekenen dat voor ieder verband opart een wetelijke voorziening moet worden getroffen. Het lijkt inmiddels wel ruimte te bestaan voor verstrekking van gegevens door de Belastingdienst aan het OM, zonder dat daarvoor een verandering van het OM op grond van artikel 226nd Wetboek van Strafrecht (WvS) nodig is.⁷⁰ Die ruimte is echter nog niet bevestigd door de Hoge Raad.⁷¹ De mogelijkheden om op grond van de WvS gegevens naar andere partijen te verstrekken, is vanwege het wettelijke karakter van de informatievergaringen van financiële ondernemingen aan de toezichthouders aan strenge voorwaarden verboden.⁷² De Wet Suwi biedt een goede basis voor gegevensuitwisseling, maar doet dat niet voor de vermen van fraudebestrijding, laat staan voor andere doeleinden op het terrein van rechtshandhaving en criminaliteitsbestrijding. Tot slot valt erop te wijzen dat, voor zover een bepaalde wet al verstrekking van gegevens aan derden mogelijk maakt, deze mogelijkheden niet veelal beperken tot andere partijen binnen de overheid. De ruimte voor verstrekking aan private partijen is beperkt.

⁶⁹ De Moor-van Vugt, a.w. 33.

⁷⁰ Zie Hof Arnhem-Leeuwarden 8-11-2013, ECLI:NL:GHARL:2013:6476. In dit arrest heeft het Hof uitgesproken dat verstrekking van gegevens door de belastingdienst aan het OM zonder vordering mogelijk is, voor zover dit zijn basis vindt in een convenant tussen betrokken partijen. Tenzij het convenant dat zou uitsluiten, is verstrekking ook mogelijk in het geval dat de persoon om wens gegevens het gaat, als verdachte wordt aangemerkt. Daarvoor doet volgens het Hof niet af dat in dit geval ook toepassing had kunnen worden gegeven aan de regeling van artikel 226nd WvS. Zie in dit verband ook § 3.6.

⁷¹ Een cassatieberoep dat tegen de in de vorige voetnoot genoemde uitspraak van het Hof Arnhem-Leeuwarden was ingesteld, is inmiddels ingetrokken.

⁷² De Moor-van Vugt, a.w. 33-34.

Wat zich hier voordoet, is dat, zoals ook hiervoor al is gesigneerd, de verschillende mogelijkheden tot verstrekking van gegevens aan andere partijen hoofdzakelijk zijn gekwalificeerd vanuit het perspectief van de verschillende sectoren en niet met het oog op een overkoepelend globaal belang van samenwerkingsverbanden. De geheimhoudingsbepalingen in de sectorwetten gaan voor verstrekking aan dergeïjke verbanden uit van "nee, tenzij". Een kaderwet zou die paradigma kunnen doorbreken naar "ja, tenzij". Het "nee, tenzij" doet in de praktijk meer dan "de discussie vooral gaat over wat mag en wat niet mag en daarmee primair een juridische discussie is. De kanteeling naar "ja, tenzij" zal meebrengen dat de discussie een meer beleidsmatig karakter krijgt. Zij zal zich beperken tot de vraag "Wanneer wij met elkaar samenwerken en de desornte hoofdzakelijke gegevens uitwisselen en welke gegevens moeten wij eventueel daarvan te moeten uitzonderen?".

Een en ander heeft niet tot doel de betekenis van geheimhoudingsbepalingen als zodanig ter discussie te stellen. Integendeel, geheimhoudingsbepalingen dienen, zoals aan het begin van deze paragraaf naar voren is gebracht, zeer legitieme belangen. Dit impliceert ook dat naar de mate waarin deze belangen meer gewicht hebben, de prudentie des te groter dient te zijn bij het besluiten van de rijksoverheid een eventuele lidmaat zou bladen om in het afdoende gevolg van een samenwerkingsverband gegevens te verstrekken die in andere gevallen onder de werking van een geheimhoudingsplicht (blijven) vallen. Deze belangen kunnen zelfs een zodanig gewicht hebben dat een kaderwet de werking van geheimhoudingsbepalingen met betrekking tot bepaalde categorieën van gegevens overkort in sterk zou moeten laten. Dat geldt in het bijzonder ten aanzien van bepaalde categorieën van bijzondere persoonsgegevens (zie hiervoor § 2.4). Hoe dit in een kaderwet zou kunnen worden uitgewerkt, komt in § 4.4 aan de orde.

3.6 Gegevensverwijping door opsporingsdiensten en OM

Voor het bestuursrechtelijke en het strafrechtelijke domein gelden verschillende wettelijke regimes. Dit heeft verband met het feit dat ten aanzien van personen die verdachte worden van een strafbaar feit, al naar gelang de aard en aard van het feit, verdergaande bevoegdheden kunnen worden ingezet en aan deze personen zwaardere sancties kunnen worden opgelegd dan in het bestuursrecht mogelijk is. Daar staat tegenover dat voor verdachten op grond van internationale verdragen ook meer waarborgen gelden.

Het verschil in wettelijke regimes voor beide domeinen neemt niet weg dat bestuursrechtelijke handhaving, controle en toezicht in de praktijk kunnen overgaan in opsporing en vervolging zonder dat deze overgang altijd duidelijk is te maken. Daar komt bij dat binnen het strafrechtelijk domein opsporingsdiensten en OM steeds vaker al activiteiten ontplooiën vóór het moment waarop sprake is van een (vermoeden van een) strafbaar feit en van een mogelijke verdachte. Ook die ontwikkeling draagt ertoe bij dat bestuursrechtelijke en strafrechtelijke handhaving naast elkaar kunnen gaan lopen. Dit gaat gepaard met een groeiende behoefte bij opsporingsdiensten en OM aan gegevens die andere organisaties hebben ten behoeve van het signaleren van trends en het maken van analyses om de criminaliteit beter te kunnen bestrijden. Het kan daarbij gaan om analyses in een meerwet context, waarbij partijen gezamenlijk bepaalde interventies of maatregelen geschiedt zijn om in de desbetreffende casus op te treden. Het kan ook gaan om een strategie die een meer pro-actief of preventief karakter heeft. Te denken valt aan het uitwisselen van gegevens om tot gezamenlijke "intelligence" te komen. Juist zulke vormen van samenwerking tussen bestuursrechtelijke toezichthouders en strafrechtelijke opsporingsdiensten kunnen bij uitbreiding meewerken hebben bij fraudebestrijding en andere activiteiten op het terrein van de rechtsaandrijving en criminaliteitsbestrijding.

Deze ontwikkelingen mogen intussen niet de ogen doen sluiten voor een aantal wezenlijke factoren die bij verstrekking van gegevens vanuit het bestuursrechtelijk naar het strafrechtelijk domein een grote mate van prudentie vergen. Zo kent het WvSv in de artikelen 125a e.v. een uitgebalanceerd en uitgewerkt systeem voor het verdienen van informatie door opsporingsdiensten en OM in het

geval dat sprake is van een verdenking.⁷⁵ Dit hangt samen met de bevoegdheden die de opsporingsinstanties en het OM hebben om met die gegevens wat te doen. Wanneer het OM in het kader van een samenwerkingsovereenkomst over gegevens komt te beschikken die het vervolgproces inzetting en behoefte van opsporing en vervolging ontstaat een mogelijkheid voor het OM gegevens te rechtlijnen bij de WSV om, zonder de waarborgen die het WSV biedt.⁷⁶ Een tweede factor is dat artikel 6 EVRM de verdachte vanaf het moment waarop sprake is van een "criminal charge" rechten geeft waaronder bij voorbeeld het recht dat een verdracht met zijn eigen verstand heeft mee te werken (beginsel van "nemo tenetur"). Als onderdeel van het recht op een "fair trial" wordt gezien de noodzaak van het hebben van een "safer trial" er moet worden vastgesteld welke informatie meewerkende komt. Aan de hand van de "trial" kan worden bepaald of de informatie rechtmatig is verkregen. Rechtmatige informatieverwerking via samenwerkingsovereenkomsten dient derhalve nauwkeurig te worden omschreven. Voorts verdient aandacht dat het bestuursrecht een ander bewijsrecht kent dan het strafrechtelijke systeem. In het bestuursrecht geldt de vrije bewijsleer. Conclusies kunnen worden getrokken en tekenen kunnen worden vast te staan op basis van voldoende aannemelijkheid. Indien een feit des altes is komen vast te staan, wordt uitgegaan van de opsporingsfase, kan dit ongemak op gegevens voort komen te staan met de strikte bewijzen in het strafrecht. Tot slot wordt hier gewezen op het feit dat onder dwang verkregen informatie in de controlefase niet mag worden gebruikt als bewijs bij de boete (of de vervolging) in verband met het verbod op zelfincriminatie.⁷⁷

Al deze factoren geven de burger een bepaalde mate van bescherming. Bij de verstrekking van gegevens resulteert het bestuursrechtelijk aan het strafrechtelijk domein alleen samenwerkingsovereenkomsten zal daarom ook in de toekomst met deze factoren rekening moeten worden gehouden. Voor één van de genoemde factoren ware een uitzondering te maken. Dit betreft de verstrekking van identificerende en andere dan identificerende gegevens die niet gevraagd zijn, aan de politie en andere opsporingsinstanties, respectievelijk aan het OM waarvoor nu ingevolge artikel 126bis, respectievelijk 126ter WSV een verdracht nodig is. De reden voor een dergelijke uitzondering is dat de derde bij wie de gegevens worden gevraagd, in het algemeen minder goed in staat is tot het maken van een afweging over de verstrekking, omdat hij geen kennis draagt van alle achtergronden van het verzoek. Daarnaast is de derde in geval van vrijwillige medewerking verantwoordelijk en aansprakelijk voor de verstrekking van de gegevens.⁷⁸ Bestuursorganen die aan samenwerkingsovereenkomsten deelnemen, zijn evenwel in het algemeen veel beter dan willekeurige anderen in staat tot het maken van een afweging over de verstrekking, omdat zij veelal wel enige kennis dragen van de achtergrond van het verzoek. Het is bij verstrekking door bestuursorganen dan ook niet uitzonderlijk nodig de verantwoordelijkheid voor het vergaan van gegevens uitsluitend naar te leggen bij de met opsporing belaste instanties.

Nu de ratic achter de artikelen 126bis en 126ter WSV in het geval van gegevensuitwisseling binnen samenwerkingsovereenkomsten vaak ontbreekt, levert het vereiste van een verdracht een onnodige belemmering voor een efficiënte gegevensuitwisseling binnen samenwerkingsovereenkomsten op.⁷⁹

⁷⁵ Wanneer er geen sprake is van een verdenking, en dat zal in geval van gegevensuitwisseling in samenwerkingsovereenkomsten vaak voorkomen, vindt de gegevensverwerking door opsporingsinstanties OM plaats op grond van de algemene taakstellende artikelen van de Politiewet (artikel 3), de Wet op de bijzondere opsporingsinstanties (artikel 3) en het Wetboek van Strafrecht (artikelen 141 en 143). Dit mag te rechter af een kleine tekortkoming op de bescherming van de persoonlijke levenssfeer worden gemaakt. Zie o.a. HR 19 december 1995, NJ 1995, 249 (Jordans).

⁷⁶ Er is dan door de (algemeen) wetgever bij het opmaken van een specifieke versterkingsbesluitting kennelijk wel een expliciete overweging gemaakt dat een actieve verstrekking aan opsporingsinstanties en OM gerechtvaardigd is.

⁷⁷ EHRM 25-3-1993, NJ 1993, 485 (Punkel), EHRM 17-12-1996, NJ 1997, 699 (Saunders) en EHRM 3-5-2000, NJR 2002/26 (J.B. vs Zwitserland).

⁷⁸ Kamerstukken II, 2003-2004, 25 441, nr. 3, blz. 2.

⁷⁹ Tegen deze achtergrond heeft de Voorzitter van het College van Procureurs-Generaal de Minister van Veiligheid en Justitie bij brief van 4 juni 2012 verzocht de wetgeving op dit punt zo aan te passen dat een

Wettigzwaar lijkt er op grond van een arrest van het Hof Arrnhem-Leeuwarden inmiddels ruimte te zijn voor verstrekking van gegevens door de Belastingdienst aan het OM zonder dat daarvoor een vordering van het OM op grond van artikel 126nd WvSv nodig is⁵⁶, maar de Hoge Raad heeft het bestaan van deze ruimte nog niet bevestigd. Los van dit specifiek geval blijkt uit de jurisprudentie met betrekking tot artikel 126nd WvSv dat een vordering door het OM als daarin bedoeld alleen dan uitbreide kan lijken, indien de verstrekking van de desbetreffende gegevens niet alleen vrijwillig, maar ook uit eigen beweging geschiedt.⁵⁷ Aangevraagd mag worden dat eenzelfde lijn geldt voor een vordering van identificerende gegevens als bedoeld in artikel 126nd WvSv. Zo lang deze lijn voor andere gevallen dan gegevensverstrekking door de Belastingdienst, aan het OM bijt, gelden en ook de ruimte voor gegevensverstrekking door de Belastingdienst nog ongewis is, blijft er sprake van een barrière voor de gegevensverstrekking aan de politie, andere opsporingsdiensten en het OM, ten eventuele kadervet zou te samen worden ingericht dat deze barrière verdwijnt. Daarbij zou rekening moeten worden gehouden met eventuele wensen van deelnemers aan een samenwerkingsverband omtrent het gebruik dat opsporingsdiensten en OM vervolgens van de ontvangen gegevens maken. Hoe daaraan invulling zou kunnen worden gegeven, komt in § 4.4 aan de orde.

3.7 Verstrekking van strafrechtelijke gegevens

In § 2.4 is naar voren gekomen dat de verwerking van bijzondere persoonsgegevens in begroef verboden is (art. 16 WvG). Wat bevat de WvG een aantal uitzonderingen op dat verbod. Zo is het verbod om strafrechtelijke persoonsgegevens te verwerken, niet van toepassing, ind en de verantwoordelijke deze heeft verkregen krachtens de WvG of de WvG (art. 22, eerste lid, WvG).

In de praktijk bestaat grote behoefte bij partijen die aan samenwerkingsverbanden deelnemen, aan betere mogelijkheden om strafrechtelijke gegevens door politie, bijzondere opsporingsdiensten en OM aan andere partijen binnen het samenwerkingsverband te laten verstrekken. Uit § 3.5 komt het beeld naar voren dat de mogelijkheden die de WvG en de WvG bieden om strafrechtelijke persoonsgegevens aan samenwerkingsverbanden te verstrekken, echter niet optimaal zijn. Ook een recente wijziging van de Wet Suut heeft daarin voor samenwerkingsverbanden op het terrein van de fraudebestrijding geen verandering gebracht.⁵⁸

De mogelijkheden om strafrechtelijke persoonsgegevens te verstrekken, kunnen worden verbeterd door in de WvG en WvG bepalingen op te nemen die een algemene grondslag voor gegevensverstrekking aan samenwerkingsverbanden als bedoeld in de kadervet geeft. Een dergelijke algemene grondslag zou impliceren dat het niet meer nodig zou zijn om voor ieder samenwerkingsverband afzonderlijk een basis voor gegevensuitwisseling in het Bpg, respectievelijk het Biso te leggen.

3.8 Typen van verwerking

De behoefte aan gegevensuitwisseling bestond in het verleden vooral uit informatie in een concreet geval. Deze behoefte bestaat nog steeds, maar wordt langzamer na d overvloedig door de behoefte aan gegevens ten behoeve van operationele bestandsvergelijkingen voor het onderkennen van trends en patronen en het opstellen van profielen. De ontwikkeling van geavanceerde analysestechnieken onder de noemer van "big data analytics" is daar mede debet aan. Met het oog op deze ontwikkeling wordt in de kabinetsafel van 30 december 2013 over de aanpak van fraude ervan uitgegaan dat de verkenning mede betrekking heeft op de mogelijkheden om op verkenkende wijze fraudepatronen te onderkennen.⁵⁹

gegevensverstrekking binnen een samenwerkingsverband mogelijk is zonder dat daaraan een vordering op grond van het stebel van strafvondertij te bevoegdheden ten grondslag ligt

⁵⁶ Zie Hof Arrnhem-Leeuwarden 8-12-2013, ECLI:NL:GHARL:2013:0476, de ook § 3.5.

⁵⁷ HR 27-11-2012, 1.8. RW015.

⁵⁸ Zie Kamerstukken II 2012-2013, 33579, nr. 3, blz. 22.

⁵⁹ Kamerstukken II 2013-2014, 17050, nr. 40, blz. 2.

De praktijk worstelt met de vraag of en, zo ja, in hoeverre de huidige regelgeving allerlei typen van gegevensverwerking binnen samenwerkingsverbanden toestaat. Dat geldt vooral voor de eerder bedoelde moderne analysemethoden. Mag bijvoorbeeld ICOW een ce-hand van een gerichte selectie van naar verwachting relevante databestandten met behulp van geavanceerde software mogelijk relevante patronen in beeld brengen die dit samenwerkingsverband kan gebruiken voor het opstellen van profielen? En mag ICOW een door haar te ontwikkelen profiel van bijvoorbeeld betrouwbare melders met alle data waarover zij rechtmatig de beschikking heeft, om een lijst vast te stellen van personen aan wie de grootste risico's zijn verbonden dat zij fraude plegen?

De thees behandelende onduidelijkheid op dit punt belemmert de ontwikkeling en het gebruik van diensten en producten die met moderne analysemethoden geleverd kunnen worden. Dit doet niet alleen voort uit het veelal ontbreken van bepalingen in de huidige regelgeving die specifieke beperking hebben op samenwerkingsverbanden²², maar ook uit het ontbreken van bepalingen over de wijze van gegevensverwerking. In zijn plaats ontbreekt wettelijke bepalingen die iets zeggen over geautomatiseerde gegevensverwerking of het geautomatiseerd toezien in de eigen systemen op verzoek van een derde waarvan de gegevens van belang zijn (door tussenkomst van een intermediair) worden verstrekt.²³

Een kaderwet gegevensuitwisseling zou de bestaande onduidelijkheid kunnen oplossen door voldoende te bevestigen dat de door deze wet gereguleerde gegevensuitwisseling binnen samenwerkingsverbanden betrekking kan hebben op alle in de wet beschreven typen van verwerking. Deze typen zouden in beginsel alle typen gegevensuitwisseling moeten betreffen die in § 2.5 zijn beschreven. In § 4.6 wordt dit nader uitgewerkt.

3.9 Kwaliteit gegevens en zorgvuldigheid bij verwerking

De Wetenschappelijke Raad voor het Regeringsbeleid heeft in zijn rapport IOverheid uit 2011 aangegeven dat voor het bewaken van de kwaliteit van gegevens relevant is dat te worden gehouden met een drietal ontwikkelingen:

1. het vernetwerken van informatie, i.e. het gezamenlijk gebruik en beheer van informatie in een netwerk van actoren,
2. het samenstellen en verkrijgen van informatie, d.w.z. het creëren van nieuwe informatie en profielen op basis van verschillende bronnen uit verschillende contexten,
3. het voeren van preventief en proactief beleid op basis van informatie, d.w.z. het actief beoogden van en ingrijpen in de samenleving op basis van informatiegestuurde risicoprofielen.

Deze ontwikkelingen brengen mee dat gegevens die uit bronnen met verschillende, soms zeer uiteenlopende doeleinden worden geput, eerst worden gecontextualiseerd om vervolgens te worden gerecontextualiseerd, wanneer zij worden gecombineerd met andere gegevens in een andere beleidscontext. Daaraan kleven risico's voor de kwaliteit van de gegevens in termen van betrouwbaarheid en betrouwbaarheid. Dat geldt voor de professionals die met deze gegevens moeten werken (en informatie uit een andere professionele context moeten interpreteren) en wordt nog versterkt wanneer het gaat om informatie die het resultaat is van technische bewerkingen, zoals "profiling" en "data mining". Aandacht voor de kwaliteit van informatie vereist ook gedegen aandacht voor technische en organisatorische randvoorwaarden zoals beveiliging, werkprocessen en een betrouwbare authenticatie- en identificatie-infrastructuur.²⁴

De hier geschetste ontwikkelingen doen zich vooral ook voor bij gegevensuitwisseling in samenwerkingsverbanden. Bij een onderzoek naar gegevensuitwisseling door toezichthouders

²² Uitzonderingen zijn te vinden in artikel 22, tweede lid, Wbp, artikel 20 Wpg, artikel 28, tweede lid, onder 4, Wet Bibbom artikel 54 Wet Suw. Zie ook § 8.2.

²³ Voorbeelden hiervan zijn artikel 23 Wpg, artikel 107c Kadasterwet en artikel 28 Handelsregisterwet 2007.

²⁴ Wetenschappelijke Raad voor het Regeringsbeleid, IOverheid, 2011, blz. 214-217.

brachten experts naar voren dat onder andere politiegegevens niet altijd even hard zijn. Welke hardheidsgraad de gegevens hebben, is vaak niet bekend. De gegevens kunnen uit meerdere bronnen komen, of het reeds kan onvolledig zijn. Dat is niet goed te controleren. Databestanden kunnen daardoor "vervuld" zijn met zachte informatie. Verder blijkt uit het onderzoek het risico dat gegevens niet helemaal betrouwbaar zijn wanneer deze binnen een gegevensverzameling worden vrijgemaakt voor andere informatie. Dit leidt tot leersing van de gegevens, die in een andere context en binnen een andere gegevensverzameling verkeerd of onjuist kan worden opgevat. Omgekeerd kunnen gegevens worden gebruikt alvorens zij worden verstrekt aan een andere partij, waarbij het belangrijke elementen verloren kunnen gaan.⁴⁵

Wil een kaderwet gegevensuitwisseling een integrale verbetering van de gegevensuitwisseling in samenwerkingsverband opleveren, is vaak niet bekend, dan zal deze kaderwet niet alleen een verruiming van de mogelijkheden van gegevensuitwisseling moeten bieden, maar ook voldoende maatregelen bevatten die bijdragen aan de kwaliteit van de gegevens en de zorgvuldigheid bij de verwerking daarvan. In § 4.7 zal worden ingegaan op de vraag welke voorzieningen dat zouden kunnen zijn.

3.10 Verantwoordelijke

Het is uit het oogpunt van privacybescherming van belang duidelijk vast te stellen wie met betrekking tot de gegevensverwerking als verantwoordelijke is de zwaarte van de Wbp is aan te merken. Op deze verantwoordelijke rusten immers verschillende verplichtingen, zoals de informatieplicht, de bevestigingsplicht, de meldingsplicht en de verplichting betrokkenen gebruik te kunnen laten maken van hun inzage- en correctierecht.

Als er sprake is van een samenwerkingsverband, moet het duidelijk zijn over de vraag wie verantwoordelijk is voor de gegevensverwerking binnen het samenwerkingsverband. In een kaderwet zou, in navolging van artikel 64, tweede lid, van de Wet SMO, als uitgangspunt kunnen worden genomen voor het gezamenlijke verantwoordelijkheid van de deelnemers aan het samenwerkingsverband. Uit uitgangspunt komt overeen met de keuze die men, gelooft op het gedingde karakter van de verschillende verwerkingen, nu meestal in de praktijk maakt. Het is evenwel denkbaar dat de verschillende verwerkingen een andere keuze rechtvaardigen. Er kan bijvoorbeeld sprake zijn van afzonderlijke verantwoordelijkheid per (deel)verwerking. Ook kan de situatie komen dat, ook al namen aan de verwerkingen verschillende organisaties deel, er voor één gemeenschappelijke verantwoordelijke wordt gekozen. Het is het oog op deze mogelijkheden zal een kaderwet ruimte dienen te bevatten om van het in de wet gekozen uitgangspunt af te wijken.

3.11 Informatieplicht

In de praktijk blijkt dat samenwerkingsverbanden vaak worstelen met de vraag of en, ja, in hoeverre zij moeten voldoen aan de informatieplicht van artikel 3a Wbp. Die vraag speelt vooral in het geval van grootschalige geautomatiseerde bestandsverwerkingen in een fase die voor het overgrote deel van de betrokkenen niet tot gevolgen leidt. De informatieplicht wordt in dat de betrokkenen voor de verantwoordelijke worden gatenmenen over de verwerking van hun persoonsgegevens. Deze plicht is niet van toepassing, indien de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven. In dat geval dient de verantwoordelijke de betroffende op de meest verzekte te informeren over het wettelijk voorschrift dat tot vastlegging of verstrekking van de hem betreffende gegevens heeft geleid (art. 34, vijfde lid, Wbp).

De keuze voor een kaderwet zou het mogelijk maken van deze uitzondering op de informatieplicht gebruik te maken. Daarvoor zou dan wel nodig zijn dat uit die kaderwet blijkt dat, indien partijen een samenwerkingsverband aangaan, zij – uitzondering daargelaten – verplicht zijn de

⁴⁵ De Moor van Ylft, a.w., blz. 53-57 en 75.

⁴⁶ Kamerstukken II 1997-1998, 25892, nr. 3, blz. 58.

noodzakelijke gegevens aan dat samenwerkingsverband te verstrekken.¹⁷ Het zou de transparantie voor de burger bevorderen, als in de kaderwet ook zou worden bepaald dat bij de oprichting van een samenwerkingsverband ervoor wordt gezorgd dat er algemene informatie wordt gegeven over de gegevensverwerking door het desbetreffende samenwerkingsverband. Deze informatie zou dan bijvoorbeeld op een website kunnen worden geplaatst. Het het oog daartoe zou de kaderwet de verplichting kunnen bevatten in het informatieprotocol beslissingen op te nemen met betrekking tot de informatieverstrekking over de gegevensuitwisseling aan het publiek (zie nader § 4.10).

Een dergelijke regeling in een kaderwet zou dus meebrengen dat niet iedere betrokkene afzonderlijk zou moeten worden geïnformeerd over de verwerking van gegevens over hem of haar. Dat heeft het voordeel dat alle inspanningen die hiervoor nodig zijn, achterwege kunnen blijven, zonder dat het noodzakelijk is precies na te gaan of die inspanningen zijn aan te merken als een onevenredige inspanning, die ingevolge het vierde lid van artikel 34 eveneens kan leiden tot het buiten toepassing laten van de informatieplicht. De vraag rijst is dat het in een samenwerkingsverband op het niveau van de fraudebestrijding al gauw gaat om gegevensverwerking die, als zij bij betrokkenen bekend wordt, tot calculerend gedrag bij hen kan leiden.¹⁸

3.12 Vertrouwen in het gebruik van gegevens door andere partijen

Bij gegevensuitwisseling in samenwerkingsverbanden geldt dat geen enkele partij graag gegevens verstrekt, als niet duidelijk is wat er mee gebeurt. Dat geldt vooral als het om gevoelige gegevens gaat. Het bestaat van onduidelijkheid op dit punt kan een belemmering vormen voor de gegevensuitwisseling. Het gaat hier vooral om de vraag of verstrekking aan derden buiten het samenwerkingsverband mogelijk moet zijn en, zo ja, onder welke voorwaarden. Als hierover onduidelijkheid bestaat, wordt mogelijk in strijd gehandeld met het zorgvuldigheidsbeginsel dat in artikel 6 WvG is verankerd.¹⁹

Om voldoende vertrouwen in het gebruik van gegevens door andere partijen te kunnen hebben, wordt soms het "globe"-principe gehanteerd: geen actie register overleg. Dit gebeurt bijvoorbeeld bij samenwerkingsverbanden die te maken hebben met meldingen op grond van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wvft), zoals het FIC. Verder is denkbaar dat expliciet wordt vastgelegt dat informatieverstrekking aan een derde alleen plaatsvindt met instemming van de partner van wie de persoonsgegevens oorspronkelijk afkomstig zijn.²⁰ Met het oog daarop kan het zinvol zijn doorverzekking aan derden te "loggen". In een kaderwet kunnen op dit punt bepaalde voorkeuren worden getrokken.

¹⁷ Vgl. artikel 64, tweede lid, Wet Suwi.

¹⁸ Zie ook Kamerstukken II 2012-2013, 33593, nr. 3, blz. 26.

¹⁹ Vgl. ABROU 4 juli 2007, overweging 2.4.5, UN: BA3742, 200608203/L.

²⁰ Zie de artikelen 4 en 13 informatieprotocol FEC 2011, Stcrt. 2011, 23708.

4. Contouren kaderwet

4.1 Inleiding

In de vorige paragraaf is aangegeven dat de daarin genoemde knelpunten kunnen worden weggenomen door een kaderwet voor de gegevensuitwisseling in samenwerkingsverbanden. In deze paragraaf worden de contouren van zo'n kaderwet geschetst. Daarvoor is mede gebruik gemaakt van elementen uit een reeds wet tot wijziging van de Wet Suwi.¹⁶ Deze wijzigingwet bevat een nieuw artikel 64 *Wet Suwi*, waarin een regeling voor de gegevensverstrekking ter behoeve van samenwerkingsverbanden is opgenomen. Aan het slot van deze paragraaf wordt achtereenvolgens ook ingegaan op de rechtsbescherming en het toezicht, de verhouding van de kaderwet tot de Lissabon- en wijzigingswet, de betrekking van de kaderwet tot het bestaande samenwerkingsverbanden aan de verhouding van de kaderwet tot het EVRM en reguleerend van de B.J.

Een belangrijk kenmerk van het nieuwe artikel 64 *Wet Suwi* is dat het niet geschreven is voor één specifiek samenwerkingsverband. Daarmee heeft de artikel al en geeft het karakter van een kaderregeling. Een verschil met een kaderwet, zoals bedoeld in deze noot, is dat de reikwijdte van artikel 64 beperkt is dan van zo'n kaderwet. Dat artikel bestrijkt maar een – overigens niet onbelangrijk – deel van de mogelijke vormen van fraude en bevat vanwege die relatief beperkte reikwijdte een aantal elementen, zoals de (goede of slechte) samenstelling van een samenwerkingsverband¹⁷, die in een kaderwet uit een oogpunt van flexibiliteit geheel aan regeling bij convenant zouden moeten worden overgelaten. Een ander verschil is dat artikel 64 bijke van de toelichting uitsluit dat aan het samenwerkingsverband ook strafrechtelijke persoonsgegevens worden versierd.¹⁸

Een kaderwet (of normwet) is een wet die de algemene principes, verantwoordelijkheden en procedures regelt, maar geen detailsaande regelt. Een belangrijke eigenschap van kaderwetten (ijk den ook dat zij) doorgaans niet zelf inhoudelijk-nuutlijke regulatieve beuring vastleggen, maar vooral randvoorwaarden scheppen waarbinnen bijvoorbeeld legale regelgevers, beleidsmakers of uitvoerders dienen te opereren.¹⁹ Een kaderwet zal in dat licht bezien niet voor ieder samenwerkingsverband in detail regelen waaraan dat samenwerkingsverband zich heeft te houden. Dat zou ook niet goed mogelijk zijn onder te verstaan in de rigide structuur die onvoldoende ruimte voor maatwerk voor ieder afzonderlijk samenwerkingsverband levert.²⁰ Wel zal een kaderwet een raamwerk bieden waarbinnen de deelnemers aan een samenwerkingsverband hun samenwerking onder uitwerken in een convenant en in een informatieprotocol, dat de nodige waarborgen voor de bescherming van persoonsgegevens bevat. Een kaderwet kan deel bij de knelpunten wegnemen die nu in de praktijk bij het opstellen van zo'n convenant en protocol worden ervaren. Een kaderwet zou echter niet alleen regulerend en faciliterend, maar ook normerend moeten zijn.²¹ Zij zou de leeflijnen moeten toelichten voor een aantal knelpunten voor een zorgvuldige gegevensuitwisseling, die in het convenant en het informatieprotocol van een samenwerkingsverband nader moeten worden uitgewerkt.

¹⁶ Wet van 3 oktober 2015 tot wijziging van de *Wet structuur uitvoeringsorganisatie werk en inkomen* en enige andere wetten in verband met fraudeaanpak door gegevensuitwisseling en het effectief gebruik van Minier de overheid behorende zijnde gegevens, Stb. 2015, 495.

¹⁷ Artikel 64, eerste lid, van de *Wet Suwi* noemt de colleges van burgemeester en wethouders, het ZWV, de SVB, toezichthouders op het terrein van SZW, de Belastingdienst en de andere bestuursorganen en personen, voor zover zij zijn belast met een publieke taak en daartoe bij regeling van de Ministers van SZW of Financien zijn aangewezen.

¹⁸ Kamerstukken II 2011-2012, 35579, nr. 3, blz. 22.

¹⁹ R.A.J. van Tol en A. Vlaspolder, *Wetgeving van het primaat van de wetgever: de betekenis van de*

kaderwetgeving en delegatie, 2012, blz. 16.

²⁰ De werkgroep herijking toelichtingswetgeving (wv) in 2008 met betrekking tot de gegevensuitwisseling tussen toezichthouders tot dezelfde conclusie. Zie § 2.8.

²¹ De Moor van Vugt, a.w., blz. 59.

Gelet op het kabinetseinpunt over het WODC-rapport "Gegevensuitwisseling door toezichthouders" zal een kaderwet ook niet het karakter kunnen krijgen van een wet waarin de huidige Wbp wordt omgevormd tot een brede kaderwet, evenwel met nadere uitwerking in sectorale wetgeving. Het kabinetseinpunt laat wel ruimte voor een meer bescheiden opzet van een kaderwet, maar wel de Wbp, de Wpg, de Wpgs en de bepalingen over gegevensverwerking in sectorale wetten, op mogelijk een enkele kleine aanpassing na, in stand blijven. Deze opzet zou niet alleen het voordeel hebben dat de voorbereiding van een dergelijke kaderwet niet of nauwelijks zou interfereren met de lopende herziening van de Europese regelgeving inzake de verwerking en bescherming van persoonsgegevens en het vervolg op de evaluatie van de Wpg en Wpgs. Zij zou ook de voorkeur verdienen, omdat bij een keuze voor een brede kaderwet waarin de Wbp opgaat, voortdurend zou worden gegaan aan het feit dat de Wbp ook betekenis heeft voor al die normen van gegevensverwerking die buiten samenwerkingsverbanden plaatsvinden. Hetzelfde geldt met betrekking tot de Wpg en Wpgs en bepalingen over gegevensverwerking in sectorale wetten, voor zover de gedachte zou bestaan deze regelgeving of de en daarvan eveneens in z'n brede kaderwet op te nemen. Een kaderwet met deze opzet zou dus ook geen alles omvattende kader voor gegevensuitwisseling in samenwerkingsverbanden bieden. De Wbp, Wpgs, Wpgs en de bepalingen over gegevensverwerking in sectorale wetten zullen ook in relatie tot samenwerkingsverbanden onder de werking van de kaderwet vallen, hun betekenis blijven houden, tenzij een specifieke bepaling uit de kaderwet deze tenzijde schuift (zie nader § 4.1.2). In zoverre dekt de term "kaderwet" niet geheel de lading. Aan de andere kant is de term "kaderwet" in die zin wel op haar plaats, nu zij kan opvulke van verder uitdraaiende regelgeving en aanvullend kader voor gegevensuitwisselingen in samenwerkingsverbanden geeft, waarbinnen een convenant en een informatieprotocol nadere regels over deze gegevensuitwisseling kunnen bevatten.

Tot slot verloop te wijzen dat een kaderwet voor gegevensuitwisseling een algemeen normatief zou vormen op de wettelijke regeling die in specifieke gevallen van samenwerking voortvloeit en daarbij regels over gegevensuitwisseling geven, zoals de in artikel 9 van de Wet Samenwerkingsverbanden tussen het UWV, de SVB en de gemeenten bij de uitvoering van de wet en enige andere wetten. Deze aanpak impliceert niet dat ook de kaderwet samenwerkingsverbanden overheidsonderzoek voorschrijft. Dat zou, gelet op de vele, soms zeer uiteenlopende belangen van deze organisaties, niet wettelijk. De aanvullende betekenis van een kaderwet zal wel zijn gelegen in het feit dat, als partijen tot samenwerking besluiten in de uitvoering van gegevens onder de werking van de kaderwet willen laten vallen, deze kaderwet de uitwisseling van gegevens in z'n samenwerkingsverband legitimeert, faciliteert en normeert. Hiermee is ook gezegd dat de kaderwet niet tot doel heeft een exclusief regime voor gegevensuitwisseling in samenwerkingsverbanden te creëren. Het staat huidige en toekomstige samenwerkingsverbanden vrij ervoor te kiezen hun gegevensverwerking in te richten op grond van de thans al geldende wetgeving, zolang het kan samenwerkingsverbanden bestaan, indien de kaderwet voor een samenwerkingsverband, geldt op haar behoeften aan informatie, niet of nauwelijks betere mogelijkheden tot gegevensuitwisseling boven de bestaande wetgeving biedt.

Tegen de achtergrond van deze overwegingen zou een kaderwet de elementen kunnen bevatten die in de volgende paragrafen worden beschreven.

4.2 Reikwijdte kaderwet

In de brief van het kabinet van 20 december 2013 over de aanpak van fraude wordt de verkenning naar een kaderwet toegepast op fraudebestrijding. De brief van de kabinetsschreef brengt dat begrip (plan) mee. De vraag rijst evenwel, of een kaderwet gegevensuitwisseling in samenwerkingsverbanden zich tot dat domein zou moeten beperken.

Zoals in § 2.3 al naar voren is gekomen, zou de van de samenwerkingsverbanden die zich met fraudebestrijding bezighouden, in feite een minderheid zich uitsluitend met fraudebestrijding bezig. De meeste samenwerkingsverbanden hebben een taak die zich in meerdere of mindere mate ook tot andere terreinen uitstrekt. Een kaderwet die zich beperkt tot gegevensuitwisseling ten behoeve van de fraudebestrijding zou tot gevolg hebben dat samenwerkingsverbanden ten dele wel en ten dele niet onder de werking van de kaderwet vallen. Dat zou voor die samenwerkingsverbanden een onverklaarbare situatie opleveren. Het zou al lastig zijn, als gegevens voor uitwisseling ten doel zouden worden verzameld. Gegevens die samenwerkingsoverborden verwerken, kunnen echter *overeenkomstig* mogelijk dienen. Ze kunnen de RIEC's bepaalde persoonsgegevens verwerken met het oog op tegelijkertijd georganiseerde hennepzetten én fraude in de vastgoedsector. Het is dan niet moeilijk deze verwerking te laten plaatsvinden onder de gelijktijdige werking van de kaderwet en van daaraan afwijkende bepalingen in andere wetgeving.

Lós van deze overweging kan worden vastgesteld dat een kaderwet voor veel meer samenwerkingsverbanden in de publiek steer betekenis kan hebben dan alleen de verbanden die (mede) op het terrein van de fraudebestrijding bezig zijn. Geduiden uit de praktijk bevestigen dit. Bij een relatief smalle kaderwet zou dus al gauw de behoefte ontstaan om voor bepaalde specifieke domeinen een kaderwetgeving op te stellen. Dat pleit voor een kaderwet die een breder domein dan fraudebestrijding bestrijkt. Gekozen zou dan kunnen worden voor een kaderwet op het brede terrein van de voorkoming van onrechtmatig gebruik van overheidsgegevens en overheidsvoorzieningen, de uitvoering van toezicht op de naleving van wettelijke voorschriften en de handhaving van de openbare orde en veiligheid (‘bestuursrechtelijke preventie en handhaving’) en de voorkoming, opsporing en vervolging van strafbare feiten (‘strafrechtelijke preventie en handhaving’). Het is immers dit brede terrein waarop zich allerlei samenwerkingsverbanden manifesteren die gegevens binnen en tussen het bestuursrechtelijke en strafrechtelijke domein willen uitwisselen.¹⁷

Blijft vanuit de overheid kan de relatie van burgers en overheid worden gegroepeerd in drie categorieën: dienstverlening, zorg en criminaliteit. In dat licht bezien zou een kaderwet met de hiervoor voorgestelde reikwijdte zich richten op de controle-taak van de overheid. Het gaat hier om een weliswaar breed, maar wel samenhangend terrein, waarop de overheid verschillende functies vervult. Deze variëren van toetsing van de antecedenten van een burger die een vergoeding aanvraagt, tot de vervolging van een burger die een strafbaar feit pleegt. Dit neemt niet weg dat de drie genoemde categorieën in analytische zin weliswaar van elkaar te onderscheiden zijn, maar in praktische zin sterk naar elkaar toep. Voor het uitvoeren van de controle-taak wordt immers regelmatig een beroep gedaan op gegevens die oorspronkelijk op de andere terreinen – dienstverlening en zorg – zijn verkregen. Niettemin zal bij het uitvoeren van een kaderwet – mede het oog op het principe van doelbinding – rekening moeten worden gehouden met het feit dat het hier om verschillende terreinen gaat. Dit geldt met name voor gegevens op het terrein van de zorg, omdat het op dat terrein al bijzondere privacyvoorzieningen kan zijn. Te denken valt aan gegevens met betrekking tot iemands gezondheid, waarvoor het modisch beroepsgeheim geldt. Nu ku consumenten hiervan voor een eventuele kaderwet moeten worden vrijgesteld, komt in § 4.4 aan de orde.

Erkend zij dat ook een kaderwet op een breed terrein als de controle-taak van de overheid het probleem kan oproepen van de toepasbaarheid op samenwerkingsverbanden die op zurel het terrein van de kaderwet als daarbuiten opereren. Naarmate het terrein dat de kaderwet dekt, groter is, zal dit probleem zich naar verwachting evenwel minder snel voordoen. Daarbij moet worden bedacht dat bijvoorbeeld de gegevensverwerking binnen veiligheidsdiensten volledig onder de reikwijdte van zo'n bredere kaderwet is te vatten. Weliswaar nemen aan veiligheidsdiensten ook partners uit de zorg deel, maar het doel van veiligheidsdiensten en daarmee ook van de gegevensverwerking staat in het teken van het terugcringen van overlast, huiselijk geweld en

¹⁷ Hoe een kaderwet met deze strekking zich tot de bestaande wetgeving zou verhouden, komt in § 4.12 aan de orde.

¹⁸ De Wetenschappelijke Raad voor het Regeringsbeleid, Overheid, 2013, Nr. 72.

criminaliteit en valt daarmee onder de noemer van handhaving van de openbare orde en veiligheid en voorkoming van strafbare feiten en aldus onder de reikwijdte van zijn bredere kaderwet.³⁹

Een andere vraag die de reikwijdte van een eventuele kaderwet bepaalt, is de vraag of deze wet alleen voor samenwerkingsverbanden zou moeten gelden die op nationaal niveau optreden, of ook voor verbanden die op regionaal of lokaal niveau werkzaam zijn. Het het oog op de belangen die de kaderwet wil dienen, ligt een beperking tot samenwerkingsverbanden op nationaal niveau niet voor de hand. Juist op lokaal en regionaal niveau bestaan samenwerkingsverbanden die maatwerk vergen, waarvoor een kaderwet een koolstofmorfende, filterende en normerende functie kan uitoefenen.

Voor de reikwijdte van een kaderwet is tot slot van belang of een samenwerkingsverband die onder de kaderwet vallen, ook private partijen mogen deelnemen. Om de redenen die in § 2.3 zijn genoemd, valt daar veel voor te zeggen. Omdat het delen van informatie tussen publieke en private partijen gevoelig ligt, is het wenselijk dat de kaderwet voldoende waarborgen bevat wat de gegevensuitwisseling en de rechtvaardigen doel dient. De belangrijke waarborg is dat dit doel een publiek belang dient te zijn, vaststelling van gegevens aan private partijen met het oog op bijvoorbeeld commerciële belangen van die partijen is ongepast. Met een kaderwet die betrekking heeft op gegevensuitwisseling met als doel de bestuursrechtelijke en strafrechtelijke preventie en handhaving te bevorderen, is dat publieke belang verzekerd. Een andere waarborg is dat de kaderwet de kring van private partijen die aan samenwerkingsverbanden kunnen deelnemen, beperkt tot partijen die een relatie tot enig publiek belang hebben. Dat belang kan zich uiten in het feit dat het om private partijen gaat die een wettelijke taak hebben. Het zou daarbij ook om koepel- of brancheorganisaties van dergelijke partijen kunnen gaan. Met deze beperking valt te denken aan banken, die op grond van de Wet ter voorkoming van misstanden en financiering van terrorisme aan zijn cliëntenonderzoek moeten houden. Bij brancheorganisatie kan in dit verband worden gedacht aan het Verbod van verspreiding, nu ook verspreiders van degelek cliëntenonderzoek moeten houden. Omdat niet geheel op voorhand valt in te zien of er niet nog andere private partijen zijn die op goede gronden aan een samenwerkingsverband zouden kunnen deelnemen, lijkt het wenselijk te bepalen dat private partijen ook dan aan een samenwerkingsverband onder de reikwijdte van deze wet kunnen deelnemen, indien zij voortkomen op een tijd die bij nationale wetgeving is vastgesteld.⁴⁰ Daarmee dragen de ministers op wat beleidsterrein het desbetreffende samenwerkingsverband functioneert, ingeval van deelname van private partijen van deze lijst made verantwoordelijkheid voor de samenstelling van het verband en kunnen zij daarop door het parlement worden aangesproken. Dit kan vooral van belang zijn bij regionale of lokale samenwerkingsverbanden voorwaar de ministeriële verantwoordelijkheid, afhankelijk van de deelnemers van overtuiging, niet of slechts in beperkte mate samewerkend zou zijn.

Als resumé van voorgaande besprekingen bepaalt de wetgeving een eventuele kaderwet zo in te richten dat zij betrekking heeft op samenwerkingsverbanden die voor een specifiek doel binnert het brede kader van bestuursrechtelijke en strafrechtelijke preventie en handhaving werkzaam zijn, op zowel nationaal, regionaal als lokaal niveau, en waarvan ook private partijen kunnen deelnemen.

4.3 Regeling samenwerkingsverband in convenant

Een kaderwet gegevensuitwisseling in samenwerkingsverbanden zou in de eerste plaats moeten bepalen dat bestuursorganen⁴¹ en private partijen aan een samenwerkingsverband kunnen

³⁹ Zie voor het doel en de opzet van veiligheidszaken: <http://veiligheidszaken.nl/achtergrond>.

⁴⁰ Gedacht kan worden een lijst die is vastgesteld door de Minister van Veiligheid en Justitie en de Minister op wien beleidszaken de desbetreffende of private werkzaam is. Bij deelname van bijvoorbeeld het Verbod van verspreiding gaat het dan om de Minister van Financiën.

⁴¹ Het feit dat hier over bestuursorganen wordt gesproken sluit uiteraard niet uit dat in de praktijk een voor een bestuursorgaan gemachtigde persoon, dienst of instelling aan het samenwerkingsverband deelneemt en met het oog daarop ook het convenant ondertekent.

deelnemers ten behoeve van een integraal optreden in het belang van de voorkoming van onrechtmatig gebruik van overreeds geldend en overtuigendvoorzettingen, de uitoefening van toezicht op de naleving van wettelijke voorschriften, de handhaving van de opstapende en veiligheids van de voorkoming, opsporing en vervolging van strafbare feiten. Hiermee zou een kaderwet het bredere doel omschrijven waarbinnen samenwerkingsverbanden voor een meer specifiek doel kunnen worden aangegán. Met integraal optreden wordt in dit verband bedoeld dat de deelnemers aan een samenwerkingsverband tot een integrale venging van alle relevante informatie komen, zodat zij daarop hun optreden kunnen baseren. Het hoeft niet te betrekken dat ook alle deelnemers tot actie overgaan. Dat beruht af van wat als het meest effectieve optreden wordt gezien.

De kaderwet zou vervolgens moeten bepalen dat de deelnemers aan het samenwerkingsverband in een convenant nauwkeurig het specifieke doel van de samenwerking en de daarvoor noodzakelijke gegevensuitwisseling vastleggen. Dit doel moet passen binnen de reikwijdte van de breedere wettelijke doelomschrijving en niet onverenigbaar zijn met het doel waarvoor de gegevens die aan het samenwerkingsverband worden verstrekt, oorspronkelijk zijn verzameld. Als het huidige voorstel voor een Algemeen verordening gegevensbescherming wordt aangenomen, zal er ruimte ontstaan om bij onverenigbaarheid van doelen in een samenwerkingsverband toch tot gegevensuitwisseling over te gaan (zie § 3.4). Bij de voorbereiding van een eventuele kaderwet zal hiermee rekening moeten worden gehouden.

De brede wettelijke doelomschrijving kan uitbreiden niet tot gevolg hebben dat samenwerkingsverbanden worden opgevoerd die over de volle breedte daarvan zullen gaan opereren. De verenigbaarheidstoets die artikel 9 WvG voorziet, zou daar al gauw een stokje voor steken. De opdrinking van dergelijke zeer brede samenwerkingsverbanden zou kunnen op gespannen voet staan met het in artikel 8 EVRM verankerde vereiste van noodzakelijkheid en de daaruit voortvloeiende beginselen van proportionaliteit en subsidiariteit (zie hierna § 4.7). Deelnemers aan een samenwerkingsverband zullen het specifieke doel van het samenwerkingsverband en de daarvoor noodzakelijke gegevensuitwisseling dan ook slechts moeten kunnen verdedigen in het licht van dit vereiste en deze beginselen. Het is nu al te zien dat onder de werking van de kaderwet niet veranderen.

Over de vraag of een samenwerkingsverband onder de werking van de kaderwet valt, mag geen ruzieverband bestaan. Dit geldt te meer, nu de kaderwet – zie 4.1 – een exclusief regime voor samenwerkingsverbanden beoogt te zijn. Om die reden zullen de deelnemers aan een samenwerkingsverband in hun convenant uitdrukkelijk moeten aangeven dat het samenwerkingsverband onder de werking van de kaderwet valt. Het impliceert uitdrukkelijk dat zij niet alleen de beschikking over betere mogelijkheden tot gegevensuitwisseling krijgen, maar ook aan de extra waarborgen moeten voldoen die in § 4.7 aan de orde komen.

De kaderwet zou kunnen bepalen dat het convenant naast het specifieke doel van het samenwerkingsverband in ieder geval ook het volgende regelt:

- de taken en verantwoordelijkheden die binnen het samenwerkingsverband worden uitgevoerd,
- de wijze waarop het samenwerkingsverband wordt bestuurd,
- de inrichting van een eventuele bureau dat het samenwerkingsverband ondersteunt,
- de rechten en de verplichtingen van de deelnemers,
- de datum van inwerkingtreding en de geldigheidsduur van het convenant, en
- de mogelijkheden van toetreding tot en opzegging van het convenant.

De regeling van taken en verantwoordelijkheden, bedoeld onder a, dient te minste een specifieke beschrijving te bevatten van de in § 4.6 genoemde typen van gegevensuitwisseling, voor zover het samenwerkingsverband deze typen uitvoert. Daarbij moet uitdrukkelijk worden getoetst of deze taken en verantwoordelijkheden voldoende mate samenhang vertonen met de taken van de deelnemende organisaties.

De regeling van de onder b bedoelde wijze waarop het samenwerkingsverband wordt bestuurd, kan onder meer regels bevatten over bijvoorbeeld een stuurgroep, bestaande uit vertegenwoordigers van de deelnemers, die de regie over de werkzaamheden van het verband

voert. De regeling zou ook – zie § 4.8 – een registreur kunnen aanwijzen die de deelnemers ondersteunt bij de uitvoering van hun rol als gezamenlijk verantwoordelijke in de zin van de Wbp. In de regeling kan, tot slot, doorgewoont gebruik worden gemaakt van de in § 4.0 genoemde mogelijkheid één van deelnemers als verantwoordelijke voor de gehele gegevensverwerking in het samenwerkingsverband aan te wijzen.

Bij de onder d bedoelde verplichtingen kan onder meer worden gedacht aan verplichtingen op het terrein van de bescherming van de samenwerking, inclusief een eventueel ondersteund bureau. Denkbaar is ook dat de verplichtingen betrekking hebben op het omtrekken van medewerkers bij het bureau.

Met de aanwijzing in het convenant dat het samenwerkingsverband onder de werking van de kaderwet valt, vormt het samenwerkingsverband een publiekrechtelijke rechtsvorm. Er is immers sprake van een georganiseerd verband dat op basis van de kaderwet door middel van een convenant tot stand komt, waarbij de kaderwet de voorwaarden formuleert waaraan het samenwerkingsverband moet voldoen. Ook een eventueel bureau dat het samenwerkingsverband ondersteunt, kan als een publiekrechtelijke rechtsvorm worden aangemerkt, als dit op basis van de kaderwet door middel van het convenant in het leven wordt geroepen. Voor het ziele van een publiekrechtelijke rechtsvorm is het niet nodig dat het samenwerkingsverband of het bureau ook rechtspersoonlijkheid bezit.¹⁰⁰ Macht voor een bepaald samenwerkingsverband aanleiding bestaat dit rechtspersoonlijkheid te geven, dan verdient de vorm van publiekrechtelijke rechtspersoonlijkheid de voorkeur. Daarvoor zal een speelse wet nodig zijn. Onder omstandigheden is ook denkbaar dat een samenwerkingsverband de vorm van een privaatrechtelijke rechtspersoon krijgt, bijvoorbeeld die van stichting. Doordat kan afrekening bestaan bij deelname van private partijen. In dat geval is geen sprake van een nalg. Omdat de kaderwet het samenwerkingsverband en een eventueel bureau tot publiekrechtelijke rechtsvormen zou maken, zou deze wet ook de basis kunnen bieden voor verstrekking van gegevens aan alle deelnemers van het samenwerkingsverband, tegelijk en aan het bureau. Daarmee zou de vraag of verstrekking daaraan wel een voldoende juridische grondslag heeft, tot het verleden gaan behoren.

De kaderwet zou met betrekking tot het convenant tot slot kunnen bepalen dat het wordt gepubliceerd in de Staatscourant en overigens op een voor het publiek toegankelijke wijze openbaar wordt gemaakt.

4.4 Verplichte uitwisseling van gegevens

De deelname aan een samenwerkingsverband kan niet vrijwillig zijn. De kaderwet zou dan ook moeten voorschrijven dat de deelnemers verplicht zijn de voor het samenwerkingsverband noodzakelijke gegevens aan de andere deelnemers te verstrekken, waar zij er bij daarop geen uitzonderingen mogelijk hebben gemaakt. Benadrukt wordt dat deze verplichting alleen geldt voor noodzakelijke gegevens. Het noodzakelijkheidsoverzicht, zoals dat uit het EVRM voortvloeit en in artikel 8 Wbp is neergelegd, blijft dus overeind.

De verplichting tot gegevensverstrekking in een kaderwet voor specifieke samenwerkingverbanden zou als een "lex specialis" kunnen worden gezien ten opzichte van de generieke geheimhoudingsbepalingen in sectorwetten en zou aldus voorrang hebben boven die bepalingen. Om op dit punt echter geen misverstand te laten ontstaan verdient het de voorkeur in de kaderwet

¹⁰⁰ Samenwerkingsverbanden die onder de kaderwet vallen, kunnen in dit opzicht misschien worden vergeleken met adviescolleges. Ook zij hebben geen rechtspersoonlijkheid. Wel worden zij aangemerkt als een publiekrechtelijke rechtsvorm. Het verschil met adviescolleges is dat de kaderwet voor samenwerkingsverbanden die onder de wet willen vallen, voorschrijft dat zij bij convenant worden opgericht, terwijl de huidige Kaderwet adviescolleges voorschrijft dat adviescolleges worden ingesteld bij wet. Voor het ziele van een publiekrechtelijke rechtsvorm doet dat verschil echter niet ter zake.

uitdrukkelijk te bepalen dat geheimhoudingsbepalingen in andere wetten buiten toepassing blijven. Naarmee kan een kadernet knelpunten als ondereken in § 3.5 wegemen.

Op de verplichting tot gegevensverstrekking en het buiten toepassing laten van geheimhoudingsbepalingen zou voorts een uitzondering moeten worden gemaakt, voor zover het om bijzondere persoonsgegevens als bedoeld in artikel 16 WvG zou gaan. Het gaat om gegevens met betrekking tot iemands godsdienst of levensovertuiging, ras, lichtelijke gezondheid, gezondheid, seksuele levenswijze, lidmaatschap van een vakbond, en strafrechtelijke gegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. De gevoelige aard van deze gegevens doet mee te brengen dat de verplichting tot gegevensverstrekking en het buiten toepassing laten van geheimhoudingsbepalingen – dierk noem aan het medisch beroepsgewest – in beginsel niet voor dergelijke gegevens geldt. Mocht er aanleiding bestaan om met betrekking tot (bepaalde categorieën van) dergelijke gegevens toch een bevoegdheid dan wel verplichting tot gegevensverstrekking aan bepaalde samenwerkingsverbanden in het leven te roepen, dan zal daarvoor een specifieke wettelijke grondslag nodig blijven.

Op het beginsel om de verplichting tot gegevensverstrekking en het buiten toepassing laten van geheimhoudingsbepalingen niet op bijzondere persoonsgegevens betrekking te laten hebben, zou zo zijn teurt tenminste één uitzondering moeten worden gemaakt. Deze uitzondering zou betrekking hebben op strafrechtelijke gegevens, met betrekking tot gegevens die bij uitstek relevant kunnen zijn voor samenwerkingsverbanden op het brede terrein van de in § 4.2 beschreven controle-taak van de overheid. Om die reden is in § 3.7 dan ook bepaald de mogelijkheid om strafrechtelijke gegevens aan samenwerkingsverbanden te verstrekken, te verbeteren. Dit zou kunnen geschieden door in de WvG en WvS bepalingen op te nemen die een algemene grondslag voor gegevensverstrekking aan samenwerkingsverbanden als bedoeld in de kadernet geeft. Een dergelijke algemene grondslag zou impliceren dat het niet meer nodig zou zijn om voor ieder samenwerkingsverband afzonderlijk een lijst van gegevensuitwisseling in het Bijl. en het Bijl. te leggen.

Een mogelijke andere uitzondering op voornoemd beginsel zou kunnen gelden voor persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. Dergelijke gegevens kunnen immers relevant zijn voor samenwerkingsverbanden op het terrein van de handhaving van de openbare orde en veiligheid.

De verplichting tot gegevensverstrekking is ook anderszins niet absoluut. Partijen kunnen in het informatieprotocol (zie hierna § 4.10), uitzonderingen hierop opnemen. Een uitzondering moet zijn ingegeven door een belang bij de desbetreffende deelnemer dat zwaarder weegt dan het gemeentelijke belang van de deelnemers aan het samenwerkingsverband. Te denken valt aan een belang bij politie en OM om gegevens uit een lopend opsporingsonderzoek waarin een relatie met één van de andere deelnemers is te leggen, niet met die andere deelnemers te delen.

Onder de verplichting tot gegevensverstrekking zou ook de verstrekking aan politie, andere overheidsinstellingen en OM vallen. In § 3.6 is in dit verband bepaald dat gegevens in samenwerkingsverbanden voortaan aan de politie, andere opsporingsdiensten of het OM kunnen worden verstrekt, zonder dat daarvoor een vermelding als bedoeld in artikel 126c of 126d WvS nodig is. Daarom zou in het wetsvoorstel voor een kadernet een uitzondering van het Wetboek van Strafvordering moeten worden opgenomen met als strekking dat voor de verstrekking in een samenwerkingsverband van gegevens aan de politie, andere opsporingsdiensten of het OM een mogelijke verontreiniging achterwege kan blijven. Mocht het onder omstandigheden zo zijn dat een vastuursorgaan onvoldoende kennis over de achtergrond van het desbetreffende verzoek heeft of andere redenen heeft om de verantwoordelijkheid en eventuele aansprakelijkheid voor de verstrekking van de gegevens niet te willen dragen, dan kan het gebruik maken van de hiervoor beschreven mogelijkheid in het informatieprotocol vast te leggen dat van verstrekking kan afzien. In dat geval zal de politie, de opsporingsdienst of het OM buiten het samenwerkingsverband, zo nodig, althans een voorzetting op grond van artikel 126c, respectievelijk 126d kunnen instellen. Verder zou rekening moeten worden gehouden met eventuele wensen van deelnemers aan een samenwerkingsverband omtrent het gebruik dat opsporingsdiensten en OM

vervolgen van de ontvangen gegevens maken. Daarnaast zou invulling kunnen worden gegeven door in een kaderwet te bepalen of de deelnemers aan een samenwerkingsverband naast ook opsporingsdiensten en OM deelnemers, in het informatieprotocol (als 5.4.10) kunnen vastleggen het gegevens die deze instanties zonder voorering verkrijgen, door hen alleen mogen worden gebruikt voor uitvoering van het doel die zijn vastgesteld op afleveren die de gezamenlijke deelnemers in het kader van het samenwerkingsverband hebben opgesteld. De deelnemers zouden desgewenst in het informatieprotocol ook kunnen vastleggen dat, indien het OM mede op basis van de ontvangen gegevens een vervolgij wil starten, deze gegevens daarvoor alleen mogen worden gebruikt als deze alsnog worden gevraagd.

4.5 Specifieke vastlegging van soorten gegevens

Uit een oogpunt van transparantie zou het wenselijk kunnen zijn in de kaderwet of een daaraan volgende AMvB een te geven welke soorten van gegevens door de samenwerkingsverbanden kunnen worden gewaardeerd. Daarbij zou het de voorkeur verdienen dat bij AMvB te deze vaneinde voldoende flexibel te kunnen inspelen op een eventueel behoorde de lijst van soorten gegevens aan te passen.

Voor zo'n lijst kan worden gedacht aan de volgende soorten van gegevens:

- arbeidsgegevens, zijnde gegevens waarmee aan Jov van een persoon of natuurlijke werksamenheden vastgesteld kunnen worden;
- gegevens inzake bestuursrechtelijke maatregelen en sancties, zijnde gegevens waaruit blijkt dat een natuurlijke persoon of een rechtspersoon een bestuurrechtelijke keuze uitoefend heeft gekregen dan wel dat een andere bestuurrechtelijke maatregel is getroffen;
- strafrechtelijke gegevens, zijnde gegevens als bedoeld in de Wet politiegereguleerders en de Wet justitie en strafvondelijke gegevens;
- fiscale gegevens, zijnde gegevens waarmee de fiscale verplichtingen van een natuurlijk persoon of rechtspersoon kunnen worden vastgesteld;
- gegevens roerende en onroerende goederen, zijnde gegevens waarmee het bezit en het gebruik van bepaalde goederen door een natuurlijk persoon of rechtspersoon kunnen worden vastgesteld;
- gegevens over uitsluitingsorders van bijstand of uitkeringen, zijnde gegevens waaruit blijkt dat een persoon niet in aanmerking komt voor een uitkering;
- handelsgegevens, zijnde gegevens waarmee de aard en werkzaamheden van een rechtspersoon kunnen worden vastgesteld;
- huishoudingsgegevens, zijnde gegevens waarmee de (daadwerkelijke) verblijfs- of vestigingsplaats van een natuurlijk persoon of rechtspersoon kunnen worden vastgesteld;
- identificerende gegevens, zijnde bij een natuurlijk persoon: naam, adres, voornamen, postadres, geboortedatum, geslacht, burgerservicenummer en andere administratieve kenmerken en bij een rechtspersoon: naam, adres, postadres, rechtsvorm, vestigingsplaats en administratieve kenmerken;
- inschrijvingsgegevens, zijnde gegevens waarmee kan worden vastgesteld of een persoon inschrijvingsverplichtingen zijn opgelegd;
- naelingsgegevens, zijnde gegevens waarmee de nalevingshistorie van wet- en regelgeving van een natuurlijk persoon of rechtspersoon kan worden vastgesteld;
- orderingsgegevens, zijnde gegevens waarmee de financiële ondersteuning ten behoeve van de bekostiging van onderwijs kan worden vastgesteld;
- persoonsgegevens, zijnde gegevens waarmee de persoonsgegevens kunnen worden vastgesteld;
- re-integratiegegevens, zijnde uitsluitend de gegevens waarmee kan worden vastgesteld of een persoon re-integratieverplichtingen zijn opgelegd en of deze worden nageleefd;
- schuldenlastgegevens, zijnde gegevens waarmee de eventuele schulden van een natuurlijk persoon of rechtspersoon kunnen worden vastgesteld;
- uitkeringen, toeslagen- en subsidiegegevens, zijnde gegevens waarmee de financiële ondersteuning van een natuurlijk persoon of rechtspersoon kan worden vastgesteld;
- verrekeningen en ontblijfslijnen, zijnde gegevens waarmee kan worden bepaald van welke activiteiten een natuurlijk persoon of rechtspersoon toestemming heeft gevraagd of verkregen;
- verzekeringsgegevens, zijnde uitsluitend de gegevens waarmee kan worden vastgesteld of een persoon is verzekerd voor de Zorgverzekeringswet

- d. gegevens over incidenten die hebben plaatsgevonden op het terrein van de openbare orde en veiligheid;

Wij deze lijst uit een oogpunt van transparantie en rechtszekerheid voldoende bijtellenis hebben, dien dient zij een limitatief karakter te hebben. Dat zou impliceren dat voor iedere soort van gegevens die in deze opsomming niet is genoemd maar ten aanzien waarvan in de praktijk zou gaan blijken dat zij relevant voor uitwisseling in samenwerkingsverbanden is, de AHVb aanpassing behoeft. Om op dit punt enige extra flexibiliteit te hebben, lijkt het vernutelijk in de kaderwet de mogelijkheid te waken dat aanvulling van deze opsomming bij ministeriële regeling kan plaatsvinden.

De lijst is voor het overgrote deel ontleend aan artikel 5a.1, derde lid, Besluit Surv. De opsomming in die bepaling dekt al nagenoeg volledig de soorten van gegevens die relevant kunnen zijn voor uitwisseling in samenwerkingsverbanden. Toegevoegd zijn de strafrechtelijke gegevens (onderdeel c). Deze toevoeging houdt verband met het plichtdel in § 3.7 om in de kaderwet voor alle samenwerkingsverbanden die onder de reikwijdte van de wet zouden vallen, de mogelijkheid tot verstrekking van strafrechtelijke persoonsgegevens te creëren, zodat het niet langer noodzakelijk is dat voor ieder samenwerkingsverband afzonderlijk in het Bg en het Bja te regelen. Ook zijn toegevoegd de gegevens over incidenten die hebben plaatsgevonden op het terrein van de openbare orde en veiligheid (onderdeel d). Deze toevoeging houdt verband met de wens een eventuele kaderwet mede betrekking te laten hebben op gegevensuitwisseling ten behoeve van de handhaving van de openbare orde en veiligheid (zie § 4.2).

De kaderwet zou uit een oogpunt van transparantie ook kunnen expliciteren uit welke gegevensbronnen een samenwerkingsverband mag putten. Daarlijken worden gedacht aan gegevens die anderszins zijn:

- van de deelnemers,
- uit bij wet ingestelde openbare registers,
- uit openbare bronnen,
- uit registraties met autorisatie gegevens,
- van derden, voor zover deze aansprekelijk kunnen maken dat zij rechtmatig over deze gegevens beschikken.

Deze opsomming dekt in voldoende mate de bronnen die in de praktijk worden gebruikt, met dien verstand dat bij gebruik van gegevens, anderszins onder e, de eis wordt gesteld dat de verstrekker van gegevens tegenover het samenwerkingsverband in voldoende mate aansprekelijk moet maken dat hij rechtmatig over deze gegevens beschikt. Deze eis wordt niet alleen ingegeven door het belang van transparantie over het gebruik, maar ook door het belang te voorkomen dat de verantwoordelijke voor de gegevensverwerking in het samenwerkingsverband aansprekelijk wordt gesteld voor de verwerking van gegevens die de betrokken derde anderszins heeft verzameld.

4.6 Legitieme typen van gegevensverwerking

Om de bestaande onduidelijkheid over welke typen van gegevensverwerking zijn toegestaan weg te nemen, wordt in § 3.8 aangegeven dat een kaderwet zou kunnen expliciteren dat de door deze kaderwet geregelde gegevensuitwisseling binnen samenwerkingsverbanden betrekking kan hebben op alle in de wet beschreven typen van gegevensverwerking. Deze beschrijving zou de volgende typen kunnen bevatten:

- het opstellen van rapporten waarin inzichten worden geboden of trends worden geïdentificeerd die voor het bereiken van het doel van het samenwerkingsverband relevant zijn,
- het opstellen van adviezen over acties om het doel van het samenwerkingsverband te bereiken, en het uitvoeren daarvan,
- het uitvoeren van analyses om de hiervoor bedoelde rapporten en adviezen te kunnen opstellen,
- het opstellen van profielen van groepen van personen, organisatie of bedrijven die met het oog op het doel van het samenwerkingsverband een verhoogd risico laten zien,
- het koppelen van deze profielen aan gegevens waarover het samenwerkingsverband rechtmatig de beschikking heeft, ten einde een lijst te kunnen opstellen van persoon,

- organisaties of bedrijven die met het oog op het doel van het samenwerkingsverband een verhoogd risico laten zien;
- f. het signaleren van patronen en het opstellen van risico-indicatoren voor het uitvoeren van analyses en het opstellen van profielen, of
- g. het delen van informatie, kennis en kennis in andere dan de hiervoor bedoelde vormen, voor zover dat voor het bereiken van het doel van het samenwerkingsverband relevant is.

Voor deze opnemings typen van verwerking is mede acht geslagen op bestaande vormen van gegevensverwerking in samenwerkingsverbanden en op nieuwe vormen daarvan die nog in ontwikkeling zijn, maar daar bijvoorbeeld twijfel over de toelaatbaarheid daarvan onder de huidige wetgeving, in de praktijk nog niet worden toegepast.

Waar met de onder a bedoelde rapporten bedoeld wordt op documenten met een louter beschrijvend karakter, wordt evenaangegeven dat daarvan als bedoeld onder b aanbevelingen beval, bijvoorbeeld met betrekking tot het uitvoeren van een gezamenlijke interventiestrategie. De acties waarop onderdeel c doelt, kunnen zijn opgenomen in een interventiestrategie. Het zal primair gaan om acties van de deelnemers zelf. Daarbij kan het ook gaan om acties die eventuele private deelnemers aan het samenwerkingsverband kunnen uitvoeren om de naleving van wettelijke voorschriften te bevorderen of strafbare feiten te voorkomen. Zo kunnen bestuursrechtelijke en strafrechtelijke handhaving worden aangevuld met privaatrechtelijke handhaving. Dankbaar is dat een interventiestrategie ook acties omvat die door andere organisaties dan de deelnemers zullen moeten worden uitgevoerd. Met betrekking tot alle acties waarop het advies betrekking heeft, stelt onderdeel d buiten twijfel dat de verwerking van gegevens zich ook uitstrekt tot het uitvoeren van deze acties.

De onder c en d bedoelde analyses en profielen kunnen officiële producten van een samenwerkingsverband zijn, maar uiteraard ook zijn geïntegreerd in de rapporten en adviezen die onder a en b zijn bedoeld.

De lijst, bedoeld onder e, kan het karakter van een zwaarte lijst krijgen. De implicaties van opnemingen en deroderlijke lijst kunnen fors zijn. Om die reden is bij het opstellen van een deroderlijke lijst extra voorzichtigheid geboden. De checklist die het CBP heeft opgesteld voor het opstellen van zwaarte lijsten in bedrijven of bedrijfsstakken, kan hierbij behulpzaam zijn.¹⁴³

Opmeming van deze opsomming in de kaderwet zou mede luid moeten buiten twijfel te stellen dat de onder a tot en met f genoemde typen van verwerking toelaatbaar zijn. Omdat opnemingen daarvan ook tot doel heeft een limitatieve opsomming van toelaatbare typen te geven, levert onderdeel g een restrictie op, die enerzijds uitsluitend geldt voor andere vormen van verwerking, maar deze anderzijds wel uitdrukkelijk bindt aan het doel van het samenwerkingsverband.

De kaderwet zou daarnaast moeten bepalen dat samenwerkingsverbanden ten behoeve van het signaleren van patronen en het opstellen van risico-indicatoren bestanden kunnen koppelen die zijn opgesteld op basis van van deroderlijke relevantie voor het signaleren van deze patronen of het opstellen van deze indicatoren. Aldus zou de kaderwet ook op dit punt de bestaande twijfel met betrekking tot de toelaatbaarheid van bepaalde typen van gegevensverwerking kunnen wegnemen. Daarmee zou een expliciete basis ontstaan voor vormen van "data mining", waarbij een computer met behulp van geavanceerde software bepaalde patronen kan signaleren die van belang zijn voor het opstellen van risico-indicatoren. Het kan hierbij niet gaan om analyses op basis van onoprecht verzamelde informatie; de kaderwet zou moeten voorschrijven dat het om analyses moet gaan op basis van gerichte selecties van bestanden. Uit een oogpunt van transparantie zou de kaderwet tevens moeten voorschrijven dat de selectie van bestanden op een voor het publiek toegankelijke wijze openbaar moet worden gemaakt.

4.7 Zorgvuldigheid bij verwerking

¹⁴³ Zie: http://www.cbpre.nl/downloads/overig/checklist_zwaarte_ljsten.pdf.

Wij een kaderwet gegevensuitwisseling een integrale verbetering van de gegevens uitwisseling in samenwerkingsverbanden opleveren, dan zal deze kaderwet op grond van de overwegingen in § 2.6, 3.9 en 3.12 niet alleen een verbetering van de mogelijkheden van gegevensuitwisseling moeten bieden, maar ook voorzieningen moeten bevatten die bijdragen aan de kwaliteit van de gegevens en de zorgvuldigheid bij de verwerking daarvan.

Met het oog daarop is het wettelijk in de kaderwet de volgende voorzieningen te treffen, die deels al voortvloeien uit de oude wet:

- De gegevensuitwisseling moet betrekking hebben op gegevens waarvan kan worden aangenomen dat de uitwisseling noodzakelijk is voor het doel van het samenwerkingsverband.
- Een wettelijke aantasting van de belangen van de natuurlijke personen of rechtspersonen op wie de uitwisseling van gegevens betrekking heeft, mag niet onaanvaardig zijn in verhouding tot het doel dat met de uitwisseling wordt beoogd.
- Het doel dat met de uitwisseling wordt beoogd, kan in redelijkheid niet op minder ingrijpende wijze voor de betrokken personen of rechtspersonen worden bereikt.
- Uitvoert op de verstanden is tot en met c, wordt de verwerking van gegevens zo mogelijk verstrekt plaats, voor zover dat geen onredelijke inspanning vergt en geen nadelige invloed op de effectiviteit van het samenwerkingsverband heeft.
- De onderbouwing van de wijze waarop bij een eventuele koppeling van bestanden de selectie van deze bestanden plaatsvindt, en de eventuele gehanteerde risico-indicatoren zijn openbaar gemaakt op een voor het publiek toegankelijke wijze, voor zover de openbaarmaking daarvan geen nadelige invloed op de effectiviteit van het samenwerkingsverband heeft.
- Dij de verstrekking van gegevens aan andere deelnemers wordt, waar nodig en mogelijk, aangegeven wat de graad van juistheid en betrouwbaarheid van de gegevens is, en of de gegevens zijn gebaseerd op feiten dan wel een persoonlijk oordeel.¹⁰⁴
- Vooraf de deelnemers aan het samenwerkingsverband tot verwerking van persoonsgegevens overgaan, indien zij een zijn "Privacy Impact Assessment" (PIA) uit.
- De door de deelnemers aangewezen vertegenwoordigers die betrekken zijn bij de gegevensverwerking in het samenwerkingsverband, en de medewerkers van een eventueel ondersteunend bureau zijn verplicht tot geheimhouding van de door het samenwerkingsverband ontvangen en verder verwerkte persoonsgegevens en andere gegevens waarvan redelijkerwijs is aan te nemen dat bekendmaking daarvan de belangen van de deelnemers zou schaden, behoudens voor zover de bekendmaking van het doel van het samenwerkingsverband tot bekendmaking daarvan noodsaakt.
- De deelnemers voeren, behoudens uitzonderende gevallen, acties op grond van de afgevoerde gegevens slechts uit na overleg met de deelnemers van wie de gegevens afkomstig zijn.
- De deelnemers aan het samenwerkingsverband stellen een informatieprotocol vast waarin in ieder geval de in § 4.10 genoemde onderwerpen zijn geregeld.

De clausule onder a, b en c voert, voor zover zij op persoonsgegevens betrekking hebben voort uit artikel 9 EVRM. Daarin liggen het vereiste van noodzakelijkheid en de dweluit vooraf te bepalen beginselen van proportionaliteit en substantiële verwerking. Hoewel deze al rechtstreekse gelding op basis van het EVRM hebben, lijkt het wettelijk deze in de kaderwet te expliciteren. Hiermee wordt benadrukt dat ook het gebruik van de ruimere mogelijkheden van gegevensverwerking die de kaderwet biedt, moet worden getoetst aan deze eisen.¹⁰⁵

De clausule onder d ziet op de toepassing van vormen van anonimisering en pseudonisering. Waar dat met een redelijke inspanning mogelijk is, dienen dergelijke vormen conform het principe van "Privacy by Design" te worden ingepast in het proces van gegevensverwerking. Een goede

¹⁰⁴ Deze waarborg is ook terug te vinden in artikel 6 van het voorstel voor een Europese richtlijn gegevensbescherming opgesteld in vervolg van 25 januari 2012, COM(2012)10.

¹⁰⁵ De kaderwet volgt in dit opzicht dezelfde lijn als onder andere in het nieuwe artikel 6a 1, vierde lid. Artikel 6a 1 is neergelegd.

voorbeeld hiervan is de pseudonimisering die in het proces van gegevensverwerking met behulp van SYRI plaatsvindt. Dit proces tufft in dat aan de hand van desbetreffende gegevens en met behulp van vooraf bepaalde risico-indicatoren potentiële treffers worden bepaald ten aanzien van (gepseudonimiseerde) personen die een verhoogd risico laten zien dat zij fraude plegen. Op basis van dit "hit-or-miss"-systeem worden potentiële treffers vervolgens onderzocht voor een nader analyse op naam.¹⁹⁵

De onder a opgenomen eis is bedoeld om processen van "datamining" en "profiling" een meer transparant karakter te geven. Juist bij dergelijke processen lijkt het nodig om de uitkomst van dergelijke processen beter toetsbaar te doen zijn. De openbaarmaking op een voor het publiek toegankelijke wijze kan bestaan uit bijvoorbeeld publicatie op de website van het samenwerkingsverband.

Bij gegevensuitwisseling in samenwerkingsverbanden is het bij uitstek van belang dat de context waarbinnen een gegeven is verzameld of ontstaan, zo nodig en mogelijk wordt meegegeven aan de andere deelnemers aan het samenwerkingsverband. Met het oog daarop is de onder f bedoelde eis van toepassing.¹⁹⁷

Met het onder g bedoelde "Privacy Impact Assessment" (PIA) kan op gestructureerde en transparante wijze zichtbaar worden gemaakt wat de eventuele effecten van de gegevensuitwisseling voor de bescherming van persoonsgegevens zijn. Tijdens het proces waarin de PIA wordt uitgevoerd, kunnen bepaalde elementen van de gegevensuitwisseling zo nodig worden herenvoegen om tot een betere bescherming van persoonsgegevens te komen. De eis van een PIA vloeit voort uit het Reguleringskader.¹⁹⁸ Voor het uitvoeren van een PIA op rijksniveau heeft het kabinet een toetsmodel vastgesteld, dat sinds 1 september 2013 verplicht moet worden toegepast.¹⁹⁹

Onderdeel ii bevat een geheimhoudingsplicht met betrekking tot door het samenwerkingsverband uitgewisselde en/of verwerkte gegevens. Deze plicht is zo geformuleerd dat er ruimte blijft voor de deelnemers aan het samenwerkingsverband om gegevens, zo nodig, bekend te maken bij het uitvoeren van acties op grond van analyses en adviezen die het samenwerkingsverband heeft opgesteld.

Onder i is het "gast"-principe vastgelegd. Opneming van dit principe moet – zie § 3.12 – bijdragen aan het vertrouwen dat deelnemers hebben in het gebruik van hun gegevens door andere deelnemers. Bij acties waaraan verafgoerd overleg moet plaatsvinden, kan worden gedacht aan bijvoorbeeld het stopzetten van een uitkering. Als het voorgenomen inbreken daarvan mede op gegevens van de uitkerende wordt gebaseerd, kan overleg met de politie aanleiding zijn om bijvoorbeeld de inbreuk uit te stellen, omdat dit in verband met een lopend politieverzoek de voorkeur verdient.

4.8 Verantwoordelijke

Gelet op de verantwoordelijkheidsdeling, zoals deze zich meestal in de praktijk voordoet, zou een kadervet de deelnemers aan het samenwerkingsverband als gezamenlijk verantwoordelijke in de zin van de Wbp kunnen aanwijzen, tenzij zij in het convenant anders overeenkomen. Voor dat laatste kan aanleiding zijn, indien er sprake is van afzonderlijke verantwoordelijkheid per (deel)verwerking. Dit kan de situatie bestaan dat, ook al nemen aan de verwerkingen verschillende organisaties deel, er voor één gemeenschappelijke verantwoordelijke wordt gekozen. In dat geval zal die partij wel een dusdanige positie in het samenwerkingsverband dienen te hebben dat zij deze verantwoordelijkheid kan dragen. Anders gezegd: de duidelijkheid die de

¹⁹⁵ Vgl. Kamerstukken 2012-2013, 33520, nr. 3, blz. 3 e.v. Zie ook artikel 5a.2 Besluit SUWI.

¹⁹⁶ Zie ook § 3.9 almede De Moer van Vuur, a.w., blz. 73.

¹⁹⁷ Reguleringskader VVD-PvdA van 29 oktober 2012, "Bruggen slaan", blz. 28.

¹⁹⁸ Kamerstukken II 2012-2013, 26643, nr. 282 Hierin.

keuze voor één verantwoordelijke biedt, mag niet ten koste gaan van de mate waarin aan deze verantwoordelijkheid invulling kan worden gegeven.

De gezamenlijke verantwoordelijkheid geldt uitsluitend voor de verwerking van gegevens binnen het samenwerkingverband. De deelnemers zijn en blijven ieder voor zich verantwoordelijk in de zin van de Wbp voor het "voortreccen", d.w.z. het verstrekken van gegevens aan het samenwerkingverband.¹³³

Het uitgangspunt dat partners gezamenlijke verantwoordelijke zijn, kan leidende meebrengen dat de partners hun verantwoordelijkheden onvoldoende onderkennen. Dit risico kan worden beperkt door een "regisseur" aan te wijzen die de partners ondersteunt in de uitvoering van hun rol als verantwoordelijke. De huidige praktijk kent hiervan reeds enkele voorbeelden.¹³⁴ Het gaat hier om een louter ondersteunende rol; zij neemt de gezamenlijke verantwoordelijkheid van de partners niet weg. In een eventuele kaderwet behoort zij dan ook geen expliciete regeling.

4.9 Informatieplicht

In § 4.4 is aangegeven dat in de kaderwet wordt bepaald dat de deelnemers aan een samenwerkingsverband verplicht zijn de noodzakelijke gegevens aan dat samenwerkingsverband te verstrekken. Zoals in § 3.11 al is beschreven, maakt een dergelijke bepaling het mogelijk dat niet iedere betrokken afzonderlijk zou moeten worden geïnformeerd over de verwerking van gegevens over hem of haar. Op basis van de kaderwet en het op grond van die wet verplichte convenant en informatieprotocol (zie nader § 4.10) is in algemeen zin al genoegzaam of te leiden welke gegevens ten behoeve van welk doel worden verwerkt. De kaderwet dient n verband daarmee voor te schrijven dat convenant en informatieprotocol worden openbaar gemaakt (zie §4.3 en 4.10). De kenbaarheid van de gegevensverwerking kan verder worden vergroot via de getuikelijke voorlichtingsactiviteiten op websites en door middel van brochures.

4.10 Informatieprotocol

Uit een oogpunt van "accountability" is het wenselijk dat de deelnemers zal voorschrijven dat de deelnemers aan het samenwerkingverband in een informatieprotocol een aantal elementen vastleggen die bij de gegevensverwerking in een samenwerkingsverband in het belang van gegevensbescherming van belang zijn. Omdat het daarbij niet alleen om persoonsgegevens kan gaan maar bijvoorbeeld ook om bedrijfsgegevens, wordt de term "informatieprotocol" in plaats van "privacyprotocol" gekozen.

De kaderwet zal moeten bepalen welke elementen dit informatieprotocol in ieder geval dient te bevatten. Daarbij kan worden gedacht aan de volgende elementen:

- een beschrijving van de (soorten van) gegevens die worden uitgewisseld;
- een verantwoording van de wijze waarop aan de afzender is voldaan aan het in § 4.2 uitgewoest is c.q. zal worden gegeven;
- de inrichting van het proces van gegevensuitwisseling en de waarborgen die hierin zijn opgenomen met het oog op de bescherming van persoonsgegevens;
- uitzonderingen op de verplichting tot gegevensuitwisseling (zie § 4.4);
- de bevestiging van de gegevens, met inbegrip van de autorisatie van personen die toegang tot de gegevens of aan te wijzen categorieën daarvan mogen hebben (art. 13 Wbp);
- informatieverstrekking over de gegevensuitwisseling aan het publiek en aan betrokkenen;
- de rechten van betrokkenen: inzage, correctie, verzet (art. 15, 35, 36, 40 Wbp);
- verstrekking aan derde van de omzetting daarvan;
- bewaartijdens (art. 13 Wbp);
- de verwijdering en vernietiging van bewaarde gegevens.

¹³³ Vgl. Kamerstukken II 2012-2013, 33579, nr. 3, blz. 37-38.

¹³⁴ Vgl. de regisseur die in artikel 10 Informatieprotocol REC 2011 is aangegeven.

Op grond van onderdeel a zal het informatieprotocol een nadere aanduiding moeten geven van de soorten van gegevens uit de in § 4.5 opgenomen lijst die in het samenwerkingsverband zullen worden uitgewisseld.

Bij de inrichting van het proces van gegevensuitwisseling gaat het om een beschrijving van het proces van gegevensverwerking en van het eventuele gebruik van een informatiesysteem in dat rij. Bij waarborgen voor de bescherming van persoonsgegevens die in de inrichting van het proces van gegevensuitwisseling zijn opgenomen, kan worden gedacht aan het hanteren van een getrapte vorm van overeenkomstige (eerst "hit-ne-hit"), pas bij voldoende hits uitwisseling van de inhoud van gegevens) en vormen van pseudonimisering.

Met betrekking tot onderdeel d kan worden opgemerkt dat een uitzondering op de verstrekkingplicht: zowel kan slaan op een individuele casus als op bepaalde, zeer bijzondere gegevens die in structurele zin niet aan het samenwerkingsverband worden verstrekt. Het doel van de regeling in het informatieprotocol moet zijn dat voor alle partijen vooraf helder is in welke geval en op deze uitzonderingsmogelijkheid een beroep kan worden gedaan.

Bij informatieverstrekking aan het publiek (onderdeel f) kan worden gedacht aan informatieverstrekking over het doel van het samenwerkingsverband en de categorieën van gegevens. Dit kan ook worden uitgewisseld, op websites en in brochures. Het gaat hier om informatieverstrekking in aanvulling op de voorgeschreven openbaarmaking van het convenant en het informatieprotocol. Op grond van artikel 34, vijfde lid, WvG is het niet nodig iedere persoon van wie bij het samenwerkingsverband persoonsgegevens worden verwerkt, daarvan persoonlijk op de hoogte te stellen. Wel dient betrokkene op diens verzoek te worden geïnformeerd over het wettelijk voorschrift dat tot vastlegging of verstrekking van de desbetreffende gegevens heeft geleid. Uit onderdeel f blijkt voort dat het informatieprotocol ook daarmee nationale regels dient te bevestigen.

Voor de bevordering van gegevens is het wenselijk in het informatieprotocol de richtsnoeren die het CBP daartoe heeft opgesteld, als uitgangspunt te nemen.¹²²

Het informatieprotocol zou ter uitvoering van onderdeel h kunnen bepalen dat doorverstrekking aan een derde (met inbegrip van een ander samenwerkingsverband) alleen plaatsvindt met toestemming van de partner van wie de gegevens oorspronkelijk afkomstig zijn.

Het gaat hier om een niet-uitputtende opsomming: de deelnemers aan het samenwerkingsverband kunnen desgewenst andere elementen aan het informatieprotocol toevoegen.

De kadervet zou met betrekking tot het informatieprotocol tot slot kunnen bepalen dat, het wordt gepubliceerd in de Staatscourant en overigens op een voor het publiek toegankelijke wijze openbaar wordt gemaakt.

4.11 Rechtsbescherming en toezicht

Een kadervet voor gegevensuitwisseling in samenwerkingsverbanden zou een aanvulling vormen op de bestaande wetgeving met betrekking tot verwerking van persoonsgegevens. Dit impliceert dat de bestaande rechten van personen omtrent wie een samenwerkingsverband gegevens verwerkt, onverkort in stand blijven. Dat geldt voor rechten als het inzagerecht, het correctierecht en het recht van verzet, zoals geregeld in onder andere de artikelen 33, 36 en 40 WvG of daarmee vergelijkbare rechten in specifieke wetgeving (vgl. art. 25 en 26 WvG en 18, 22 en 26 Wvrg).

Burgers dienen over voldoende informatie te beschikken om te kunnen beoordelen of voor hen aanleiding bestaat deze rechten uit te oefenen. Nu een kadervet – zie § 4.9 – het mogelijk zou,

¹²² Zie Stort, 2013, §174.

naakt dat niet iedere betrokken burger afzonderlijk zou moeten worden geïnformeerd over de verwerking van gegevens over hem of haar, is het van belang dat aan burgers wel al zekere voldoende in staat is te voorzien of zijn of haar gegevens worden verwerkt. Deze voorlichtbaarheid zal in de eerste plaats kunnen blijken uit de kaderwet zelf, de parlementaire stukken over deze wet, het convenant en het informatieprotocol. Van belang daarbij is dat convenant en protocol gepubliceerd moeten worden. De kenbaarheid van de gegevensverwerking zal verder worden vergroot door de regels die het samenwerkingsverband in het informatieprotocol moet vastleggen over de informatieverstrekking aan het publiek en aan betrokkenen. Afhankelijk van het doel van het samenwerkingsverband, is het wettelijk in het informatieprotocol te bepalen dat personen ten aanzien van wie het voornemen bestaat een bepaalde interventie te plegen, in beginsel informatie wordt verschaft omtrent de gegevensverwerking die aan de voorgenomen interventie ten grondslag ligt. Dit vergroot in belangrijke mate de transparantie van het doel en de aard van de gegevensverwerking voor de betrokken burger. Het protocol zou kunnen bepalen dat op de beginsel alleen uitzondering wordt gemaakt, indien in het protocol genoemde gronden oerbetreft aantekening, geven. Daarbij kan worden gedacht aan gronden die in artikel 43 Wbp worden genoemd.¹¹³ Het lijkt niet doeltreffend dergelijke regels ook in de kaderwet zelf vast te leggen, nu het sterk afhangt van het specifieke samenwerkingsverband of dit al dan niet adviezen over te plegen interventies afgeeft en, zo ja, in welke mate en onder welke voorwaarden betrokkenen geïnformeerd kunnen worden over de gegevensverwerking die daaraan ten grondslag ligt. Dat vereist maatwerk in het informatieprotocol. Van belang is wel dat met het oog op de belangen van betrokkenen informatieverstrekking in voldoende mate zin als uitgangspunt wordt genomen.

Aan de transparantie van de gegevensverwerking en daarmee aan de aanspreekbaarheid van het samenwerkingsverband op een zorgvuldige verwerking ("accountability") wordt verder bijgedragen door een aantal waarborgen die een aanvulling vormen op de waarborgen in de bestaande privacywetgeving. Het betreft in de eerste plaats de verplichting om de onderbouwing van de wijze waarop zij een eventuele opspeling van bestanden of selectie van deze bestanden plaatsvindt, en de eventueel gehanteerde selectiecriteria openbaar te maken (zie § 4.7). Verder valt te wijzen op de elementen die in § 4.10 worden genoemd als verplichte elementen van een op te stellen en openbaar te maken informatieprotocol. Welke waar is de wijze waarop deze elementen precies worden ingevuld, een kwestie van maatwerk per samenwerkingsverband, maar het enkele feit dat deze elementen regeling vergen, draagt bij aan de transparantie van de gegevensverwerking.

Naast de bestaande rechten van de betrokken burger en de voorzieningen in de kaderwet die de transparantie van de gegevensverwerking kunnen vergroten, kan de kaderwet ook waarborgen bevatten die anderszins aan de bescherming van persoonsgegevens zijn bijlagen. Het gaat om waarborgen, zoals die in § 4.7 zijn beschreven. De belangrijkste daarvan is wellicht de verplichting om een "Privacy Impact Assessment" (PIA) uit te voeren. Een dergelijke verplichting bestaat nu alleen op grond van een kabinetbesluit voor het rijksoverheid, maar zal in de kaderwet een wettelijke verankering voor gegevensuitwisseling in samenwerkingsverbanden krijgen en zevens gaan gelden voor deelnemers uit de kring van de medeoverheden en private partijen.

Voorts gelden uitsluitend de waarborgen voor de bescherming van persoonsgegevens, zoals die in de Wbp zijn neergelegd. Dat geldt ook voor verstrekking en dierden in landen buiten de Europese Unie, waarbij de artikelen 78 tot en met 70 Wbp in acht moeten worden genomen.

¹¹³ Ingevolge artikel 43 Wbp kan een verantwoordelijke voor de gegevensverwerking de informatieverplichtingen, bedoeld in artikel 34 Wbp, buiten toepassing laten, voor zover dit noodzakelijk is in het belang van o.a. de voorkoming, opsporing en vervolging van strafbare feiten en het toezicht op de naleving van wettelijke voorschriften. Omdat artikel 43 Wbp aan zijn toepassing kan blijven op grond van het vijfde lid van dat artikel (zie § 3.1.1), heeft artikel 43 Wbp in dit verband in eerste instantie geen relevantie. Dat neemt niet weg dat de gronden die in dat artikel worden genoemd aan informatieverstrekking een bepaalde achtergrond te betrekken, wel bruikbaar zijn voor het formuleren van gronden om een uitzondering te maken maken op een in het informatieprotocol vast te leggen informatieverplichting.

Aan de bescherming van persoonsgegevens draagt, tot slot, ook het houden van toezicht bij. Het liet oog daarop is overwogen of in de kaderwet een verlichting zou moeten worden opgenomen om periodiek een zog. privacy audit¹¹⁴ uit te voeren. Uitvoering daarvan kan immers bijdragen aan de bescherming van persoonsgegevens. Voor sommige grote organisaties als de politie is een privacy audit voor geschikter (vgl. art. 33 Wvg). Het lijkt echter te ver voeren een dergelijke verplichting ook voor samenwerkingsverbanden die onder de kaderwet vallen, in te voeren. Verschillende samenwerkingsverbanden zullen een te kleine schaal hebben om de lasten die een dergelijke verplichting metbrengt, te kunnen dragen. Het staat grotere samenwerkingsverbanden echter vrij om in een informatieprotocol de verplichting te leggen dat periodiek een privacy audit wordt uitgevoerd.

Extern toezicht vindt plaats door het College bescherming persoonsgegevens (Cbpg). Ingevolge artikel 51 Wbp houdt het Cbpg toezicht op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde. Deze taak is niet beperkt tot het terrein van de Wbp, maar strekt zich ook uit tot andere wetten, AHWA's en andere wettelijke regelingen op grond waarvan persoonsgegevens worden verwerkt. Dat geldt dus ook voor wetten waarin in aanvulling op de Wbp nadere regels zijn vastgesteld.¹¹⁵ Dit impliceert dat de verwerking van persoonsgegevens onder de werking van een kaderwet voor gegevensuitwisseling in samenwerkingsverbanden onder toezicht van het Cbpg plaatsvindt.

4.12 Verhouding tot bestaande wetgeving

In § 4.1 is als uitgangspunt gekozen voor een opzet van een kaderwet gekozen waarbij de Wbp, de Wpg, de Wvpg en de bepalingen over gegevensverwerking in sectorale wetten, op modelijk een enkele kleine aanpassing toe, in stand blijven. In deze opzet zal een kaderwet een aanvulling op deze wetten vormen, voor zover het om gegevensuitwisseling in samenwerkingsverbanden gaat.

Dit impliceert dat bepalingen uit die wetten over verstrekking van gegevens aan derden, ook in relatie tot samenwerkingsverbanden die onder de werking van de kaderwet vallen, ten betrekking blijven houden, tenzij een specifieke bepaling uit de kaderwet deze buiten toepassing verklaart. Een voorbeeld van een bepaling die haar betekenis blijft houden, is artikel 32, eerste lid, onder f, Wpg, waarin is vastgelegd dat de politie de verstrekking van persoonsgegevens aan derden schriftelijk vastlegt (protocolplicht). Een voorbeeld van bepalingen die de kaderwet in zekere tot samenwerkingsverbanden buiten toepassing zou vestoren, zijn de geheimhoudingsbepalingen in andere wetten, tenzij het om geheimhouding gaat van bijzondere persoonsgegevens anderszins strafrechtelijk gegevens (zie § 4.4). Een essentiële aanvulling die de kaderwet met betrekking tot de verstrekking van gegevens bevat, is de verplichting tot verstrekking van de noodzakelijke gegevens aan het samenwerkingsverband, voor zover daarop in het informatieprotocol geen uitzondering wordt gemaakt.

De bepalingen in de kaderwet over de verdere verwerking van gegevens in en door het samenwerkingsverband geven ten opzichte van de bestaande wetgeving vooral een aantal aanvullende randvoorwaarden. Vooral deze verwerking mag plaatsvinden. Het gaat om randvoorwaarden die slechts een beperkend karakter hebben, zoals de bepalingen die een nadere duiding geven van bepaalde typen van gegevensverwerking (zie § 4.6). Andere randvoorwaarden hebben een meer normend karakter, zoals de bepalingen met betrekking tot een zorgvuldige gegevensverwerking en de bepalingen over de inhoud van het overeenkomstig het informatieprotocol (zie respectievelijk § 4.7, 4.3 en 4.10). Ook voor deze fase van gegevensverwerking gaat het om aanvullende bepalingen. Zo blijven de bepalingen in de bestaande wetgeving waarin de rechten van betrokkenen worden geregeld (recht op toegang, correctie en recht van verzet), onverstoort in stand hangt. Welke wetgeving in dit verband geldt, hangt, zoals ook nu al het geval is, af van het antwoord op de vraag of aan het samenwerkingsverband gegevens als bedoeld in de Wpg en Wvpg worden verstrekt, en of deze

¹¹⁴ Zie het Raamwerk privacy audit (http://www.cbpgweb.nl/pages/ind_wetten_relf_compliance_raa.aspx).

¹¹⁵ Kamersnukken II 1997-1998, 25892, nr. 3, blz. 172.

binnen dat verband op geautomatiseerde wijze worden verwerkt dan wel, voor zover dat niet het geval is, in een apart bestand worden opgeslagen.¹³⁴ Is dat niet het geval, dan gelden de richtlijn, zoals neergelegd in de WvG (artt. 25 en 28) en Wvgb (artt. 18, 22 en 26). Is dat wel het geval, dan gelden de rechten die in de Wvbg zijn vastgelegd (artt. 35, 36 en 40).

In § 4.1 is al naar voren gekomen dat de kaderwet ook als een algemene aanvulling kan worden gezien op wettelijke regelingen die in specifieke gevallen samenwerking voorschrijven en daarbij regels over gegevensuitwisseling geven, zoals de in artikel 9 van de Wet Sirevi voorgeschreven samenwerking tussen het wvv, de bva en de gemeenter bij de uitvoering van die wet en enige andere wetten. Deze specifieke wettelijke regelingen blijven uiteraard onverkort hun gelding houden. Hetzelfde geldt met betrekking tot wetten die een specifiek regime bevatten voor gegevensverwerking die tot een bepaald product moet leiden. Hierbij kan in de eerste plaats worden gedacht aan de Wet Bibob, die een specifieke regeling van de gegevensverwerking bevat die tot een Bibob-advies moet leiden.¹³⁵ Een ander voorbeeld van zo'n regime is de Wvz. Ook die wet bevat een specifieke regeling van de gegevensverwerking die tot een zgn. risicobekening met betrekking tot een rechtspersoon moet leiden. Het kan uiteraard niet zo zijn dat de specifieke waarborgen die dergelijke wetten kennen om gegevens tot bepaalde producten te verwerken, te niet te doen door een samenwerkingsovereenkomst of de kaderwet op te richten met het doel op eenvoudige wijze tot dezelfde producten te komen.

Hoewel de kaderwet primair een aanvullend karakter zou hebben, zou het in het licht van deze verkenning wettelijk o.a. noodzakelijk zijn in het voorstel voor een kaderwet ook enkele aanpassingen van bestaande wetten mee te nemen.

Een eerste aanpassing die in dit verband kan worden genoemd, betreft artikel 20 Wvg. Dit artikel vormt één van de zeer weinige artikelen waarin over een samenwerkingsverband wordt gesproken. Op grond van dit artikel kan de korpschef van de nationale politie in overeenstemming met het bevoegd gezag bepaalde zelfrijdende en onbemande voertuigen inzetten, voor zover dat noodzakelijk is met het oog op een zwaarwegend algemeen belang en voor de volgende doeleinden:

- a. het voorkomen en opsporen van strafbare feiten,
- b. het handhaven van de openbare orde,
- c. het verlenen van hulp aan ien die deze behoeven,
- d. het uitvoeren van toezicht op de naleving van regelgeving.

Gelet op § 4.2 zou de verstrekking voor de doeleinden a, b en d voortaan door de kaderwet worden bestreken. De korpschef behoort voor die doeleinden geen overeenstemming met het bevoegd gezag meer te zoeken en niet te hoefden of er sprake is van een zwaarwegend algemeen belang. Die laatste twee lijn de het ware al opgesloten in de kaderwet. Om die reden zou overnemen kunnen worden artikel 20 Wvg zo aan te passen dat de in dat artikel verstaalde mogelijkheid van gegevensverstrekking alleen nog maar betrekking heeft op verstrekking voor het verlenen van hulp aan ien die deze behoeven.

Een andere bepaling waarin over samenwerkingsovereenkomsten wordt gesproken, is artikel 22, tweede lid, Wvbg. Deze bepaling geeft ruimte om gegevens die op basis van artikel 20 Wvg of artikel 39f Wvg aan een deelnemer aan een samenwerkingsovereenkomst zijn verstrekt, door deze deelnemer in het kader van een (ander) samenwerkingsovereenkomst worden doorverstrekt aan een andere organisatie. Deze bepaling kan komen te vervallen, omdat de kaderwet deze ruimte ook zal bieden.

¹³⁴ Vgl. ABW 16-7-2014, ECLI:NL:RVS:2014-2964.

¹³⁵ De Wet Bibob bevat niet alleen een specifieke regeling van gegevensverwerking die tot inzet van het Bibob instrumentarium kan leiden, in deze wet komt ook een verwijzing voor naar de 'RVC's' als samenwerkingsovereenkomsten waarvan gegevens worden verstrekt, voor zover dat noodzakelijk is voor de ondersteuning van een bestuursorgaan of een rechtspersoon met deze wettelijke taak bij het toepassen van die wet (artikel 28, tweede lid, onder d).

Buiten deze bepalingen bestaan op het niveau van wetgeving in formele zin geen bepalingen over samenwerkingverbanden die mogelijk wijziging behoeven.¹³⁹ Wel kunnen dergelijke bepalingen in lagere regelgeving voor. Gedacht kan worden aan artikel 43c, eerste lid, onder m, van de Uitvoeringswetgeving AWR. Als het tot indiening van een Voorstel voor een kaderwet komt, zal te zamen tijd moeten worden bevestigd of deze en andere bepalingen op het niveau van lagere regelgeving aanpassing behoeven.

Tot slot zijn er nog enkele andere aanpassingen van wetten nodig. Het kaderwet is in de eerste plaats een aanpassing van de Wv op Wv met het doel daarin een algemene grondslag voor verstrekking van persoonsgegevens, anderszins dan juist die en anderszins dan gegevens aan samenwerkingverbanden mogelijk te maken, voor deze onder de werking van de kaderwet vallen. Met een dergelijke grondslag is het niet meer nodig per individueel samenwerkingverband een grondslag in deze wetten of in het bpg c.q. het bpg te creëren. Verder is een aanpassing van de artikelen 120nc en 120nd van het Wv nodig die ervoor zorgen dat het niet langer nodig is een voorafgaand tot verstrekking van gegevens in te stellen, als het om een verkrijging binnen een onder de kaderwet vallend samenwerkingverband gaat.

4.13 Betreft de voor bestaande samenwerkingverbanden

In § 4.1 is al naar voren gebracht dat de kaderwet niet tot doel heeft een exclusieve regeling voor gegevensuitwisseling in samenwerkingverbanden te creëren. Het staat bestaande samenwerkingverbanden dan ook vrij ervoor te kiezen hun gegevensverwerking in te blijven rechten op grond van de thans al geldende wetgeving. Daarmee kan aanleiding bestaan, bij het toekennen voor een samenwerkingverband, geleid op naar behoeven aan informatie, niet of nauwelijks betere mogelijkheden tot gegevensuitwisseling boven de bestaande wetgeving biedt.

Tal tot de deelnemers aan een bestaand samenwerkingverband wel aanleiding te zien onder de werking van de kaderwet te willen vallen, dan zal daarvan eerst sprake kunnen zijn, ind en het samenwerkingverband aan alle randvoorwaarden voldoet die de kaderwet daarvoor stelt. Het gaat daarbij in de eerste plaats om het voldoen aan de voorwaarden die in § 4.7 zijn genoemd. Verder valt te denken aan het opstellen van een overeenkomst en van een informatieprotocol dat aan het aanpassen van een bestaand contract of informatieprotocol die aan de voorwaarden voldoen die in § 4.3 anderszins dan artikel 4.1f zijn genoemd. Pas als aan voorwaarden als deze is voldaan, kan in het convenant ook worden vastgelegd dat het samenwerkingverband onder de werking van de kaderwet valt.

4.14 Toetsing aan het EVRM

De vraag kan rijzen hoe de kaderwet zich verhoudt tot het recht op bescherming van persoonsgegevens, zoals dat geregeld is in artikel 8 EVRM. Het eerste lid van dat artikel beschermt het recht op respect voor het privéleven. Dit recht is echter niet absoluut. Ingevolge het tweede lid van artikel 8 EVRM is een inbrenging in de uitoefening van dit recht wettelijk slechts gerechtvaardigd, wanneer de inbrenging bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede ordening of voor de bescherming van de rechten en vrijheden van anderen.

Het toezicht op de naleving van wettelijke voorschriften draagt, afhankelijk van de inhoud van deze voorschriften, bij aan het economisch welzijn van ons land, de bescherming van de gezondheid of de goede ordening en aan de bescherming van de rechten en vrijheden van burgers.

¹³⁹ Wel waar wordt in 56 wetten over samenwerkingverbanden gesproken, maar in alle andere gevallen dan de Wv en Wv gaat het om samenwerkingverbanden die niet een zijn, controletoezicht van de overheid uitvoeren.

De handhaving van de openbare orde en veiligheid dient de openbare veiligheid en het voorkomen van wanordelijkheden. De voertuigen, opeparing en vervolging van strafbare feiten staat in het teken van het voorkomen van strafbare feiten. Daarmee worden alle doeleinden waarbinnen het meer specifieke doel van een samenwerkingsverband moet vallen, afgedekt door de doeleinden die artikel 8 EVRM noemt.

De eis uit artikel 8 EVRM dat de inbrenging in de uitvoering van het recht op respect voor het privéleven bij wet moet zijn voorzien, houdt in dat er sprake is van een wettelijke basis die voor de burger voldoende toegankelijk en voorsienbaar is.¹⁴⁹ Aan deze eis wordt voldaan met de in deze paragraaf beschreven kadwet en de daerop berustende bepalingen in een AMVB en ministeriële regeling, die gepubliceerd worden in het Staatsblad, respectievelijk de Staatscourant. Aan de toegerekende grondslag bij wet uit de parlementaire stukken over een kadwet als toelichting op deze wet kan worden afgeleid. De voorsienbaarheid neemt verder toe door de in de kadwet opgenomen verplichtingen om bepaalde onderwerpen in het convenant en het informatieprotocol nader te regelen en deze te publiceren in de Staatscourant en overigens op een voor het publiek toegankelijke wijze openbaar te maken.

De eis dat de inbrenging noodzakelijk is in een democratische samenleving, wordt in de jurisprudentie van het EVRM nader ingevuld met het vereiste van een dringende maatschappelijke behoefte ("pressing social need"). Of hiervan sprake is, wordt bepaald aan de hand van een aantal criteria. Zo moet een maatregel om noodzakelijk te zijn, relevant zijn om het beoogde doel te bereiken en verder moet voldaan zijn aan het proportionaliteits- en het subsidiariteitsvereiste. In algemene zin kan worden gesteld dat samenwerkingsverbanden op de terreinen die de kadwet behandelt, effectieve en efficiënte kunnen opereren, als zij gegevens kunnen uitwisselen. Sterker nog, de primaire aanleiding om een samenwerkingsverband aan te gaan, is vastel gelegen in de behoefte aan gegevensuitwisseling. Of de gegevensverwerking in een samenwerkingsverband ook in een concreet geval aan de hier genoemde vereisten voldoet, zal moeten worden getoetst bij de toetsing van het samenwerkingsverband op de inbrenging van het personen-gegevensverwerking. De kadwet zal expliciet voorzien in de verplichting de gegevensverwerking te toetsen aan het noodzakelijkheidsvereiste en de daartoe voortvloeiende beginselen van proportionaliteit en subsidiariteit.

4.15 Toelichting aan regeling van de EU

In het kadwet die een opzet kent als in de voorgaande paragrafen beschreven, past binnen de voorschriften van de Europese privacyrichtlijn. De in de kadwet gereguleerde verwerking van persoonsgegevens kan worden gekoördineerd op twee gronden uit deze richtlijn.

De eerste grond is te vinden in artikel 7, onder d, van de richtlijn. Daarin is bepaald dat lidstaten de verwerking van persoonsgegevens mogen toestaan, indien deze verwerking noodzakelijk is om een wettelijke verplichting na te komen waarvan de voor de verwerking verantwoordelijke is onderworpen. Deze bepaling is terug te vinden in artikel 8, onder c, WvG. Nu in § 4.4 wordt voorgesteld in de kadwet voor te schrijven dat deelnemers aan een samenwerkingsverband verplicht zijn de voor het samenwerkingsverband noodzakelijke gegevens te verschaffen, wordt aan deze voorwaarde voldaan. Daarmee zal ook worden voldaan aan artikel c, eerste lid, onder c, en derde lid, van het voorstel voor een Algemeen Verdrag gegevensbescherming¹⁵⁰, waarbij deze voorwaarde terugkomt. Weliswaar is de uitvoering van deze verplichting afhankelijk van een besluit van de deelnemer om aan het desbetreffende samenwerkingsverband deel te nemen, maar dat doet niet af aan het verplichte karakter van de gegevensverschikking op zich.

De tweede grond is gelegen in artikel 7, onder e, van de richtlijn. Ingevolge dat onderdeel mogen lidstaten de verwerking van persoonsgegevens toestaan, indien de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang. Met de combinatie van het doel van de

¹⁴⁹ EHRM 25 april 1979 (Sunday Times), NJ 1980, 146.

¹⁵⁰ Zie de tekst van 25 januari 2012, COM(2012)1.

gegevensuitwisseling en het noodzakelijkheidsvereiste, zoals in § 4.2, respectievelijk § 4.7 zijn beschreven, wordt aan deze voorwaarde voldaan. Daarmee zal ook worden voldaan aan artikel 6, eerste lid, onder c, en derde lid, van het voorstel voor een Algemene verordening gegevensbescherming, waarin deze voorwaarde terugkomt. De desbetreffende voorwaarde is desalniettemin getyptenleidend in artikel 8, onder c, Wbp. In dat onderdeel heeft een preciserende plaatsgevonden bij gegevensverwerking die noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt. Daarmee valt gegevensverwerking die noodzakelijk is voor de vervulling van een taak van algemeen belang in de vorm van gegevensuitwisseling met private partijen, buiten de onderdelen. Een kaderwet zal in zoverre een aanvulling op het onderdelen geven dat zij – binnen de voorwaarde uit de Europese privacyrichtlijn – ook een wijze van gegevensuitwisseling met private partijen mogelijk maakt die – zie § 3.3 – de Wbp nu niet toelaat.

In § 3.4 is naar voren gekomen dat er voorafzorging lijkt te kunnen in de omstandigheid dat de Europese privacyregulering weinig tot geen ruimte laat voor verdere versiering van persoonsgegevens voor een doel dat niet, verschijnsel is met het doel waarvoor zij zijn verzameld. Als het huidige voorstel voor een Algemene verordening gegevensbescherming wordt aangenomen, zal er meer ruimte ontstaan om bij onverenigbaarheid van doelen in een same werkingsverband tot gegevensuitwisseling over te gaan. Bij de voorbereiding van een eventuele kaderwet zal hiermee rekening moeten worden gehouden.

De vaststelling van strafrechtelijke persoonsgegevens door politie en OM aan een samenwerkingsverband valt in de toekomst onder de nieuwe riedlijn gegevensbescherming opsporings en vervolging. Ingevolge artikel 7, aanhef en nader a, van het voorstel van de richtlijn¹²³ dienen lidstaten te bepalen dat het verwerken van strafrechtelijke persoonsgegevens die onder de werking van deze richtlijn valt, slechts rechtmatig is wanneer en voor zover die verwerking noodzakelijk is voor – onder meer – het uitvoeren van een taak door een bevoegde autoriteit, op grond van een wettelijke bepaling, voor de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen. Deze bepaling geeft voldoende ruimte om door middel van de kaderwet versterking van strafrechtelijke persoonsgegevens door politie en OM aan een samenwerkingsverband mogelijk te maken, voor zover het om het voorkomen, opsporen en vervolgen van strafbare feiten gaat. Voor zover het om de overige doeleinden van de kaderwet gaat, zal een hennep kunnen worden gedaan op artikel 7, aanhef en onder b, van het voorstel van de richtlijn. Daarin is, in navolging van de Europese privacyrichtlijn, bepaald dat lidstaten dienen voor te schrijven dat verwerking van strafrechtelijke persoonsgegevens die onder de werking van deze richtlijn vallen, slechts rechtmatig is wanneer en voor zover de verwerking noodzakelijk is om – onder meer – een wettelijke verplichting na te komen waaraan de voor de verwerking verantwoordelijke is onderworpen. Bij de grond geldt dezelfde redenering als hiervoor met betrekking tot artikel 7, onder c, van de Europese privacyrichtlijn is gegeven.

¹²³ Zie de tekst van 25 januari 2012, COM(2012)10.

5. Slotbeschouwing

Een kaderwet gegevensuitwisseling samenwerkingsverbanden zal vooral op doel moeten hebben om bestaande knelpunten in de gegevensuitwisseling weg te nemen en een aantal waarborgen voor een zorgvuldige gegevensverwerking vast te leggen. Die knelpunten betreffen zowel onduidelijkheden die de bestaande wetgeving in de toepassing op samenwerkingsverbanden metrekend en die vanwege hun soms handreiking karakter niet met louter voorlichting zijn weg te nemen, als ook beperkingen die uit deze wetgeving voortvloeien. Beperkingen, zoals geheimhoudingsbepalingen, waaraan in algemene zin een grote waarde moet worden toegekend, maar die in relatie tot samenwerkingsverbanden tot onnodige belemmeringen leiden.

Een kaderwet kan dergelijke onduidelijkheden en belemmeringen wegnemen. Het betreft in de eerste plaats een betere regulerings van de verstreking van gegevens aan de deelnemers en eventueel tussen een samenwerkingsverband en van de uitwisseling met private partijen. De kaderwet zal verder praktische barrières streken om binnen een samenwerkingsverband gegevens aan politie en OM te verstrekken. Omgekeerd zal juist gelden dat strafrechtelijke gegevens voortaan gemakkelijker door politie en OM aan de andere partners in een samenwerkingsverband kunnen worden verstrekt. De kaderwet zal ook een expliciete legitimatie geven aan gegevensverwerking in de vorm van "datamining" en "profilage" om daarmee de mogelijkheden voor de opbouw van "intelligence" te verbeteren. De kaderwet zal – tot zbt – de noodzaak wegnemen om iedere persoon van wie gegevens worden verwerkt, daarvan afzonderlijk op de hoogte brengen, zonder dat daarvoor, zoals nu is vereist, de vraag moet worden beantwoord of dat een evenredige inspanning zou vergen.

Los van het wegnemen van onduidelijkheden en belemmeringen kan een kaderwet richting en steun geven aan initiatieven die worden ontplooid om tot gegevensuitwisseling te komen, maar nu vanwege de onduidelijkheden en belemmeringen soms nog stranden of volgen dat systeem het wel moet worden uitgewerkt. Ook kan met een kaderwet het signaal worden afgegeven dat er meer mogelijk is dan wordt verondersteld.

Tegenover betere mogelijkheden tot gegevensverwerking staan ook betere waarborgen voor een zorgvuldige verwerking. De kaderwet zal een aantal belangrijke beginselen met betrekking tot de bescherming van persoonsgegevens expliciteren als toetsbaar voor een goede afdoende gegevensverwerking. Te denken valt aan het vereiste dat omgekeerd moet kunnen worden dat de gegevensverwerking noodzakelijk is en voldoet aan de beginselen van proportionaliteit en subsidiariteit. Andere vereisten zijn het vereisen van gegevens waar dat met een redelijke inspanning mogelijk is en de effectiviteit niet onwettig beïnvloedt, het openbaar maken van bijvoorbeeld eventuele risico-indicatoren die men gebruikt, en het uitvoeren van een "Privacy Impact Assessment". Zo kan een kaderwet een goede optelsom laten zien van betere mogelijkheden tot gegevensuitwisseling en de nodige waarborgen voor een zorgvuldige gegevensverwerking.

De werkgroep sluit deze verkenning graag af met de opmerking dat zij niet de pretentie heeft met deze verkenning al te tot in detail te hebben doordacht, maar wel de overtuiging dat de verkenning een voldoende basis geeft om een positieve beslissing over het opstellen van een voorstel voor een kaderwet te kunnen nemen.

SAFENWERKING	DETOEKOMENDE PARTIJEN	DOEL/TOELICHTING
Nationaal Samenwerkend Centrum (NSC)	PNR, AFN, Belastingdienst, FIU-Nederland, FIOD, Nationale Politie en OM. Voor specifieke activiteiten kunnen andere partijen betrokken worden	Versterken integratie financiële sector.
Regionale Informatie- en Expertise Centra (RIEC's)	Gemeenten, provincies, Belastingdienst, Douane, Inspectie SZW, Nationale Politie, FIOD, KMAR, LRD en OM	Versterken en ondersteunen bestuurs- en enforcementaspecten van programma's en ondernemen juridisch veilig.
Regionale Coördinatie van Fraudabestrijding (RCF's)/Landelijke Interventieteams	Belastingdienst, Inspectie SZW, OM, gemeentes, SVE, OM, Nationale Politie, departementen Financiën en Sociale Zaken en Werkgelegenheid. De deelnemers kunnen per LSI-probleem verschillen.	Voorkomen en terugdringen van belasting- en fraudefraude, uitbuitingsfraude, id, illegale bewoning en in daarmee samenhangende misdrijven. Dit kan gebeuren via het netwerk, doelgroep, fenomeen of stedelijk gebied als uitgangspunt.
Veiligheidshuizen	Gemeenten, Nationale Politie, OM, Raad voor de Kinderbescherming, Reclasseringsovereenkomsten, Welzijnsovereenkomsten	Veiligheidshuizen zijn multidisciplinaire hulpverleners, die partners uit de samenleving, die zij krijgen, gemeentelijke partners en bestuur verbinden in de aanpak van complexe problematiek. Het doel van de samenwerking is het terugdringen van overlast, huiselijk geweld en criminaliteit.
Regionale samenwerkingsverbanden	Gemeenten, Nationale Politie, OM, woningcorporaties, voorkeuren, netwerkbedrijven, netwerkbureaus, UWV, SVB (partijen kunnen variëren per regio/gebied)	Integrale aanpak van netwerkwerk om complexe situaties, criminaliteit en onnodige maatschappelijke kosten terug te dringen.
Stapnet samenwerkingsverbanden	Binnenwereldrijding in netwerken, politieverbanden, gemeenten	Verhindert dat personen die zich bezighouden met gemeentelijke of criminele activiteiten, overal goed gebruiken voor criminele activiteiten.
TaskForce Straatnet Zonland	Gemeenten, provincies, OM, Nationale Politie, Rijksoverheid, Kmar,	Gedetailleerde aanpak van overblijfselen en onderliggende criminaliteit in brabant en zonland.
Maritiem Informatiecentrum (MIIC)	NWVA, DO, Douane, FIOD, RWS, ILT.	In het kader van de nationale veiligheid, het voorkomen van wanordeligheden, het bescherm van de nationale, van wetten, die voortvloeien uit de opsporing van misdrijven, het vaststellen van informatie uitbreiden en het behoeven van de bewaakt laten plaatsen.
Infobase Criminaliteit en Overheidsvermogens (ICOV)	Belastingdienst/Douane, Belastingdienst/Toelagen, Belastingdienst/Onroerend, Belastingdienst/FIOD, FIU-Nederland, Nationale Politie	In kaart brengen van overblijfselen van criminele vermogens, het blootleggen van wijlen- of fraudeconstructies en het kunnen vinden van overblijfselen van het

		ondersteuning van de publiekrechtelijke taakuitoefening van de Jeddine en de ergerijgss.
Expertisecentrum Zorgfraudestrategie en fraudevermijding N/A	NZA, KZ, Belastingdienst, IJsselme SZH, FIOD, OM, ZN, CTZ, VWS.	Versterking van de integriteit van de zorgsector door samenwerking tussen de convenantpartijen te stimuleren, te coördineren en te vergroten door het uitwisselen van informatie en het uitwisselen van kennis, inzicht en vaardigheden.
Nationaal Platform Matchfixing	FP, Belastingdienst, FIOD, Kartspelsautoriteit, Politie, KWB, NOL-Nafr, KWB, B en de Lotto.	Verbetering van de informatiepositie van alle stakeholders, zodat meer signalen worden gedetecteerd, meer signalen tijdig via de juiste kanalen bij de juiste stakeholders terecht komen en de meest passende interventie kan worden ingezet.
Hit and Run Carpoeam (HARC)	Douane, FIOD, Zeehavenpolitie.	Onderzoek naar de invoer, uitvoer en doorvoer van verdovende middelen in het ha verplaats.
Contraterrorisme Infolux (CI-infoboo)	ANVD, MIVD, Nationale Politie, IND, FIJ-Nederland, OM.	Leveren van een bijdrage aan de bestrijding van terrorisme door het op een centraal punt bij elkaar brengen en vergelijken van informatie over netwerken en personen die op één of andere wijze betrokken zijn bij terrorisme, in het bijzonder islamistisch terrorisme, en de daaraan te relateren radicalisering.
Electronic Crimes Taskforce (ECTF)	Nationale Politie, Landelijk Parket, benr en Concreter Protection of the National Infrastructure (CPNI).	Veilig en betrouwbaar beleidsproces is van groot belang voor de stabiliteit en integriteit van het financiële stelsel. De samenwerking in de ECTF brengt daarvoor unieke en specifieke kennis, informatie en ervaringen samen. Dit zorgt voor betere analyses en versterking van de informatiepositie om cybercrime aan te pakken.
Landelijk Informatiecentrum Voorzorgcriminaliteit	RDU, Nationale Politie, de Stichting Verkeersgegevens voorzorgcriminaliteit (VVG) en de Belastingdienst.	Informatie- en kenniscentrum dat een bijdrage levert aan de opsporing en bestrijding van voorzorgcriminaliteit door vroegtijdige signalering van de potentiële criminaliteit.
Landelijk Schimmingspunt	Minister V&L, Nationale Politie, OM, NVB, Equitas SE, Belastingdienst Nederland.	Publiek-private bestrijding van fraude door schimming.
Nationaal Platform Criminaliteitsbeheersing/ Regionale Platform Criminaliteitsbeheersing	Minister van V&L, Minister EZ, VNC/NOW, MIVD-Nederland, Nederlandse Vereniging van Banken, Koninklijke Marechaussee Nederland, VNS, Verbond van Voorzorgsinstellingen, CH, Detailhandel Nederland.	• Bestuderen en analyseren van de criminaliteitspatronen die de Nederlandse samenleving en in het bijzonder het Nederlandse bedrijfsleven bedreigen; • Versterken van de beveiligingsfunctie in de breedste zin van bedrijven en installaties door middel van bijvoorbeeld scholing, deskundigheid, bevordering, voorlichting en certificatie en normalisatie en certificatie van

		beveiligingsproducten en -diensten; • Bijdragen aan een effectieve preventie en rechts handhaving met betrekking tot zaken het bedrijfsleven gerichte criminaliteit door middel van advisering van de Ministers van V&J en EZ, het OM, het binnenlands bestuur en de politie; • Bevorderen van de onderlinge samenhang tussen de beveiligingsspanningen van het bedrijfsleven en de rechts handhavingsspanningen van de overheid ter verhoging van hun doelmatigheid en effectiviteit door middel van advisering over bijvoorbeeld prioriteitenstelling en het opzetten van proefprojecten.
Convenant aanpak crim- en plekfraude	Dankens, de Nationale Politie en OM.	Door het ander uitwisselen van informatie bestaat er sneller en beter inzicht in trends en gebruikte modus operandi van potentiële daders. Hierdoor worden voorzorgsmaatregelen gebouwd en wordt de opsporing makkelijker.
Convenant aanpak verzekeringsfraude	Verbond van Verzekeraars, Zorgverzekeraars Nederland, OM en Nationale Politie.	Terugdringen van verzekeringsfraude door: 1. beter zicht te krijgen op verzekeringsfraude; 2. te komen tot een integrale, programmatische aanpak, bestaande uit preventie, detectie, divisionele en strafrechtelijke afhandeling en 3. het proces van meldingen, aangiftes en strafrechtelijke afhandeling te stroomlijnen.
Landelijk Meldpunt Internetoplichting	Nationale Politie, Rahobank, ADR-AMRO, ING, SNS (alle verenigingsvoorzitter door NIVB), en OM.	Zicht op aard en omvang van oplichting in het online private handelsverkeer, te weten te komen tot integrale preventie, detectie en strafrechtelijke afhandeling, stroomlijnen van proces van meldingen, aangiftes en strafrechtelijke afhandeling.
Surwint-inszijk	Verschillen bronnen (Geme, DUO, Kadaster, RDW) en gebruikers (gemeente, SVB, UWV).	Surwint-inszijk biedt overheidsorganisaties de mogelijkheid om voor hun wettelijke taaktoewijzing gegevens van burgers die bij andere overheidsorganisaties of basissettings zijn opgenomen, te raadplegen in een wettelijke setting.
Inspectievisie Milieu	Partijen bestaan uit broshouders en gebruikers. Sinds november 2013 hebben de volgende partijen een	Verbreiden aanpak milieuovertredingen. Gegevens worden door middel van inspectievisie Milieu uitwisseld.

	aansluitovereenkomst getekend: ITT, RIVM/A, Insectie SZW, DCMR (omgevingsdienst) en OZHE (omgevingsdienst).	vermerkt ten behoeve van vergunningverlening aan, verwerken van meldingen van en toezicht op bedrijven en andere organisaties die activiteiten verrichtten waarop de milieuwetgeving van toepassing is elkmede het handhaven in verband daarmee van wettelijke voorschriften.
Convenant samenwerking en informatie-uitwisseling bestrijding geweldadige vermogenscriminaliteit gericht op de financiële sector	Rabobank, SNS, ING, ABN- AMRO, Nationale Politie en OVG	Uitbouwen samenwerking tussen publieke en private partijen met het oog op de bestrijding van gewelddadige vermogenscriminaliteit gericht op de financiële sector. Het convenant beheft de vastlegging van de wens om binnen de wettelijke kaders en gelet op het publieke en/of maatschappelijke belang en verantwoordelijkheid die elk der convenantpartners in het kader van de voorkoming en bestrijding van deze vorm van criminaliteit heeft, unieke en organisatie-specifieke kennis, informatie en expertise met elkaar te delen.