

Vergaderjaar 2014–2015

32 761

Verwerking en bescherming persoonsgegevens

Nr. 79

BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 19 december 2014

1. Inleiding

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 rechtsgevoel. Het kabinet wil de aanpak van fraude versterken. Dit vergt een brede en integrale benadering. Zo'n brede en integrale benadering vereist een efficiënte en doeltreffende samenwerking van alle betrokken partijen. Daarvoor is uitwisseling van informatie essentieel. Alleen dan kunnen partijen tot zo effectief mogelijke en op elkaar afgestemde interventies komen. Dit heeft tot gevolg dat overheidsorganisaties sinds een aantal jaren in toenemende mate in multidisciplinaire samenwerkingsverbanden opereren om aan die brede en integrale aanpak gestalte te geven. 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. Deze ontwikkeling van intensivering en verbreding van de samenwerking tussen diverse organisaties bij het voorkomen en bestrijden van fraude heeft ook scherper zicht gegeven op grenzen en belemmeringen waar uitvoerende organisaties op stuiten als het gaat om het uitwisselen van de voor die samenwerking noodzakelijke gegevens. Tegelijkertijd is van belang om te benadrukken dat, als wordt bezien of dergelijke belemmeringen kunnen worden weggenomen, rekening moet worden gehouden met bepaalde belangen, zoals het recht op bescherming van persoonsgegevens. Bovendien moet rekening worden gehouden met grenzen die op Europees niveau aan gegevensuitwisseling worden gesteld.

Het kabinet heeft in de brief van 19 december 2013 over de kabinetsbrede aanpak over de fraude aangekondigd in 2014 een verkenning uit te voeren naar een kaderwet voor de gegevensuitwisseling op het terrein van fraudebestrijding (Kamerstuk 17 050, nr. 496). De verkenning zou een antwoord moeten geven op de vraag of zo'n kaderwet generieke knelpunten met betrekking tot de gegevensuitwisseling in bestaande wetgeving kan oplossen in plaats van het aanbrengen van afzonderlijke wijzigingen in specifieke wetten.¹ Deze verkenning is thans gereed en als bijlage bij deze brief gevoegd².

De verkenning heeft betrekking op gegevensuitwisseling op een breder terrein dan fraudebestrijding. Een eerste reden die in de verkenning daarvoor wordt aangedragen, is dat de meeste samenwerkingsverbanden die zich met de aanpak van fraude bezighouden, ook andere taken hebben. Een andere reden is dat een eventuele kaderwet evenzeer van belang kan zijn met het oog op knelpunten bij gegevensuitwisseling op andere terreinen. Volgens de verkenning zou beter kunnen worden gekozen voor een kaderwet voor de gegevensuitwisseling binnen samenwerkingsverbanden voor specifieke doelen op het brede terrein van de voorkoming van onrechtmatig gebruik van overheidsgelden 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 samenwerkingsverbanden manifesteren die gegevens binnen en tussen het bestuursrechtelijke en strafrechtelijke domein willen uitwisselen. Hierbij valt te denken aan samenwerkingsverbanden op het terrein van de aanpak van de georganiseerde criminaliteit, de bestrijding van hennepsteelt, de aanpak van verschillende vormen van fraude (uitkeringsfraude, vastgoedfraude, verzekeringsfraude, zorgfraude etc.) en de bestrijding van milieucriminaliteit, cybercrime en voertuigcriminaliteit. Het kabinet kan zich in deze brede reikwijdte goed vinden.

Uit de verkenning blijkt dat de geconstateerde knelpunten in belangrijke mate verband houden met het feit dat de huidige wetgeving niet altijd voldoende rekening houdt met het bestaan van samenwerkingsverbanden van verschillende partijen binnen de overheid en soms ook partijen uit de private sector en met de behoefte aan gegevensuitwisseling in dergelijke verbanden. Dit hangt voor een belangrijk deel samen met het feit dat de huidige wetgeving vooral betrekking heeft op gegevensverwerking binnen bepaalde sectoren of organisaties. Voor zover deze wetgeving verstrekking van gegevens door deze sectoren of organisaties aan derden mogelijk maakt, betreft het in verreweg de meeste gevallen verstrekking aan een specifieke functionaris of organisatie. Dit roept in de praktijk vragen op met betrekking tot verstrekking van gegevens aan samenwerkingsverbanden. Bij voorbeeld de vraag in hoeverre bepalingen die de verstrekking aan individuele organisaties mogelijk maken, ook een voldoende grondslag kunnen vormen voor verstrekking aan alle deelnemers van een samenwerkingsverband tegelijk, aan een samenwerkingsverband als zodanig of aan een bureau dat zo'n verband ondersteunt. De huidige wetgeving geeft op vragen als deze niet altijd voldoende duidelijkheid. Ook de basis voor verdere verwerking van gegevens in en door samenwerkingsverbanden is niet steeds duidelijk. Gelden daarvoor de desbetreffende sectorale wetten of een algemene wet als de Wet bescherming persoonsgegevens? Tot slot valt erop te wijzen dat uit het doel van de meeste samenwerkingsverbanden voortvloeit dat

¹ Kamerstuk 17 050, nr. 450, blz. 7–8.

² Raadpleegbaar via www.tweedekamer.nl

zij gegevens van deelnemende partijen met elkaar in verband willen brengen voor een gemeenschappelijke analyse. Zij hebben daarbij in toenemende mate behoefte aan het gebruik van moderne analysetechnieken met betrekking tot grote hoeveelheden gegevens. Waar de huidige wetgeving voor individuele organisaties soms al vragen met betrekking tot het gebruik van dergelijke technieken oproept, geldt dat zeker voor samenwerkingsverbanden, nu deze niet of nauwelijks een plek in bestaande wetgeving hebben.

Het gaat om vragen die blijkens de praktijk zich niet met uitleg van de huidige wetgeving laten oplossen en daardoor een rem op de uitwisseling en verdere verwerking van gegevens in samenwerkingsverbanden vormen. Dat belemmert op haar beurt een optimale aanpak van de problemen waarvoor een samenwerkingsverband in het leven is of wordt geroepen. Nu een integrale aanpak van fraude en andere vormen van criminaliteit in de recente jaren in de praktijk meer en meer vorm krijgt, zijn ook de belemmeringen die worden ervaren als gevolg van de bestaande (inrichting van) wet- en regelgeving pregnanter zichtbaar geworden. Tegelijkertijd realiseert het kabinet zich dat wat in de praktijk als een knelpunt wordt ervaren, omgekeerd een beperking van de mogelijkheden van gegevensverwerking kan inhouden die als een waarborg voor de bescherming van specifieke belangen, zoals de bescherming van persoonsgegevens, moet worden aangemerkt. Bij de weging van de in de verkenning geconstateerde knelpunten en voorgestelde oplossingsrichtingen zal het kabinet hiermee rekening houden.

Belemmeringen die uit de bestaande wetgeving voortvloeien, zijn bijvoorbeeld zichtbaar bij de zgn. subjectgerichte aanpak. In deze aanpak is men gestuit op een beroepsfraudeur die reeds tien jaar geleden voor het eerst opviel. Hij pleegt domein overstijgende fraude. Er zijn signalen dat er sprake is van faillissementsfraude, belastingfraude, arbeidsuitbuiting en fraude in de transportsector. Dit betekent dat er minimaal vier verschillende organisaties betrokken zijn, namelijk de FIOD/Belastingdienst, de Inspectie SZW, de Inspectie Leefomgeving en Transport en het OM (Functioneel Parket). Tijdens de behandeling van deze casus is geconcludeerd dat de regelgeving over gegevensuitwisseling grote verschillen toont per deelnemende organisatie. Daarnaast is de regelgeving over gegevensuitwisseling erg complex en multi-interpretabel en blijkt regelgeving de gegevensuitwisseling tussen bepaalde partijen/domeinen/regimes niet altijd toe te staan. Dit leidt tot een traag en inefficiënt proces. De deelnemende partijen kunnen hun informatie pas delen, nadat de privacy-experts van de verschillende organisaties hebben onderzocht of dit mogelijk is. Ook is er een mogelijkheid dat niet elke vorm van criminaliteit kan worden aangepakt, omdat de gegevensuitwisseling niet is toegestaan.

2. Knelpunten en oplossingsrichtingen uit de verkenning

Tegen deze achtergrond worden in de verkenning verschillende generieke knelpunten geconstateerd. Het kabinet geeft hierna de voornaamste knelpunten weer met de oplossingsrichtingen die in de verkenning daarvoor worden aangereikt. Het gaat daarbij om knelpunten die – zo blijkt uit de verkenning – vooral zijn geconstateerd in relatie tot de volgende samenwerkingsverbanden: de Regionale Informatie en Expertise Centra (RIEC's), de Infobox Crimineel en Onverklaarbaar Vermogen (iCOV) en het Financieel Expertise Centrum (FEC). Gelet op de aard van deze knelpunten, zijn zij exemplarisch voor verschillende andere samenwerkingsverbanden. Zij komen bovendien terug in verschillende rapportages en onderzoeken, zoals in het rapport van de Commissie Joldersma inzake

verwevenheid van de bovenwereld met de onderwereld³ en de Rapportage van de Landelijk Coördinator Verwevenheid boven- en onderwereld⁴. Zij worden verder herkend en onderschreven door verschillende professionals die werkzaam zijn in de dagelijkse uitvoeringspraktijk, zoals in de diverse pilots in het kader van het bestrijden van fraude die zijn gestart door de gemeente Amsterdam en het (burger)initiatief 1overheid⁵, en in de integrale uitvoeringsprogramma's van de TaskForce Brabant Zeeland, die zijn gericht op het effectief verstoren van de criminele industrie in die provincies. Overigens tekent het kabinet hier al aan dat het zich bij de voorbereiding van eventuele wetgeving om in de verkenning geconstateerde knelpunten weg te nemen, niet wil vastleggen op vormgeving daarvan in de vorm van een kaderwet. Het kabinet wil op dit punt uitdrukkelijk verschillende opties openhouden, waarop aan het slot van deze brief nog zal worden teruggekomen. Als hierna met een verwijzing naar de verkenning over een kaderwet wordt gesproken, dient met deze kanttekening dan ook rekening te worden gehouden.

Geheimhoudingsbepalingen

De geheimhoudingsbepalingen in verschillende wetten staan een optimale gegevensuitwisseling in samenwerkingsverbanden in de weg. Deze bepalingen gaan voor verstrekking van gegevens aan andere partijen uit van: nee, tenzij (er goede redenen zijn tot verstrekking over te gaan). De praktijk in samenwerkingsverbanden heeft behoefte aan: ja, tenzij (er goede redenen zijn gegevens geheim te houden). Het doel van een samenwerkingsverband zal uiteraard een voldoende rechtvaardiging moeten geven om «ja, tenzij» als uitgangspunt te hanteren. De doorbreking van de geheimhoudingsplichten zou niet moeten gelden voor plichten die betrekking hebben op zgn. bijzondere persoonsgegevens, zoals gegevens over iemands gezondheid, omdat deze extra privacygevoelig zijn. Op dit uitgangspunt zou dan wel weer een uitzondering moeten worden gemaakt voor strafrechtelijke gegevens, omdat dergelijke gegevens bij uitstek relevant kunnen zijn voor samenwerkingsverbanden op het brede terrein waarop een eventuele kaderwet betrekking zou hebben. Verder zou rekening moeten worden gehouden met specifieke belangen die met een geheimhoudingsplicht verband houden. Zo kan van afschaffing van bijvoorbeeld de fiscale geheimhoudingsplicht geen sprake zijn. Tot slot geldt dat uiteraard ook rekening moet worden gehouden met geheimhoudingsbepalingen die voortvloeien uit Europese regelgeving.

Gegevensverstrekking aan samenwerkingsverband en aan ondersteunend bureau

Voor gegevensverstrekking in een samenwerkingsverband aan alle deelnemers tegelijk en aan een bureau dat het samenwerkingsverband eventueel ondersteunt, bestaat vaak geen goede grondslag. Om die reden wordt in het FEC niet uitgegaan van verstrekking door een partner van het FEC aan het samenwerkingsverband als geheel, maar aan alle afzonderlijke partners (bilaterale verstrekking). Dit komt doordat het FEC als zodanig geen juridische status heeft. Hetzelfde geldt met betrekking tot de FEC- eenheid als ondersteunend bureau. Dit heeft tot gevolg dat iedere partner per ingebracht signaal moet beoordelen wie wel of niet aan tafel mag zitten als het signaal besproken wordt.⁶ Vanuit de visie dat alle partners van het FEC een gezamenlijke taak ten aanzien van de integriteit van de financiële sector hebben en derhalve informatie (kunnen) hebben

³ Kamerstuk 29 911, nr. 14.

⁴ Kamerstuk 29 911, nr. 84.

⁵ Zie www.1overheid.nl.

⁶ Zie ook kamerstuk 33 632, nr. 4, blz. 17–19.

die van belang is voor het verrijken van een signaal, zou ook een andere oplossing overwogen kunnen worden. Zo kan een kaderwet ervoor zorgen dat samenwerkingsverbanden een juridische status krijgen en regelen dat de verstrekking plaatsvindt aan alle partners van het samenwerkingsverband als geheel en aan een eventueel ondersteunend bureau.

Gegevensuitwisseling met private partijen

Publiek-private samenwerking bij fraudebestrijding en de aanpak van andere vormen van criminaliteit levert beide kanten voordeel op. Zo hebben banken goed zicht op klanten met een verhoogd risico op fraude. Hun informatie kan om die reden zeer relevant zijn voor partners in het FEC. Andersom kan de informatie van de FEC-partners voor de banken van belang zijn. Op basis daarvan kan de bank bijvoorbeeld bepaalde dienstverlening stopzetten. Dit kan soms effectiever zijn dan bijvoorbeeld het starten van een opsporingsonderzoek. Het antwoord op de vraag of en de mate waarin gegevensuitwisseling met private partijen mogelijk is, verschilt per sectorale wet. Dit geldt ook met betrekking tot het FEC. Een eventuele kaderwet kan bijdragen aan het vergemakkelijken van de gegevensuitwisseling met dergelijke partijen.

Gegevensverstrekking door politie en OM

De bestaande mogelijkheden voor verstrekking van gegevens in een samenwerkingsverband door politie en OM zijn niet optimaal. Dat moet nu, met gebruikmaking van de artikel 18, 19 of 20 van de wet Politiegegevens, per samenwerkingsverband afzonderlijk worden geregeld. Daarbij is vereist een zwaarwegend algemeen belang. Dit vereiste geldt eveneens voor de verstrekking van justitiële of strafvorderlijke gegevens door het Openbaar Ministerie (art. 8a en 39f Wjsg). Een eventuele kaderwet kan een generieke grondslag voor verstrekking van dergelijke gegevens aan samenwerkingsverbanden bieden, zodat het in voorkomende gevallen niet meer nodig is daarvoor een afzonderlijk besluit te nemen of een afzonderlijke regeling te treffen.

Voor verstrekking van zgn. CIE-gegevens aan de RIEC's bleek eerst een machtigingsbesluit op grond van artikel 18 van de Wet Politiegegevens nodig te zijn. Teneinde een structurele voorziening te creëren, wordt dit machtigingsbesluit gevolgd door een wijziging van het Besluit politiegegevens. Dit zijn tijdrovende trajecten, die de slagvaardigheid van samenwerkingsverbanden onnodig belemmeren.

Gegevensverkrijging door politie en OM

Voor verkrijging van gegevens door politie en OM binnen een RIEC is nu vaak nog een vordering op grond van artikel 126nc en 126nd Wetboek van Strafvordering nodig. Dit is een omslachtige procedure, die de uitwisseling van gegevens in het zgn. informatieplein bemoeilijkt. Een eventuele kaderwet kan regelen dat een vordering niet meer nodig is.

Gebruik moderne analysetechnieken

Er bestaat teveel onduidelijkheid over de toelaatbaarheid van het gebruik van moderne analysetechnieken als «datamining» en «profiling» door samenwerkingsverbanden. Dat zet een rem op het gebruik daarvan, terwijl moderne analysetechnieken een belangrijke bijdrage kunnen leveren aan het doel waarvoor het samenwerkingsverband in het leven is geroepen. Zo heeft iCOV het voornemen een profiel van beroepsfraudeurs te ontwikkelen, maar zou het zo'n profiel op basis van de huidige wetgeving

niet kunnen matchen met alle data waarover zij rechtmatig de beschikking heeft. Hierdoor kan er geen lijst gegenereerd worden van personen met een bijzonder groot risico dat zij fraude (gaan) plegen. Een eventuele kaderwet kan regelen dat deze vormen van gegevensverwerking onder bepaalde voorwaarden zijn toegestaan.

Een beroepsfraudeur fraudeert op grote schaal en structureel. Hij zet een organisatorische of administratieve structuur op met als doel frauduleuze voornemens ten uitvoer te brengen en de ware aard daarvan te verhullen. Een voorbeeld in het kader van faillissementsfraude is dat een beroepsfraudeur een bijna failliete BV opkoopt en aan het hoofd van die BV een katvanger als directeur/aandeelhouder zet. Vaak zijn dat mensen zonder inkomen of vermogen, bij wie dus niets te halen valt. Vervolgens wordt deze BV geheel leeg getrokken en worden bestellingen op naam van de BV gedaan die nooit worden betaald. Dit patroon kan mogelijk uit de verschillende data worden gedestilleerd, door te kijken naar het Handelsregister, fiscale activiteiten van (rechts)personen, maar ook of iemand eerder in aanraking is geweest met justitie.

Informatieverstrekking aan betrokkenen

De wetgeving verplicht samenwerkingsverbanden in beginsel om iedere individuele burger over wie gegevens worden verwerkt, daarover te informeren. Dat vergt veel inspanning, terwijl informatieverstrekking aan burgers in meer algemene zin op bijvoorbeeld een website ook al voldoende kan bijdragen aan transparantie van de gegevensverwerking voor de burger. Een eventuele kaderwet kan in het licht van artikel 34, vijfde lid, van de Wet bescherming persoonsgegevens ervoor zorgen dat samenwerkingsverbanden met een dergelijke wijze van informatieverstrekking volstaan.

3. Dilemma's

Het kabinet herkent deze knelpunten en wil zich ervoor inspannen deze door middel van wetgeving weg te nemen. Het kabinet realiseert zich met het oog op de genoemde knelpunten echter goed dat kabinet en Kamer nadrukkelijk aandacht zullen moeten schenken aan de vraag waar de grenzen liggen bij gegevensuitwisseling. Wat in de praktijk als een knelpunt wordt ervaren, kan, zoals eerder al is opgemerkt, immers een beperking van de mogelijkheden van gegevensverwerking inhouden die als een waarborg voor de bescherming van persoonsgegevens moet worden aangemerkt. Er moet om deze reden een goede afweging worden gemaakt tussen de belangen die worden gediend met een breder gebruik van gegevensuitwisseling en de in (internationale) regelgeving vastgelegde kaders ter bescherming van de privacybelangen van de burger. Dat deze afweging noodzakelijk is, is recent nog gebleken bij de vragen die vanuit de Eerste Kamer en Tweede Kamer zijn gesteld over het verzamelen van gegevens door de Belastingdienst en het uitwisselen van die gegevens met andere overheidsorganisaties⁷ en over het gebruik van SyRI⁸. In een discussie over de verbetering van de mogelijkheden van gegevensuitwisseling door een kaderwet zullen de relevante belangen dus scherp in beeld moeten zijn ten behoeve van een verantwoorde belangenafweging en besluitvorming. Het kabinet is het met deze zienswijze uit de verkenning eens. De verkenning bevat ten behoeve van deze belangenafweging al de eerste bouwstenen. Het kabinet wil tegen die achtergrond in

⁷ Zie kamerstuk 32 761, nr. 71.

⁸ Zie Aangangsel Handelingen II 2014/15, nrs. 428 en 429.

deze brief specifiek aandacht geven aan een vijftal dilemma's die met de geconstateerde knelpunten samenhangen.

Geheimhoudingsplichten

Het eerste dilemma betreft de bestaande geheimhoudingsplichten. Zoals ook uit de verkenning naar voren komt, zijn deze plichten ingegeven vanuit verschillende belangen. Daarbij kan het onder meer gaan om het recht op bescherming van de persoonlijke levenssfeer, bescherming van bedrijfsgeheimen, bescherming van publieke belangen (veiligheid van de staat), bescherming van de bijzondere positie van bepaalde ambten (onschendbaarheid Koning) en de zorg voor de goede werking van het openbaar bestuur (mogelijkheid van intern beraad, geheimhouding van een bepaalde werkwijze, het belang van inspectie, toezicht en controle door bestuursorganen).

In de verkenning wordt terecht erop gewezen dat voor organisaties die betrokken zijn bij gegevensuitwisseling in samenwerkingsverbanden, het recht op bescherming van de persoonlijke levenssfeer, de bescherming van bedrijfsgeheimen en de zorg voor de goede werking van het openbaar bestuur het belangrijkste zijn. Het gaat om organisaties als de gemeenten, politie, het OM, bijzondere opsporingsdiensten, de Belastingdienst, de douane, inspecties etc. De bescherming van private belangen is overigens niet alleen een 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 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 overheidsinstanties zich onderling 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 het dienen van een bepaald deelbelang binnen het openbaar bestuur, zoals de correcte belastingheffing of de bewaking van de soliditeit van banken.

Voor de dilemma's met betrekking tot de geheimhoudingsplicht wordt in de verkenning in het bijzonder stil gestaan bij de geheimhoudingsplicht van de Belastingdienst. Deze geheimhoudingsplicht strekt vanouds ertoe dat de belastingplichtige niet wordt belemmerd de voor de goede belastingheffing relevante gegevens aan de Belastingdienst te verstrekken in de wetenschap dat de Belastingdienst deze gegevens in beginsel niet aan derden verstrekt. Alleen al om die reden kan van afschaffing van de fiscale geheimhoudingsplicht geen sprake zijn. Naast het belang van het heffen van de juiste belasting is met deze plicht het privacybelang van de burger gediend. Wat betreft het aanleveren van gegevens door ondernemingen is het belang van deze plicht hierin gelegen dat fiscale gegevens veelal bedrijfsgeheimen omvatten, zoals productieprocessen, winstmarges, omzetten en dergelijke. Met zorgvuldige verwerking van dergelijke gegevens door de Belastingdienst is derhalve de juiste belastingheffing en uiteindelijk het belang van Nederland als gunstig vestigingsland voor het internationale 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.

Het kabinet is van mening dat bij het bepalen van een standpunt over verder gaande vormen van gegevensuitwisseling in samenwerkingsverbanden de hier bedoelde belangen van de bestaande geheimhoudingsbepalingen goed dienen te worden afgewogen. Deze bepalingen hebben echter ook nu al geen absoluut karakter. Waar het op aan komt is het vinden van de juiste balans tussen de belangen van geheimhouding en het belang van gegevensuitwisseling. Het kabinet onderzoekt of die balans gevonden zou kunnen worden door in de betrokken sectorale wetten te regelen dat gegevens aan door een algemene wettelijke regeling gereguleerde samenwerkingsverbanden kunnen worden verstrekt, met dien verstande dat deze wetten daarop uitzonderingen kunnen formuleren dan wel de verstrekking aan nadere voorwaarden verbinden. Aldus moet in voldoende mate rekening worden gehouden met de specifieke belangen die bij een geheimhoudingsplicht in een sectorale wet een rol spelen. Het kabinet onderzoekt hier een andere weg dan waarvoor in de verkenning is gekozen. Met de daarin gemaakte keuze voor een algemene buiten toepassing verklaring van geheimhoudingsbepalingen in een kaderwet kan immers onvoldoende rekening met die specifieke belangen worden gehouden. Komende tijd wordt dit bekeken en zal duidelijk moeten worden of de belangen die spelen bij geheimhouding van gegevensuitwisseling, zoals de bescherming van bedrijfsgeheimen, voldoende gewaarborgd kunnen worden.

Vorderingsplicht van politie en OM

Een tweede dilemma waarvoor het kabinet aandacht wil vragen, betreft de bevoegdheid tot het vorderen van gegevens door politie en OM ten behoeve van de opsporing van strafbare feiten, op grond van artikel 126nc en 126nd Sv. Uit de wetsgeschiedenis vloeit voort dat sprake is van een gesloten stelsel, waarbij het de politie c.q. de officier van justitie in beginsel niet vrij staat om vrijwillige verstrekking van de gegevens te vragen maar gehouden is de gegevens te vorderen. De ratio voor een dergelijke vordering is dat de derde bij wie de gegevens worden gevorderd, 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. In de verkenning wordt terecht erop gewezen dat bestuursorganen die aan samenwerkingsverbanden deelnemen, evenwel in het algemeen veel beter dan willekeurige derden in staat zijn tot het maken van een afweging over de verstrekking, omdat zij veelal wel enige kennis dragen van de achtergronden van het verzoek. Mocht het onder omstandigheden zo zijn dat een bestuursorgaan onvoldoende kennis over de achtergrond van het desbetreffende verzoek bezit 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 in de verkenning genoemde mogelijkheid in het informatieprotocol vast te leggen dat het van verstrekking kan afzien.

Een vraag die in dit verband ook aandacht verdient, is wat de opsporingsdiensten en het OM vervolgens met de ontvangen gegevens mogen doen. Zo zou bepaald kunnen worden dat gegevens die deze instanties zonder vordering verkrijgen, door hen alleen mogen worden gebruikt voor uitvoering van acties die zijn gebaseerd op adviezen die de gezamenlijke deelnemers in het kader van het samenwerkingsverband hebben opgesteld. Verder zou kunnen worden besloten dat, indien het OM mede op basis van de ontvangen gegevens een vervolging wil starten, deze gegevens daarvoor alleen mogen worden gebruikt met instemming van de betrokken instantie. In beide gevallen staan twee wegen open: de

wetgever regelt dit of de deelnemers regelen dit desgewenst zelf in het informatieprotocol. Het kabinet wil bij de nadere uitwerking in wetgeving bezien welke weg moet worden ingeslagen om tot een afgewogen regeling te komen. Het wil daarbij ook bezien of een regeling op dit punt moet worden meegenomen in een wetgevingstraject dat specifiek betrekking heeft op het wegnemen van knelpunten bij gegevensuitwisseling in samenwerkingsverbanden, of dient te worden betrokken in een meer algemene herziening van het stelsel van vorderingsbevoegdheden in het kader van de voorgenomen modernisering van het Wetboek van Strafvordering.

Het gebruik van moderne analysetechnieken

Het derde dilemma heeft betrekking op het gebruik van moderne analysetechnieken. In een bijlage bij de kabinetsnotitie privacybeleid uit 2011 heeft het toenmalige kabinet zich op het standpunt gesteld dat er geen principiële redenen zijn om de overheid het gebruik van profilerings technieken te ontzeggen, om de enkele reden dat deze inbreuk maakt op het recht op bescherming van de persoonlijke levenssfeer. In die bijlage wordt ook opgemerkt dat het aanbeveling verdient voor het gebruik van profileringstechnieken door samenwerkingsverbanden van verschillende toezichthouders en handhavers nieuwe wettelijke grondslagen te creëren, wanneer een samenwerkingsverband een min of meer permanent karakter krijgt en op basis van de bestaande wetgeving of op basis van geldende geheimhoudingsplichten de conclusie moet worden getrokken dat de gewenste gegevens in dat onderlinge verband niet mogen worden gedeeld of verder mogen worden verwerkt.⁹ Een heldere basis voor het gebruik van moderne analysetechnieken door samenwerkingsverbanden ontbreekt nu. Het kabinet onderschrijft het standpunt uit de verkenning dat een eventuele kaderwet hierin kan voorzien. Daarbij geldt dan wel als voorwaarde dat de deelnemers aan een samenwerkingsverband moeten kunnen rechtvaardigen dat het belang dat van de door een kaderwet toegestane analysetechniek gebruik wordt gemaakt, zwaarder weegt dan het belang van bescherming van de persoonlijke levenssfeer.

Informatieplicht jegens betrokkenen

Het vierde dilemma dat hier aandacht behoeft, betreft de informatieplicht jegens betrokkenen. Deze verplichting vormt een uitwerking van het transparantiebeginsel. Uitvoering van deze verplichting stelt de burger over wie gegevens worden verwerkt, in staat te volgen hoe gegevens over hem worden verwerkt en bepaalde vormen van verwerking of onrechtmatig gedrag van de verantwoordelijke organisatie in rechte aan te vechten.¹⁰ De Wet bescherming persoonsgegevens maakt het mogelijk dat op deze verplichting een uitzondering wordt gemaakt ingeval de verwerking plaatsvindt op grond van een wettelijk voorschrift. Het kabinet onderschrijft de redenen die in de verkenning worden aangedragen om van deze uitzonderingsmogelijkheid gebruik te maken: de grote inspanning die uitvoering van deze verplichting voor samenwerkingsverbanden meebrengt, en het tegengaan van calculerend gedrag. Het kabinet neemt daarmee eenzelfde positie in als bij een recente wijziging van de Wet structuur uitvoeringsorganisatie werk en inkomen is gedaan.¹¹ Wel zal een eventuele kaderwet maatregelen moeten voorschrijven waarmee de transparantie op andere wijze wordt gediend. Daarbij valt te denken aan de verplichting het convenant en informatieprotocol van het samenwerkingsverband op een voor de burger toegankelijke wijze te

⁹ Kamerstuk 32 761, nr. 1, bijlage, blz. 3–4.

¹⁰ Kamerstuk 25 892, nr. 3, blz. 149.

¹¹ Vgl. kamerstuk 33 579, nr. 3, blz. 26.

publiceren, zodat hij daar genoegzaam uit kan afleiden of over hem gegevens worden verwerkt. Verder zullen in ieder geval specifieke personen over de verwerking van hun persoonsgegevens geïnformeerd dienen te worden, indien het tot de taken van een samenwerkingsverband behoort om adviezen over specifieke personen te geven. De verwerking van gegevens over deze personen heeft immers een in potentie ingrijpender karakter dan de verwerking van gegevens over andere personen door het samenwerkingsverband, bijvoorbeeld personen uit de omgeving van betrokkene. De uitvoering van deze beperkte informatieplicht kan overigens achterwege blijven, voor zover dat noodzakelijk is op gronden die de bestaande privacywetgeving kent. Daartoe behoort onder meer het belang van de voorkoming, opsporing en vervolging van strafbare feiten (vgl. art. 43 Wbp).

Juridische vormgeving

Het vijfde en laatste dilemma betreft de vraag of een eventuele kaderwet voldoende precies kan zijn bij de oplossing van generieke knelpunten, nu daarbij ook specifieke belangen een rol kunnen spelen. Een vraag die hiermee samenhangt, is of een kaderwet voor een juiste balans kan zorgen tussen wat de wetgever zelf moet regelen en wat kan worden overgelaten aan regeling door de deelnemers aan een samenwerkingsverband. Het kabinet meent dat op beide vragen maar ten dele een bevestigend antwoord kan worden gegeven. Een kaderwet bevat immers algemene regels, die slechts in beperkte mate met specifieke belangen rekening kunnen houden. Dit zou impliceren dat de wetgever op punten waar die specifieke belangen een rol spelen, bij een keuze voor een kaderwet onvoldoende in staat zou zijn op die punten een goede afweging te maken. In dat licht bezien zullen knelpunten waarbij specifieke belangen een rol spelen, zich beter lenen voor oplossing binnen de context van de sectorale wetten die hierbij in het geding zijn. Het kabinet opteert dan ook voor een combinatie van bepalingen die in een algemene regeling voor gegevensuitwisseling binnen samenwerkingsverbanden worden neergelegd, en noodzakelijke wijzigingen in de bestaande sectorale wetten.

Voor regeling in algemene bepalingen kan worden gedacht aan de volgende onderwerpen uit de verkenning:

1. algemene eisen aan de inrichting van een samenwerkingsverband,
2. algemene eisen aan de inhoud van het convenant en het informatieprotocol,
3. de verplichting de voor het samenwerkingsverband noodzakelijke gegevens te verstrekken, voor zover – zie hierna – de relevante sectorale wetgeving dat toelaat,
4. de waarborgen voor een zorgvuldige gegevensverwerking (zie ook hierna),
5. de informatieverstrekking aan betrokken burgers,
6. de legitimatie van typen van gegevensverwerking.

Het gaat hier om onderwerpen die zich naar hun aard goed lenen voor een uniforme regeling op één plek.

Voor regeling in de relevante sectorale wetten dienen zich de volgende onderwerpen aan:

1. de verstrekking van gegevens aan door een algemene regeling gereguleerde samenwerkingsverbanden met, indien noodzakelijk, uitzonderingen daarop en eventuele voorwaarden waaronder verstrekt mag worden,
2. de buiten toepassing verklaring van de vorderingsplicht uit het Wetboek van Strafvordering, eventueel met nadere voorwaarden.

Met betrekking tot het eerste genoemde onderwerp geldt dat het niet alleen wenselijk is bij de verstrekking van gegevens als uitzondering op de geheimhoudingsbepalingen rekening te houden met specifieke belangen die aan een geheimhoudingsplicht verbonden zijn, maar ook dat het aan de wetgever is en niet aan partners van een samenwerkingsverband om deze specifieke belangen, zo nodig, te vertalen in uitzonderingen op de verstrekking van gegevens als uitzondering op de desbetreffende geheimhoudingsbepaling dan wel in nadere voorwaarden aan de verstrekking van gegevens. Het tweede onderwerp leent zich het best voor regeling in het Wetboek van Strafvordering. De wijzigingen die het hier betreft, kunnen worden opgenomen in een wetsvoorstel dat ook de eerder bedoelde algemene bepalingen bevat. Hetzelfde geldt overigens met betrekking tot wijzigingen die wenselijk zijn om specifieke knelpunten op te lossen, zoals die uit de inventarisatie van de behoefte aan gegevensuitwisseling in een viertal casussen voortkomen (gefingeerde dienstverbanden, faillissementsfraude, identiteitsfraude en notoire fraudeurs/subjectgerichte fraudebestrijding).¹²

Het kabinet schaaft zich achter de gedachte dat een dergelijk wetsvoorstel zich niet alleen mag richten op het wegnemen van knelpunten die op dit moment met betrekking tot het uitwisselen van gegevens bestaan. Integendeel, een verbetering van de mogelijkheden tot gegevensuitwisseling die uit het wegnemen van deze knelpunten voortvloeit, schept een navenant grotere verantwoordelijkheid voor een zorgvuldige inrichting van het proces van gegevensuitwisseling. Anders gezegd: er zal ook een goede balans moeten worden gevonden tussen enerzijds de met wetgeving beoogde verbetering van de mogelijkheden van gegevensuitwisseling en anderzijds het recht op bescherming van de persoonlijke levenssfeer. Beide kunnen hand in hand gaan, als de wet niet alleen knelpunten wegneemt, maar ook de nodige waarborgen voor een zorgvuldige gegevensverwerking bevat. Zo'n wet kan dan ook een nieuwe impuls geven aan een zorgvuldige omgang met gegevens in de al bestaande praktijk van gegevensuitwisseling.

Het kabinet meent dat de verkenning een aantal waardevolle suggesties voor dergelijke waarborgen bevat. Hierbij kan met name worden gedacht aan explicitering in de wet van het vereiste van noodzakelijkheid en de daaruit voortvloeiende beginselen van proportionaliteit en subsidiariteit, waarborgen met betrekking tot het koppelen van gegevensbestanden, de duiding van de kwaliteit van de gegevens en de transparantie van de gegevensverwerking en het uitvoeren van een Privacy Impact Assessment door het samenwerkingsverband. Het kabinet kan zich ook goed vinden in de gedachte dat een wet de deelnemers aan het samenwerkingsverband voorschrijft in een informatieprotocol een aantal elementen vast te leggen c.q. op basis van de algemene wettelijke bepalingen uit te werken die voor de bescherming van gegevens in een samenwerkingsverband van belang zijn, zoals 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. Het gaat hier om maatwerk, zodat een wet alleen kan voorschrijven dat deze elementen in zo'n protocol moeten worden opgenomen, maar de uitwerking daarvan aan het samenwerkingsverband moet overlaten. Het kabinet onderschrijft dat het vastleggen van dergelijke waarborgen in een wet en nadere uitwerking in een informatieprotocol de transparantie van de gegevensverwerking voor de burger kan vergroten en daarmee de verantwoordelijkheid en aansprakelijkheid («accountability») van de partijen in het samenwerkingsverband voor een zorgvuldige gegevensuitwisseling.

¹² Kamerstuk 17 050, nr. 450, blz. 7–8.

Het uitgangspunt voor een kaderwet, zoals deze in de verkenning is beschreven, is dat de bestaande regelgeving met betrekking tot gegevensverwerking op enkele uitzonderingen na in stand wordt gehouden. Dit 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 (recht op inzage, correctie en verzet). In zoverre zullen de algemene bepalingen over de gegevensuitwisseling in samenwerkingsverbanden een aanvulling op de bestaande regelgeving vormen. Het kabinet meent dat daarmee een verstandige keuze wordt gemaakt, omdat wetgeving die dieper in de bestaande wetgeving zou ingrijpen niet alleen tot een meer complexe wetgevingsoperatie zou leiden, maar ook sterker rekening zou moeten houden met verschillende lopende en nog in voorbereiding zijnde wetgevingstrajecten.

Tot deze trajecten rekt het kabinet ook het traject waarbinnen in de Europese Unie een Algemene verordening gegevensbescherming wordt voorbereid. Uit de verkenning komt naar voren dat een eventuele kaderwet als in die verkenning omschreven, voorshands binnen de grenzen blijft van de huidige voorstellen voor deze verordening. Het kabinet kan deze zienswijze onderschrijven. Het wijst er in dit verband op dat artikel 6 van het voorliggende voorstel voor deze verordening verwerking van persoonsgegevens toestaat, voor zover deze noodzakelijk is voor de vervulling van een taak van algemeen publiek belang of een taak die deel uitmaakt van de uitoefening van het openbaar gezag dat aan de voor de verwerking verantwoordelijke is opgedragen, en daarvoor een grondslag bestaat in EU-wetgeving of de wetgeving van een lidstaat. De wetgeving die het kabinet voorstaat, zou de hier bedoelde grondslag zijn. Verder is onder meer van belang dat een wettelijke regeling van het gebruik van bijvoorbeeld «profiling» door samenwerkingsverbanden past binnen de voorwaarden die artikel 20 van het voorstel voor de verordening stelt, nu deze regeling ook passende maatregelen zullen worden opgenomen ter bescherming van de gerechtvaardigde belangen van de betrokkenen. Het gaat hierbij met name om de in de verkenning genoemde waarborgen om de transparantie rond het gebruik van moderne analysetechnieken als «profiling» te verbeteren. Bij de voorbereiding van wetgeving zullen eventuele wijzigingen van het voorstel voor de verordening uiteraard nauwlettend gevolgd moeten worden.

Het kabinet is voorts van oordeel dat het in dit stadium nog prematuur is om zich vast te leggen op de precieze vormgeving en uitwerking van de benodigde wetgeving. Denkbaar is dat vorenbedoelde algemene bepalingen over de gegevensuitwisseling in samenwerkingsverbanden de vorm van een afzonderlijke wet krijgen. Tot de mogelijkheden behoort evenwel ook dat voor opnemng van een kaderregeling als aparte paragraaf in een bestaande wet wordt gekozen. Daarbij kan onder meer worden gedacht aan de Wet bescherming persoonsgegevens. Bij de voorbereiding van wetgeving zullen op dat punt nadere keuzes moeten worden gemaakt.

4. Conclusie

Het kabinet komt, alles overziend, tot de conclusie dat met het voorbereiden van wetgeving ter oplossing van de geconstateerde knelpunten een aanvang dient te worden gemaakt. Het onderkent tegelijkertijd dat bij de voorbereiding daarvan nog verschillende aspecten verder doordacht zullen moeten worden. Mede met het oog daarop hecht het kabinet er sterk aan met uw Kamer van gedachten te wisselen over de verschillende

aspecten van wetgeving ten behoeve van gegevensuitwisseling in samenwerkingsverbanden met daarbij in het bijzonder aandacht voor dilemma's, zoals in deze brief en de verkenning zijn beschreven.

De Minister van Veiligheid en Justitie,
I.W. Opstelten