

Wet houdende bepalingen met betrekking tot de uitwisseling van gegevens in samenwerkingsverbanden (Kaderwet gegevensuitwisseling in samenwerkingsverbanden)

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben, dat het wenselijk is voorschriften vast te stellen met betrekking tot de uitwisseling van gegevens in samenwerkingsverbanden;

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

Paragraaf 1. Algemene bepalingen

Artikel 1 *Definities*

1. In deze wet en de daarop rustende bepalingen wordt verstaan onder:
 - PM
 - Onze Minister: Onze Minister van Veiligheid en Justitie;
2. In deze wet wordt onder gegevens mede verstaan:
 - a. persoonsgegevens als bedoeld in artikel 1 van de Wet bescherming persoonsgegevens,
 - b. justitiële en strafvorderlijke gegevens als bedoeld in artikel 1 van de Wet justitiële en strafvorderlijke gegevens, en
 - c. politiegegevens als bedoeld in artikel 1 van de Wet politiegegevens.

Paragraaf 2. Samenwerkingsverband

Artikel 2 *Reikwijdte*

1. Deze wet is van toepassing op een samenwerkingsverband waarbinnen gegevens worden verwerkt voor een welbepaald doel ten dienste van een of meer van de in het tweede lid genoemde publieke belangen, indien de deelnemers de toepasselijkheid van deze wet zijn overeengekomen bij een convenant dat voldoet aan de in artikel 3 gestelde eisen.
2. Een samenwerkingsverband kan worden aangegaan met het oog op een of meer van de volgende belangen:
 - a. het voorkomen en bestrijden van onrechtmatig gebruik van overheidsmiddelen en overheidsvoorzieningen;
 - b. het uitoefenen van toezicht op de naleving van wettelijke voorschriften;
 - c. het handhaven van de openbare orde en veiligheid, en
 - d. het voorkomen, opsporen en vervolgen van strafbare feiten.

3. Een samenwerkingsverband bestaat uit twee of meer deelnemers. Ten minste een van de deelnemers is een overheidsinstantie.

5. Een overheidsinstantie kan slechts deelnemen en gegevens verstrekken aan een samenwerkingsverband indien dit bij wet is bepaald.

Artikel 3 *Convenant*

De deelnemers komen de toepasselijkheid van deze wet overeen in een convenant dat in ieder geval afspraken bevat over:

- a. het doel van de samenwerking;
- b. de taken en werkzaamheden die binnen het samenwerkingsverband worden uitgevoerd;
- c. de wijze waarop het samenwerkingsverband wordt bestuurd;
- d. de rechten en verplichtingen van de deelnemers jegens elkaar en jegens derden;
- e. de datum van inwerkingtreding en de geldingsduur van het convenant;
- f. de mogelijkheden van wijziging van, toetreding tot, uittreding uit en opheffing van het samenwerkingsverband, en
- g. de wijze waarop en de frequentie waarmee het convenant wordt geëvalueerd.

Artikel 4 *Informatieprotocol*

1. De deelnemers stellen nadere regels over de verwerking van gegevens door het samenwerkingsverband vast in een informatieprotocol.

2. Het informatieprotocol bevat in ieder geval:

- a. een beschrijving van de gegevens dan wel soorten daarvan die door het samenwerkingsverband worden verwerkt;
- b. een beschrijving van de inrichting van het proces van gegevensverwerking en de waarborgen die hierin zijn opgenomen met het oog op de bescherming van persoonsgegevens;
- c. regels over de beveiliging van de gegevens en de melding van een inbreuk op de beveiliging, bedoeld in de Wet bescherming persoonsgegevens, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die door het samenwerkingsverband worden verwerkt;
- d. regels over de geheimhouding door de deelnemers;
- e. regels over de informatieverstrekking over de gegevensverwerking aan het publiek en aan betrokkenen;
- f. regels over de wijze waarop betrokkenen hun rechten, bedoeld in de artikelen 35 en 36 van de Wet bescherming persoonsgegevens kunnen uitoefenen;
- g. regels over de verstrekking van gegevens aan derden;
- h. regels over de termijnen voor het bewaren van gegevens, en
- i. regels over de verwijdering en vernietiging van bewaarde gegevens.

Artikel 5

1. Het convenant wordt gepubliceerd in de Staatscourant.
2. Het informatieprotocol wordt elektronisch openbaar gemaakt op een algemeen toegankelijke wijze.
3. In het samenwerkingsverband worden geen gegevens verwerkt met toepassing van deze wet voordat het convenant en het informatieprotocol openbaar zijn gemaakt.

Paragraaf 3. Gegevensverwerking

Artikel 6 *Herkomst van gegevens*

De gegevens die een samenwerkingsverband verwerkt, zijn afkomstig van de deelnemers en uit voor een ieder toegankelijke informatiebronnen.

Artikel 7 *Typen gegevensverwerking*

1. Voor zover dit voor het doel van het samenwerkingsverband noodzakelijk is, is een samenwerkingsverband bevoegd om gegevens als bedoeld in artikel 6 te verwerken ten behoeve van een gemeenschappelijke casusanalyse en het opstellen van een advies op basis daarvan aan de deelnemers en geautomatiseerde data-analyse toe te passen op gegevens als bedoeld in artikel 6.

2. Indien gegevens worden verwerkt ten behoeve van geautomatiseerde data-analyse kunnen deze gegevens:

- a. op geautomatiseerde wijze onderling met elkaar worden vergeleken, dan wel in combinatie met elkaar worden vergeleken,
- b. worden doorzocht aan de hand van profielen, en
- c. worden vergeleken met het oog op het opsporen van bepaalde patronen.

3. Een samenwerkingsverband gebruikt de gegevens die het verwerkt uitsluitend voor:

- a. het opstellen van rapporten waarin inzichten worden geboden of trends worden gesignaleerd die betrekking hebben op een of meer van de in artikel 2 genoemde belangen met het oog waarop het samenwerkingsverband is aangegaan;
- b. het opstellen van adviezen over acties met betrekking tot een of meer van de in artikel 2 genoemde belangen met het oog waarop het samenwerkingsverband is aangegaan;
- c. het delen van informatie, inzicht en kennis binnen het samenwerkingsverband in andere dan de onder a en b bedoelde vormen, voor zover dat relevant voor de belangen met het oog waarop het samenwerkingsverband is aangegaan.

Artikel 8 *Waarborgen*

1. Voordat wordt overgegaan tot over een nieuwe verwerking van gegevens in een samenwerkingsverband:
 - a. wordt onderbouwd dat de gegevensverwerking noodzakelijk is voor het doel van het samenwerkingsverband en dat dit doel niet op een minder ingrijpende manier kan worden bereikt, en
 - b. wordt door middel van een gegevensbeschermingseffectbeoordeling onderbouwd dat de privacy van de betrokkenen voldoende is gewaarborgd.
2. De onderbouwing van de noodzaak en proportionaliteit van de gegevensverwerking, bedoeld in het eerste lid, onder a, en de gegevensbeschermingseffectbeoordeling, bedoeld in het eerste lid, onder b, worden elektronisch openbaar gemaakt op een algemeen toegankelijke wijze.

Artikel 9 *Waarborgen*

1. Bij de verwerking van gegevens worden tot natuurlijke personen herleidbare gegevens zoveel mogelijk geanonimiseerd of gepseudonimiseerd, waarbij een afweging wordt gemaakt tussen de inspanningen die het anonimiseren of pseudonimiseren vereist en de invloed hiervan op de effectiviteit van de gegevensuitwisseling.
2. Bij de verstrekking van gegevens door een deelnemer aan het samenwerkingsverband of door het samenwerkingsverband aan een of meer deelnemers wordt de graad van juistheid en betrouwbaarheid van de gegevens inzichtelijk gemaakt.

Artikel 10 *Waarborgen*

Indien in het kader van een nieuwe verwerking van gegevens, bestanden worden gekoppeld met andere bestanden teneinde vast te stellen of verbanden bestaan tussen zich in de verschillende bestanden bevindende gegevens, wordt voordat wordt besloten tot verwerking op een algemeen toegankelijke wijze en zonder afbreuk te doen aan de doelstelling van het samenwerkingsverband, inzicht gegeven in:

- a. de selectie van bestanden,
- b. typen gegevens waaruit de desbetreffende bestanden bestaan,
- c. de algoritmes en methoden die bij de analyse van de verkregen gegevens worden gebruikt, en
- d. het voorgenomen gebruik van de verkregen gegevens.

Artikel 11

Maatregelen jegens een persoon worden niet bevorderd of getroffen uitsluitend op basis van de resultaten van een gegevensverwerking als bedoeld in artikel 7.

Paragraaf 4 Wijzigingen in andere wetten

Deze paragraaf wordt gevuld met artikelen waarin overheidsinstanties worden aangewezen die gegevens kunnen uitwisselen in samenwerkingsverbanden.

Paragraaf 5 Slotbepalingen

Artikel @ Inwerkingtreding

Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld.

Artikel @ Citeertitel

Deze wet wordt aangehaald als: Kaderwet gegevensuitwisseling in samenwerkingsverbanden.

Lasten en bevelen dat deze wet in het Staatsblad zal worden geplaatst en dat alle ministers, autoriteiten, colleges en ambtenaren die zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

Gegeven

De Minister van Veiligheid en Justitie,

MEMORIE VAN TOELICHTING

I. ALGEMEEN

1. Inleiding

Dit wetsvoorstel strekt ertoe de uitwisseling van gegevens in samenwerkingsverbanden tussen overheidsinstanties onderling of tussen overheidsinstanties en privaatrechtelijke organisaties van een betere juridische basis te voorzien. In de praktijk bestaan er reeds vele samenwerkingsverbanden, maar omdat deze meestal geen heldere juridische status hebben, is er veel onduidelijkheid over de mogelijkheden tot uitwisseling van gegevens.

Zo berust de verstrekking van gegevens aan een samenwerkingsverband veelal op grondslagen om aan afzonderlijke deelnemers aan dat verband gegevens te verstrekken en dient om die reden de noodzaak van verstrekking per individuele deelnemer te worden aangetoond. Een heldere basis om gegevens aan het samenwerkingsverband als zodanig te verstrekken en deze gegevens binnen het verband verder te verwerken ontbreekt. Daaraan bestaat wel behoefte, bijvoorbeeld om een gezamenlijk casusoverleg of een gezamenlijke data-analyse uit te voeren. Een ander knelpunt is dat sectorale wetten veelal geen goede grondslagen bevatten voor gegevensuitwisseling binnen samenwerkingsverbanden met privaatrechtelijke partijen, terwijl dat met het oog op een publiek belang wel wenselijk kan zijn. Dit wetsvoorstel beoogt deze en andere knelpunten bij de gegevensuitwisseling binnen samenwerkingsverbanden weg te nemen.

Om die gegevensuitwisseling zorgvuldig te laten verlopen bevat dit wetsvoorstel in de tweede plaats een aantal waarborgen ter aanvulling of precisering van de meer algemene waarborgen die de bestaande wetgeving met betrekking tot persoonsgegevens al kent. Een voorbeeld daarvan is PM.

Tot slot bevat het wetsvoorstel ook een aantal wetswijzigingen die de uitwisseling van gegevens buiten de context van samenwerkingsverbanden beogen te verbeteren. Te noemen valt PM.

2. Aanleiding

Het voorstel vloeit voort uit een brief van het kabinet van 14 december 2014 aan de Tweede Kamer over de aanpak van fraude (Kamerstukken II 2014/15, 32 761, nr. 79). Het kabinet constateert in die brief dat fraude met overheidsvoorzieningen een groeiend probleem is. De effecten daarvan reiken verder dan alleen de directe financiële schade voor de overheid zelf. Fraude ondermijnt ook 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 dan ook 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 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. De intensivering en verbreding van de samenwerking tussen diverse organisaties bij het voorkomen en bestrijden van fraude heeft intussen scherper zicht gegeven op grenzen en belemmeringen waar deze 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 gezien 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.

Tegen deze achtergrond heeft kabinet een verkenning laten uitvoeren naar een kaderwet voor de gegevensuitwisseling in samenwerkingsverbanden die als bijlage bij voornoemde brief van 14 december 2014 is gevoegd. Uit het rapport van de Werkgroep Verkenning kaderwet gegevensuitwisseling "Kennis delen geeft kracht" blijkt dat zich bij deze gegevensuitwisseling knelpunten voordoen in relatie tot onder meer de juridische status van samenwerkingsverbanden, de uitwisseling met private partijen, de verstrekking van gegevens aan en door de politie en het openbaar ministerie, alsmede het uitvoeren van geavanceerde data-analyses op basis van bronnen die onder verschillende wettelijke regimes vallen (zie bijlage bij Kamerstukken 2014/15, 32 761, nr. 79). In zijn brief schrijft het kabinet zich te herkennen in deze knelpunten en trekt het de conclusie dat een aanvang dient te worden gemaakt met het voorbereiden van wetgeving ter oplossing van daarvan. De brief en het rapport zijn vervolgens besproken in het Algemeen Overleg van 8 april 2015 over de rijksbrede aanpak van fraude (Kamerstukken II, 2014/15, 17 050, nr. 505). In dat overleg zijn verschillende aandachtspunten naar voren gebracht waarmee bij de voorbereiding van het wetsvoorstel rekening zou moeten worden gehouden. Het betreft onder meer een nadere onderbouwing van nut en noodzaak van een kaderwet en van het uitgangspunt "ja, tenzij" bij gegevensuitwisseling volgens de beoogde kaderwet, het belang van goede waarborgen en het uitvoeren van een Privacy Impact Assessment. Verderop in deze toelichting zullen deze aandachtspunten nog uitgebreid aan de orde komen.

3. Hoofdpijnen wetsvoorstel

3.1 Inleiding

Zoals in het rapport van de werkgroep gegevensuitwisseling al naar voren komt, heeft gegevensverwerking 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 dienstbaar aan de opgedragen taak van praktisch iedere overheidsorganisatie. Iedere overheidsorganisatie heeft zijn eigen taak en oefent een eigen gegevenshuishouding uit bij de uitvoering van die taak. Zolang de gegevensverwerking plaatsvindt binnen het kader van de eigen taak, ligt de bevoegdheid tot dergelijke gegevensverwerking opgesloten in de taakomschrijving van de desbetreffende organisatie. In deze situatie is het opnemen van bepalingen rond gegevensverwerking veelal beperkt tot het opnemen van verplichtingen tot informatieverstrekking aan burgers die met de betrokken overheidsinstelling te maken hebben. Ook is meestal sprake van een geheimhoudingsbepaling voor de betrokken overheidsdienst zodat burgers en bedrijven erop kunnen vertrouwen dat hun gegevens in veilige handen zijn. Daarmee is in beginsel sprake van gesloten gegevenshuishoudingen per domein of zelfs per overheidsdienst.

Pas 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 een dergelijke uitwisseling van gegevens van een adequate juridische grondslag te voorzien. De bevoegdheid gegevens uit te wisselen met een ander valt immers in beginsel buiten de taakomschrijving van de betrokken overheidsdienst, zoals die door de wetgever in de vorm van taken en bevoegdheden aan die dienst is geattribueerd. De bevoegdheid gegevens te delen 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 primair 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 sectorspecifieke regelingen bepalingen bevatten over verstrekking aan derden, hebben deze bovendien meestal betrekking op unilaterale verstrekking en niet op verstrekking aan meerdere partijen tegelijk die in een samenwerkingsverband

opereren.¹ Deze systematiek van de wetgeving kan voor samenwerkingsverbanden tamelijk complex uitpakken. 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 unilaterale verstrekking mogelijk maken, ook kunnen worden benut voor gegevensuitwisseling binnen het samenwerkingsverband (zie hierna § 3.3.1). De slagkracht van de samenwerking kan zodoende teloor gaan door de veelheid aan interpretaties van de bestaande, veelal sectorale regels en door wettelijke belemmeringen. Er bestaat onzekerheid over essentiële vragen als die of gegevensuitwisseling wel is geoorloofd in een concrete situatie en wat daarbij precies de 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.

Een en ander hoeft er niet aan in de weg te staan dat de gegevensuitwisseling in samenwerkingsverbanden op basis van de huidige wetgeving verder kan worden geoptimaliseerd. Daarbij kan met behulp van convenanten en privacy- of informatieprotocollen op basis van de mogelijkheden die de huidige wetgeving biedt, vaak meer worden gedaan dan op het eerste gezicht mogelijk lijkt. Dat neemt niet weg dat er knelpunten resteren waarvoor dit wetsvoorstel een oplossing beoogt te bieden. Deze knelpunten en oplossingen komen hierna in § 3.3. aan bod, nadat hierna in § 3.2. eerst nog is stil gestaan bij de reikwijdte van het wetsvoorstel.

3.2 Reikwijdte wetsvoorstel

Het rapport van de Werkgroep Verkenning kaderwet gegevensuitwisseling heeft betrekking op gegevensuitwisseling op een breder terrein dan fraudebestrijding. Een eerste reden die daarvoor in het rapport wordt aangedragen, is dat de meeste samenwerkingsverbanden die zich met de aanpak van fraude bezighouden, ook andere taken hebben. 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 onwerkbaar situatie opleveren. Hiervan zou al sprake kunnen zijn, als gegevens voor uitsluitend één doel zouden worden verwerkt. Gegevens die samenwerkingsverbanden verwerken, kunnen echter meerdere doelen tegelijk dienen. Zo kunnen de RIEC's (Regionale Informatie- en Expertisecentra) bepaalde persoonsgegevens verwerken met het oog op tegelijkertijd

¹ Uitzonderingen hierop zijn te vinden in de artikel 20 Wet politiegegevens, artikel 28, tweede lid, onder d, Wet Bibob en artikel 64 Wet Suwi. Verder bevat ook de Wbp in artikel 22, zesde lid, een specifieke bepaling met betrekking tot verstrekking van strafrechtelijke gegevens door en ten behoeve van samenwerkingsverbanden.

georganiseerde hennepsteelt en fraude in de vastgoedsector. Het zou dan niet duidelijk zijn in hoeverre de verwerking van gegevens in dat geval onder het regime van de kaderwet zou plaatsvinden. Een andere reden is dat een kaderwet evenzeer van belang kan zijn met het oog op knelpunten bij de uitwisseling van gegevens op andere terreinen. Geluiden uit de praktijk bevestigen dit. Bij een relatief smalle kaderwet zou dus al gauw de behoefte ontstaan om voor aanpalende terreinen eveneens kaderwetgeving op te stellen.

Een en ander zou volgens het rapport pleiten voor een kaderwet die een breder terrein dan fraudebestrijding bestrijkt. Dit bredere terrein zou de volgende doeleinden kunnen omvatten: de voorkoming van onrechtmatig gebruik van overheidsmiddelen 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"). Blijkens een inventarisatie van samenwerkingsverbanden die bij het rapport is gevoegd, is het 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. In voornoemde brief van 14 december 2014 heeft het kabinet te kennen gegeven zich in deze brede reikwijdte goed te kunnen vinden.

Het kabinet erkent in navolging van het rapport van de Werkgroep Verkenning kaderwet gegevensuitwisseling dat zich ook onder een kaderwet op dit bredere terrein het geval kan voordoen van een samenwerkingsverband dat op een terrein functioneert dat deels buiten de grenzen van de kaderwet valt. Het kabinet schat echter in dat zo'n geval zich niet gauw zal voordoen. Daarbij moet worden bedacht dat bijvoorbeeld de gegevensverwerking binnen veiligheidshuizen volledig onder de reikwijdte van zo'n bredere kaderwet is te vatten. Weliswaar nemen aan veiligheidshuizen ook partners uit de zorg deel, maar het doel van veiligheidshuizen en daarmee ook van de gegevensverwerking staat in het teken van het terugdringen van overlast, huiselijk geweld en 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 zo'n bredere kaderwet.

Een vraag die de reikwijdte van een kaderwet ook bepaalt, is de vraag of deze wet alleen voor samenwerkingsverbanden zou moeten gelden die op nationaal niveau opereren, of ook voor verbanden die op regionaal of lokaal niveau werkzaam zijn. Met het oog op de belangen die de kaderwet wil dienen, ligt een

bepierking tot samenwerkingverbanden op nationaal niveau niet voor de hand. Ook op lokaal en regionaal niveau bestaan samenwerkingverbanden waarvoor een kaderwet een legitimerende, faciliterende en normerende functie kan vervullen.

3.3 Oplossing knelpunten in de gegevensuitwisseling in samenwerkingverbanden

3.3.1 Verstreking van gegevens aan samenwerkingverbanden

De mate waarin gegevens aan samenwerkingverbanden kunnen worden verstrekt, wordt sterk bepaald door de bestaande geheimhoudingsplichten en eventuele uitzonderingen daarop. Deze geheimhoudingsplichten kunnen zijn ingegeven met het oog op verschillende belangen. Het kan onder meer gaan om bescherming van private belangen (persoonlijke levenssfeer, 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).²

Bij gegevensuitwisseling in samenwerkingverbanden zijn de bescherming van private belangen en de zorg voor de goede werking van het openbaar bestuur het belangrijkste. 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 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 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 een bepaald deelbelang binnen het openbaar bestuur, zoals de correcte belastingheffing of de bewaking van de soliditeit van banken. De geheimhoudingsplicht heeft aldus meer kanten.³

Het rapport van de Werkgroep Verkenning kaderwet gegevensuitwisseling bevat een, overigens niet uitputtende, opsomming van geheimhoudingsplichten (zie

² A.M. Klingenberg, A. Logemann en S.A.J. Munneke "Geheimhouding als juridische kwaliteitseis van primaire besluitvorming" in: M. Herweijer, A.T. Marseille, F.M. Noordam, H.B. Winter (red), Alles in één keer goed. Juridische kwaliteit van bestuurlijke besluitvorming, 2005, blz. 178-179.

³ A.J.C. de Moor-van Vugt, Gegevensuitwisseling door Toezichhouders; onderzoek uitgevoerd in opdracht van het WODC, 2012, blz. 31.

blz. 31-33). De wetten waarin deze plichten zijn opgenomen, bevatten ook bepalingen die de geheimhoudingsplicht doorbreken door mogelijkheden te creëren gegevens – al dan niet onder bepaalde voorwaarden – aan derden te verstrekken. Deze mogelijkheden houden evenwel in onvoldoende mate rekening met het bestaan van samenwerkingsverbanden. Dit is toe te schrijven aan het feit dat samenwerkingsverbanden nu meestal geen heldere juridische status hebben. Zoals hiervóór in § 3.1 al naar voren kwam, kennen de meeste sectorale wettelijke regelingen dan ook geen generieke mogelijkheden tot verstrekking van gegevens aan samenwerkingsverbanden. Dit heeft tot gevolg dat men nu veelal moet terugvallen op mogelijkheden tot unilaterale verstrekking aan één partij. Op basis van die mogelijkheden moet de noodzaak van verstrekking van gegevens per individuele deelnemer van een samenwerkingsverband worden aangetoond, in plaats van dat dit alleen voor het doel van het verband als geheel behoeft (Kamerstukken II 2012/13, 33 632, nr. 4, blz. 18-19). In de praktijk bestaat behoefte aan het laatste, omdat ook de verdere verwerking van de verstrekte gegevens binnen het samenwerkingsverband veelal in het teken staat van het doel van het samenwerkingsverband als geheel.

Aan deze behoefte kan worden tegemoet gekomen door in dit wetsvoorstel samenwerkingsverbanden allereerst een heldere juridische status te geven. Daartoe wordt in dit wetsvoorstel bepaald dat een samenwerkingsverband kan worden opgericht ten behoeve van een of meer van de volgende doeleinden:

- a. het voorkomen en bestrijden van onrechtmatig gebruik van overheidsmiddelen en overheidsvoorzieningen,
- b. het houden van toezicht op de naleving van wettelijke voorschriften,
- c. het handhaven van de openbare orde en veiligheid of
- d. het voorkomen, opsporen en vervolgen van strafbare feiten.

De juridische status van samenwerkingsverbanden wordt in het wetsvoorstel verder vorm gegeven door te bepalen dat de kaderwet van toepassing is op een samenwerkingsverband waarbinnen gegevens worden verwerkt met het oog op een welbepaald doel dat binnen eerdergenoemde doeleinden valt, onder de voorwaarde dat de deelnemers dit zijn overeengekomen bij een convenant dat voldoet aan bepaalde in de wet genoemde eisen.

Voor de verstrekking van gegevens aan een samenwerkingsverband als bedoeld in de kaderwet worden in dit wetsvoorstel voorts verschillende wetten gewijzigd. Als gevolg van deze wijzigingen zullen die wetten voortaan een heldere grondslag bevatten voor verstrekking van gegevens aan een dergelijk samenwerkingsverband. Deze grondslag is steeds op dezelfde leest geschoeid: zij is geformuleerd als een verplichting om aan een samenwerkingsverband als bedoeld in de kaderwet de gegevens te verstrekken die noodzakelijk zijn om het doel van dat verband te bereiken, met dien verstande dat bij of krachtens algemene maatregel van bestuur categorieën van gegevens van de verstrekkingplicht kunnen worden uitgezonderd, alsmede voorwaarden aan deze verstrekking kunnen worden gesteld. Aldus is het mogelijk in iedere betrokken

wet en daarop berustende bepalingen op het punt van uitzonderingen en voorwaarden maatwerk te leveren, waarbij rekening wordt gehouden met de specifieke belangen die aan de geheimhoudingsplicht in de desbetreffende wet zijn verbonden. Het kan wenselijk zijn dat samenwerkingsverbanden in hun informatieprotocol aanvullende uitzonderingen en voorwaarden opnemen om op dit punt tot nog meer maatwerk te komen. Met het oog daarop zullen ook krachtens algemene maatregel van bestuur uitzonderingen en voorwaarden kunnen worden vastgelegd.

Een en ander impliceert dat verstrekking van gegevens aan een samenwerkingsverband als bedoeld in de kaderwet zal geschieden op basis van de principes "ja, tenzij" (uitzonderingen) en ja, mits" (voorwaarden). Daarmee zal de discussie over de verstrekking van gegevens aan samenwerkingsverbanden voortaan niet zozeer meer gaan over de primair juridische vraag wat op het punt van gegevensverstrekking wel en niet mag, maar veeleer over de meer beleidsmatige vraag "Willen wij met elkaar samenwerken en de daartoe noodzakelijke gegevens uitwisselen en welke gegevens menen wij eventueel daarvan te moeten uitzonderen?".

Overigens zij er nog met nadruk op gewezen dat de voorgestelde kaderwet niet tot doel 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 uitsluitend de thans al geldende wetgeving. Daartoe kan aanleiding bestaan, indien de kaderwet voor een samenwerkingsverband, gelet op haar behoeften aan informatie, niet of nauwelijks betere mogelijkheden tot gegevensuitwisseling boven de bestaande wetgeving biedt.

3.3.2 Verwerking van gegevens binnen samenwerkingsverbanden

Omdat een samenwerkingsverband meestal geen heldere juridische status heeft, mag het feit dat volgens een wettelijke regeling gegevens mogen worden verstrekt aan in die regeling genoemde partijen, er niet toe leiden dat ook gegevensuitwisseling binnen een samenwerkingsverband van die partijen mogelijk wordt. De desbetreffende partijen mogen deze gegevens slechts verstrekken in een één-op-één relatie met de in de wet genoemde partijen. Ieder van deze partijen is vervolgens gehouden deze gegevens vertrouwelijk te behandelen. Deze eis staat in de weg aan gegevensuitwisseling binnen een samenwerkingsverband (Kamerstukken II 2012/13, 33 632, nr. 4, blz. 18-19). Dat belemmert de mogelijkheden om binnen een samenwerkingsverband een gezamenlijk casusoverleg of een gezamenlijke data-analyse uit te voeren. Het wetsvoorstel lost dit knelpunt op door niet alleen aan samenwerkingsverbanden die aan de in de kaderwet gestelde vereisten voldoet, een heldere juridische basis te geven, maar ook door een expliciete grondslag voor de verwerking van gegevens binnen een samenwerkingsverband te geven.

3.3.3 Uitwisseling met privaatrechtelijke partijen

Publiek-private samenwerking levert beide kanten voordelen op. Er zit veel kennis over nieuwe ontwikkelingen, risico's en technologieën bij het bedrijfsleven en ook beschikken private partijen soms 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 actie ondernemen of een interventie plegen die bijdraagt aan het voorkomen en bestrijden van criminaliteit. In het rapport van de Werkgroep Verkenning kaderwet gegevensuitwisseling werden de volgende voorbeelden van publiek-private verbanden genoemd: energiebedrijven bij de aanpak van hennepkwekerijen, curatoren bij het voorkomen van faillissementsfraude, financiële dienstverleners bij het tegengaan van witwassen en transportondernemingen bij de handel in verboden goederen.

Sectorale wetten bevatten veelal geen grondslagen voor verstrekking aan private partijen die aan samenwerkingsverbanden (willen) deelnemen, terwijl daaraan met het oog op een publiek belang wel behoefte kan bestaan. Een voorbeeld daarvan doet zich voor bij het Financieel Expertisecentrum (FEC), dat met banken zou willen samenwerken in het project "commercieel vastgoed". Banken hebben op basis van hun interne risicobeoordeling zicht op klanten met een hoog risico. Deze informatie kan relevant zijn voor de andere partners in het FEC en andersom kan de informatie van die andere FEC-partners van belang zijn voor de banken. Op basis daarvan kan een bank bijvoorbeeld bepaalde dienstverlening stopzetten. Dit is soms effectiever dan het starten van een opsporingsonderzoek. Op basis van de huidige wetgeving kan deze informatie echter niet tussen de FEC-partners en de banken worden uitgewisseld. Hiermee vergelijkbare problemen zien we in de relatie tussen toezichthouders en private partijen die willen samenwerken en daartoe gegevens uitwisselen. Het wetsvoorstel lost dit knelpunt op door in sectorale wetten een grondslag op te nemen voor verstrekking van gegevens aan samenwerkingsverbanden als bedoeld in de kaderwet en in de kaderwet zelf te regelen dat aan samenwerkingsverbanden ook private partijen kunnen deelnemen.

3.3.4 Data-analyse

Samenwerkingsverbanden mogen met behulp van *data mining* op basis van geanonimiseerde gegevens bepaalde patronen zichtbaar maken aan de hand waarvan zij groepsprofielen kunnen opstellen. Zij kunnen daartoe gebruik maken van de mogelijkheden in de huidige wetgeving om ten behoeve van wetenschappelijke onderzoek en statistiek persoonsgegevens te verwerken. Verwezen zij naar de artikelen 9, derde lid, en 23, tweede lid, Wet bescherming persoonsgegevens (Wbp), artikel 22 Wet politiegegevens (Wpg) en de artikelen 15 en 39g Wet justitiële en strafvorderlijke gegevens (Wjsg).

Samenwerkingsverbanden mogen deze profielen echter niet matchen met persoonsgegevens om bepaalde personen met een verhoogd risico in beeld te krijgen (*profiling*). De meeste sectorale wetten geven, als zij al een grondslag voor profiling bevatten, slechts een grondslag voor profiling binnen de “eigen” kolom (vgl. artikel 11 Wpg), niet voor profiling in samenwerkingsverbanden op basis van verschillende bronnen van de verschillende deelnemers. Meer generieke voorschriften over profiling als in artikel 42 Wbp liggen opgesloten, kunnen geen betrekking hebben op gegevens waarvoor een specifiek regime, zoals de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens, geldt. Er bestaat verder gerede twijfel of partijen die aan een samenwerkingsverband deelnemen, op basis van een analyse binnen dat verband vervolgens op grond van hun eigen bevoegdheden acties mogen uitvoeren. Een en ander zet een rem op het benutten van kansen om met moderne analysetechnieken bepaalde risico's met betrekking tot individuele personen in beeld te brengen. Zo kan de infobox Crimineel en Onverklaarbaar Vermogen (iCOV) de door haar ontwikkelde profielen niet matchen met de haar ter beschikking staande gegevens om een lijst te genereren van personen met een groot risico dat zij fraude (gaan) plegen. Eenzelfde probleem was te zien bij het project FinPro, waarin men op basis van geanonimiseerde gegevens fraudepatronen heeft ontwikkeld, maar deze niet heeft mogen gebruiken ten behoeve van de uitvoering van de wettelijke taken van deelnemers aan het project (Kamerstukken II 2015/2016, Aangangs 3413).

Dit wetsvoorstel beoogt een heldere grondslag te geven voor typen van gegevensverwerking binnen samenwerkingsverbanden. Daartoe behoort ook het opstellen van profielen van groepen van personen, organisaties of bedrijven die met het oog op het doel van het samenwerkingsverband een verhoogd risico laten zien en het koppelen van deze profielen aan gegevens waarover het samenwerkingsverband rechtmatig beschikt, teneinde een lijst te kunnen opstellen van personen organisaties of bedrijven die met het oog op het doel van het samenwerkingsverband een verhoogd risico laten zien. Hierbij geldt dan wel als voorwaarde dat de deelnemers aan een samenwerkingsverband moeten kunnen rechtvaardigen dat het belang dat van de uitkomsten van een dergelijke analysetechniek ten behoeven van taakuitoefening van de deelnemers gebruik wordt gemaakt, zwaarder weegt dan het belang van bescherming van de persoonlijke levenssfeer (PM regelen bij de waarborgen).

Overigens wordt er hier nog op gewezen dat de uitkomst van een analyse binnen een samenwerkingsverband waaraan politie en justitie deelnemen, onder de voorgestelde kaderwet weliswaar tot een lijst kan leiden met bijvoorbeeld personen die een verhoogd risico op het zijn van beroepsfraudeur laten zien, maar nog geen formele verdenking oplevert. Zeker als zo'n lijst met behulp van Big Data technologie louter correlatieve en geen causale verbanden laat zien, kan van een formele verdenking (nog) geen sprake zijn. Daarvoor dienen

concrete feiten en omstandigheden met betrekking tot de desbetreffende persoon op tafel te komen die op fraude wijzen.

3.3.5 Verrijking van gegevens door politie en OM

Voor het bestuursrechtelijke en het strafrechtelijke domein gelden verschillende wettelijke regimes. Dit houdt verband met het feit dat ten aanzien van personen die verdacht worden van een strafbaar feit, al naar gelang de aard en ernst 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 markeren. Daar komt bij dat binnen het strafrechtelijk domein politie 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 eraan bij dat bestuursrechtelijke en strafrechtelijke handhaving door elkaar heen kunnen gaan lopen. Dit gaat gepaard met een groeiende behoefte bij politie en OM aan gegevens die andere organisaties hebben en die niet alleen mogelijk relevant voor de fase van opsporing en vervolging zijn, maar ook voor de fase waarin nog geen sprake van een (vermoeden van een) strafbaar feit en van een mogelijke verdachte is, maar wel behoefte bestaat aan het signaleren van trends en het maken van analyses om de criminaliteit beter te kunnen bestrijden. Het kan daarbij gaan om analyses in een concrete casus, waarbij partijen gezamenlijk bepalen welke interventies de meeste geschikte zijn om in de desbetreffende casus op te treden. Voor politie en OM kan dat betekenen dat men een voorbereidend onderzoek start. Het kan ook gaan om een situatie 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 opsporingsinstanties kunnen bij uitstek meerwaarde hebben bij fraudebestrijding en andere activiteiten op het terrein van de rechtshandhaving 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 Wetboek van Strafvordering (WvSv) in de artikelen 126nc e.v. een uitgebalanceerd en uitgewerkt systeem voor het vorderen van informatie door politie en OM. Dit hangt samen met de bevoegdheden die de politie en het OM hebben om met die gegevens wat te doen. Wanneer het OM in het kader van een samenwerkingsverband over gegevens komt te beschikken die

het vervolgens kan inzetten ten behoeve van opsporing en vervolging ontstaat een parallelle mogelijkheid voor het OM gegevens te verkrijgen buiten het Wetboek van Strafvordering om, zonder de waarborgen die dat wetboek biedt. 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 zwijgrecht. Als onderdeel van het recht op een "fair trial" wordt gezien de noodzaak van het hebben van een "paper trail": er moet worden vastgelegd welke informatie waarvandaan komt. Aan de hand van de "trail" kan worden beoordeeld of de informatie rechtmatig is verkregen. Rechtmatige informatieverkrijging via samenwerkingsverbanden dient derhalve nauwkeurig te worden omschreven. Voorts verdient aandacht dat het belastingrecht een ander bewijsrecht kent dan het strafrechtelijke systeem. In het belastingrecht geldt de vrije bewijsleer. Conclusies kunnen worden getrokken en feiten kunnen komen vast te staan op basis van voldoende aannemelijkheid. Indien een feit dat aldus is komen vast te staan, wordt uitgewisseld met de opsporingsfase, kan dit ongemerkt op gespannen voet komen te staan met de strikte bewijsleer 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.

Al deze factoren geven de burger een bepaalde mate van bescherming. Bij de verstrekking van gegevens vanuit het bestuursrechtelijk aan het strafrechtelijk domein binnen samenwerkingsverbanden 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 gevoelig zijn, aan de politie en andere opsporingsdiensten, respectievelijk aan het OM waarvoor nu ingevolge artikel 126nc, respectievelijk 126nd WSV een vordering nodig is. 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. Beide artikelen zijn destijds geschreven met in het achterhoofd het vorderen van gegevens van private partijen, zoals banken, die liever een vordering kregen dan dat zij vrijwillig verstrekten. Bestuursorganen die aan samenwerkingsverbanden 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 achtergronden van het verzoek. Het is in dat geval dan ook niet nodig de verantwoordelijkheid voor het vergaren van gegevens uitsluitend neer te leggen bij de met opsporing belaste instanties.

Nu de ratio achter de artikelen 126nc en 126nd WSV in het geval van gegevensuitwisseling binnen samenwerkingsverbanden ontbreekt, levert het

vereiste van een vordering een onnodige belemmering voor een efficiënte gegevensuitwisseling binnen samenwerkingsverbanden op. De Voorzitter van het College van Procureurs-Generaal heeft de Minister van Veiligheid van Justitie daarom bij brief van 4 juni 2012 verzocht de wetgeving zo aan te passen dat een versterking van gegevens binnen een samenwerkingsverband mogelijk is zonder dat daaraan een vordering op grond van het stelsel van strafvorderlijke bevoegdheden ten grondslag ligt. Weliswaar lijkt er op grond van een arrest van het Hof Arnhem-Leeuwarden ([redacted]) 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 WSV nodig is, maar de Hoge Raad heeft deze uitspraak nog niet bevestigd. Los van dit specifieke geval blijkt uit de jurisprudentie met betrekking tot artikel 126nd WSV dat een vordering door het OM als daarin bedoeld alleen dan achterwege kan blijven, indien de verstrekking van de desbetreffende gegevens niet alleen vrijwillig, maar ook uit eigen beweging geschiedt. Aangenomen mag worden dat eenzelfde lijn geldt voor een vordering van identificerende gegevens als bedoeld in artikel 126nc. Zo lang deze lijn voor andere gevallen dan gegevensverstrekking door de Belastingdienst aan het OM blijft 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. Tegen deze achtergrond bevat wetsvoorstel dit wetsvoorstel wijzigingen van het Wetboek van Strafvordering die erop neer komen vorderingen als bedoeld in de artikelen 126nc en 126nd achterwege kunnen blijven, indien een bestuursorgaan de desbetreffende gegevens verstrekt aan een samenwerkingsverband als bedoeld in de kaderwet.

3.3.6 Verantwoordelijke voor de gegevensverwerking

Het is uit een oogpunt van bescherming van persoonsgegevens van belang duidelijk vast te stellen wie met betrekking tot de gegevensverwerking als verantwoordelijke in de zin van de Wet bescherming persoonsgegevens c.q. verwerkingsverantwoordelijke in de zin van de Algemene Verordening Gegevensbescherming is aan te merken. Op deze verantwoordelijke rusten immers verschillende verplichtingen, zoals de beveiligingsplicht, de meldingsplicht en de verplichting betrokkenen gebruik te kunnen laten maken van hun inzage- en correctierecht.

Als er sprake is van een samenwerkingsverband, kan dat een discussie oproepen over de vraag wie verantwoordelijke is voor de gegevensverwerking binnen het samenwerkingsverband. Overwogen is om, in navolging van artikel 64, tweede lid, van de Wet Suwi, als uitgangspunt te kiezen voor een gezamenlijke verantwoordelijkheid van de deelnemers aan het samenwerkingsverband. Dit uitgangspunt komt overeen met de keuze die men, gelet op het geïntegreerde 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 bestaan dat, ook al nemen aan de verwerkingen verschillende organisaties deel, er voor één gemeenschappelijke verantwoordelijke wordt gekozen.⁴ 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 keuze voor één verantwoordelijke biedt, mag niet ten koste gaan van de mate waarin aan deze verantwoordelijkheid invulling kan worden gegeven.

Teneinde voldoende ruimte voor verschillend keuzes met betrekking tot de regeling van de verantwoordelijkheid voor de gegevensverwerking te houden, is er van afgezien in het wetsvoorstel zelf te bepalen wie als verantwoordelijke dient te worden aangemerkt. Om toch te bewerkstelligen dat er op dit punt voldoende duidelijkheid is, bevat het wetsvoorstel wel de verplichting in een informatieprotocol vast te leggen wie de verantwoordelijke voor de gegevensverwerking in het samenwerkingsverband is. Het gaat hier uitsluitend om de verwerking van gegevens *binnen* het samenwerkingsverband. De deelnemers zijn en blijven ieder voor zich verantwoordelijke in de zin van de Wet bescherming persoonsgegevens voor het verstrekken van gegevens *aan* het samenwerkingsverband.

Indien men ervoor kiest in het informatieprotocol vast te leggen dat de deelnemers gezamenlijk verantwoordelijke zijn, kan dat het risico 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 uitoefening van hun rol als verantwoordelijke. De huidige praktijk kent hiervan reeds enkele voorbeelden.⁵ Het gaat hier om een louter ondersteunende rol; zij neemt de gezamenlijke verantwoordelijkheid van de partners niet weg. In de kaderwet zelf behoeft zij dan ook geen expliciete regeling. Wel kunnen partijen er desgewenst voor kiezen de rol van regisseur in het informatieprotocol vast te leggen.

3.3.7 Individuele informatieplicht

In de praktijk blijkt dat samenwerkingsverbanden worstelen met de vraag of en, zo ja, in hoeverre zij moeten voldoen aan de informatieplicht van artikel 34 Wbp (art. 14 Algemene Verordening Gegevensbescherming (AVG)). Die vraag speelt vooral in het geval van grootschalige geautomatiseerde bestandsvergelijkingen in een fase die voor het overgrote deel van de betrokkenen niet tot gevolgen leidt. De informatieplicht houdt in dat iedere betrokkene door de verantwoordelijke wordt geïnformeerd over de verwerking van zijn of haar persoonsgegevens. Deze plicht is niet van toepassing, indien mededeling van de informatie aan de betrokkenen onmogelijk blijkt of een onevenredige inspanning kost. In dat geval

⁴ Kamerstukken II 1997-1998, 25892, nr. 3, blz. 58.

⁵ die in artikel is aangewezen.

legt de verantwoordelijke de herkomst van de gegevens vast (art. 34, vierde lid, Wbp; art. 14, vijfde lid, onder b, AVG). Zij is ook niet van toepassing, indien de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven. In dat geval dient de verantwoordelijke de betrokkene op diens verzoek te informeren over het wettelijk voorschrift dat tot vastlegging of verstrekking van de hem betreffende gegevens heeft geleid (art. 34, vijfde lid, Wbp; art. 14, vijfde lid, onder c, AVG).

Op grond van dit wetsvoorstel komen in verschillende sectorale wetten bepalingen te staan die deelnemers aan een samenwerkingsverband als bedoeld in de Kaderwet ertoe verplichten om – uitzonderingen daargelaten – aan dat samenwerkingsverband de gegevens te verstrekken die noodzakelijk zijn om het doel van dat verband te bereiken. Dit brengt mee dat niet iedere betrokkene afzonderlijk behoefte te worden geïnformeerd over de verwerking van zijn of haar gegevens. 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. Van belang is ook dat het in samenwerkingsverbanden op sommige terreinen – denk hierbij aan fraudebestrijding – al gauw om gegevensverwerking kan gaan die, als zij bij betrokkenen bekend wordt, tot calculerend gedrag bij hen kan leiden.

De transparantie van de gegevensverwerking wordt wel op geaggregeerd niveau gewaarborgd. Het wetsvoorstel schrijft voor dat de deelnemers aan een samenwerkingsverband in een convenant onder meer het doel van de samenwerking vastleggen, alsmede de taken en werkzaamheden die binnen het verband worden uitgevoerd. Het wetsvoorstel schrijft ook voor in een informatieprotocol nadere regels dienen vast te leggen over de verwerking van gegevens in het verband. Zo dient het protocol onder meer een beschrijving te bevatten van de gegevens dan wel soorten daarvan die in het samenwerkingsverband worden verwerkt, een beschrijving van de inrichting van het proces van gegevensverwerking en de waarborgen die hierin zijn opgenomen met het oog op de bescherming van persoonsgegevens en regels over de verstrekking van informatie over de gegevensverwerking aan het publiek en aan betrokkenen. Zowel het convenant als het informatieprotocol dienen te worden gepubliceerd in de Staatscourant. Op basis van het convenant en het informatieprotocol is aldus in algemene zin genoegzaam af te leiden welke gegevens ten behoeve van welk doel worden verwerkt. De kenbaarheid van de gegevensverwerking kan verder worden vergroot via de gebruikelijke voorlichtingsactiviteiten op websites en door middel van brochures.

3.3.8 e.v. Andere onderwerpen, w.o. waarborgen voor een zorgvuldige gegevensverwerking

PM

4. Voorbereiding van het wetsvoorstel

4.1 Inleiding

4.2 Grondrechtentoets

4.3 Privacy Impact Assessment

4.4 Consultatie

5. Financiële gevolgen

6. Administratieve lasten en bestuurslasten

II. ARTIKELSGEWIJS

Artikel 1 Begripsbepalingen

PM

Gegevens

Gegevens zijn te omschrijven als de vastgelegde uitdrukking van feiten. Omwille van de duidelijkheid is in het tweede lid bepaald dat de term gegevens in deze wet ook ziet op persoonsgegevens als bedoeld in de Wet bescherming persoonsgegevens (Wbp), justitiële en strafvorderlijke gegevens als bedoeld in de Wet justitiële en strafvorderlijke gegevens (Wjsg) en politiegegevens als bedoeld in de Wet politiegegevens (Wpg).

Onder persoonsgegevens verstaat artikel 1 Wbp "elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon". Onder verwerking van persoonsgegevens verstaat de Wbp "elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens". Onder verantwoordelijke verstaat de Wbp "de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

De Wjsg verstaat onder justitiële gegevens: bij algemene maatregel van bestuur te omschrijven persoonsgegevens of gegevens over een rechtspersoon inzake de toepassing van het strafrecht of de strafvordering. Onder strafvorderlijke gegevens wordt in deze wet verstaan: persoonsgegevens of gegevens over een rechtspersoon die zijn verkregen in het kader van een strafvorderlijk onderzoek en die het openbaar ministerie in een strafdossier of langs geautomatiseerde weg verwerkt.

De Wpg verstaat onder politiegegevens: elk persoonsgegeven dat in het kader van de politietaak wordt verwerkt.

Artikel 2

Dit artikel regelt de reikwijdte van deze wet. De wet is van toepassing op een samenwerkingsverband indien de deelnemers bij convenant zijn overeengekomen dat deze wet op hun samenwerkingsverband van toepassing is en mits dit convenant voldoet aan de eisen gesteld in artikel 3. Op deze wijze zal

geen misverstand kunnen bestaan over de vraag of een samenwerkingsverband onder de werking van de kaderwet valt. Een samenwerkingsverband dat onder de werking van de kaderwet valt krijgt de beschikking over betere mogelijkheden tot gegevensuitwisseling dan een samenwerkingsverband dat niet onder deze wet valt (zie artikel 7).

De deelnemers aan een samenwerkingsverband gaan de samenwerking aan met het oog op een publiek belang. Dit gemeenschappelijke publieke belang moet, vanwege het principe van doelbinding, concreet worden geformuleerd en moet gelegen zijn op het brede terrein van: a. het voorkomen en bestrijden van onrechtmatig gebruik van overheidsmiddelen en overheidsvoorzieningen, b. het houden van toezicht op de naleving van wettelijke voorschriften, c. het handhaven van de openbare orde en veiligheid of d. het voorkomen, opsporen en vervolgen van strafbare feiten.

De deelnemers aan een samenwerkingsverband werken hun samenwerking nader uit in een convenant en een informatieprotocol (zie de artikelen 3 en 4). Voorstelbaar is dat na verloop van tijd behoefte ontstaat nieuwe deelnemers toe te laten tot een samenwerkingsverband. Het vereiste dat er sprake moet zijn van een welbepaald doel dat past binnen de doeleinden die in het tweede lid onder a tot en met d zijn geformuleerd, geldt onverkort voor het samenwerkingsverband in de nieuwe samenstelling. Het tweede lid stelt dit buiten twijfel. Als er niet meer wordt voldaan aan het vereiste, valt het samenwerkingsverband niet meer onder de reikwijdte van deze wet. Op grond van artikel 3 regelen de deelnemers aan het samenwerkingsverband ook uittreding uit en opheffing van het samenwerkingsverband bij convenant.

Op grond van het vierde lid kunnen overheidsinstanties uitsluitend deelnemen aan een samenwerkingsverband indien daarvoor een grondslag in een wet in formele zin bestaat. Van een samenwerkingsverband kunnen zowel publieke als private partijen deel uitmaken. Vanwege de publieke belangen die worden nagestreefd met een samenwerkingsverband, zal het niet kunnen bestaan uit uitsluitend private partijen, maar zal er altijd ten minste een overheidsinstantie deel van uitmaken. Of een privaatrechtelijke organisatie deelneemt aan een samenwerkingsverband kan zij zelf bepalen. Voor deze organisaties geldt daarom niet het vereiste van een grondslag in een wet. Uiteraard kunnen ook zij alleen deelnemen aan een samenwerkingsverband voor zover hun deelname noodzakelijk is voor het doel of de doelen van het samenwerkingsverband.

Deze wet heeft betrekking op alle samenwerkingsverbanden, ongeacht of de deelnemers hoofdzakelijk nationaal, regionaal dan wel lokaal werken of dat het samenwerkingsverband bestaat uit een mix van nationaal, regionaal of lokaal werkende deelnemers bestaat.

Artikel 3

De deelnemers in een samenwerkingsverband regelen hun samenwerking in een convenant. In paragraaf @@@ van deze toelichting is ingegaan op alternatieven voor convenanten die in overweging zijn genomen. Dit artikel geeft minimumeisen waaraan een dergelijk convenant dient te voldoen. In het convenant dient het doel van de samenwerking te worden omschreven (onderdeel a). Op grond van artikel 2 streven de deelnemers aan een samenwerkingsverband een gemeenschappelijk doel na ten behoeve van een publiek belang. Dit gemeenschappelijk doel moet, vanwege het principe van doelbinding, concreet worden geformuleerd en moet gelegen zijn op het brede terrein van: a. het voorkomen en bestrijden van onrechtmatig gebruik van overheidsmiddelen en overheidsvoorzieningen, b. het houden van toezicht op de naleving van wettelijke voorschriften, c. het handhaven van de openbare orde en veiligheid of d. het voorkomen, opsporen en vervolgen van strafbare feiten. Voorts dient in het convenant een aantal meer praktische zaken te worden geregeld (onderdelen b tot en met g). De regeling van de onder c 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. Ook kan worden gedacht aan een regeling van verplichtingen met betrekking tot de bekostiging van de samenwerking, inclusief een eventueel ondersteunend bureau. Met de regeling dient tevens te worden voldaan aan artikel 26 AVG. Op grond van dit artikel zijn de deelnemers immers gezamenlijke verwerkingsverantwoordelijken en dienen zij op transparante wijze hun respectievelijke verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van de verordening vast te stellen.

Artikel 4

Naast een convenant dienen de deelnemers een informatieprotocol op te stellen. In dit informatieprotocol leggen zij een aantal zaken vast die bij de gegevensverwerking in een samenwerkingsverband in het belang van gegevensbescherming nodig zijn. Omdat in een samenwerkingsverband niet alleen persoonsgegevens kunnen worden uitgewisseld, maar bijvoorbeeld ook bedrijfsgegevens, wordt de term informatieprotocol gehanteerd, in plaats van privacyprotocol. Het tweede lid bevat een niet-uitputtende opsomming. De deelnemers aan het samenwerkingsverband kunnen desgewenst andere elementen aan het informatieprotocol toevoegen.

Lid 2

Het informatieprotocol zal een nadere aanduiding moeten geven van de soorten gegevens die binnen een samenwerkingsverband worden uitgewisseld (onderdeel a).

Onderdeel b verplicht tot het beschrijven van de inrichting van het proces van gegevensuitwisseling. Daarbij gaat het om een beschrijving van het proces van

gegevensverwerking en van het eventuele gebruik van een informatiesysteem daarbij. 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 gegevensuitwisseling (eerst "hit-no hit", pas bij voldoende hits uitwisseling van de inhoud van gegevens) en vormen van pseudonimisering.

Bij informatieverstrekking aan het publiek (onderdeel e) kan worden gedacht aan informatieverstrekking over het doel van het samenwerkingsverband en de categorieën van gegevens die hiertoe 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, Wbp is het niet nodig iedere persoon van wie in het samenwerkingsverband persoonsgegevens worden verwerkt, daarvan persoonlijk op de hoogte te stellen. Wel dient betrokkene op diens verzoek te worden geïnformeerd over het wettelijke voorschrift dat tot vastlegging of verstrekking van de desbetreffende gegevens heeft geleid. Uit onderdeel f vloeit voort dat het informatieprotocol ook daarover nadere regels dient te bevatten.

Voor de beveiliging van gegevens verdient het aanbeveling in het informatieprotocol de richtsnoeren die het College bescherming persoonsgegevens, thans de Autoriteit Persoonsgegevens, daartoe heeft opgesteld, als uitgangspunt te nemen (Zie Stcrt. 2013, 5174).

Het informatieprotocol zou ter uitvoering van onderdeel g 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.

Artikel 5

Op grond van dit artikel worden het convenant en het informatieprotocol openbaar gemaakt zodat transparant is voor welke doeleinden er gegevens worden verwerkt in het samenwerkingsverband en hoe binnen het samenwerkingsverband wordt gewerkt en wordt omgegaan met gegevens. Het convenant dient in de Staatscourant te worden gepubliceerd (Aanwijzing 25 Aanwijzingen voor convenanten). Het informatieprotocol wordt ook openbaar gemaakt, maar het staat het samenwerkingsverband c.q. de deelnemers vrij om te bepalen op welke wijze dit gebeurt. Als het samenwerkingsverband een website heeft, ligt het voor de hand dat het informatieprotocol daarop wordt openbaar gemaakt. De individuele deelnemers kunnen het desgewenst ook op hun eigen website opnemen. Overigens staat het de deelnemers uiteraard vrij

om het convenant behalve in de Staatscourant, ook nog op een andere wijze openbaar te maken, bijvoorbeeld samen met het informatieprotocol zodat alle informatie bij elkaar te vinden is.

In verband met deze openbaarmakingsplicht is in het derde lid bepaald dat er in samenwerkingsverbanden die zijn overeengekomen dat zij onder de reikwijdte van deze wet willen vallen, geen gegevens worden verwerkt voordat het convenant en het informatieprotocol zijn openbaar gemaakt.

Artikel 6

Dit artikel heeft betrekking op de herkomst van gegevens. Gegevens die het samenwerkingsverband verwerkt zijn afkomstig van de deelnemers en uit voor een ieder toegankelijke informatie bronnen. Een belangrijke, wellicht zelfs de belangrijkste, bron van de gegevens zullen bij een samenwerkingsverband de deelnemers zelf zijn. De samenwerking zal immers mede gestoeld zijn op de veronderstelling dat de deelnemers over gegevens beschikken die voor andere deelnemers met het oog op het doel van het samenwerkingsverband van belang zijn. De gegevens kunnen echter ook een andere herkomst hebben, zoals openbare registers, gegevens uit andere openbare bronnen, gegevens uit registraties met authentieke gegevens, zoals de Basisregistratie personen.

Artikel 7

Dit artikel regelt wat er met de gegevens die binnen het samenwerkingsverband worden verwerkt, mag worden gedaan. De gegevens kunnen worden gebruikt voor casusanalyse en geautomatiseerde data-analyse. Dit artikel geeft derhalve een expliciete basis voor geautomatiseerde data-analyse met betrekking tot gegevens uit eigen geautomatiseerde gegevensbestanden en gegevens uit voor een ieder toegankelijke informatiebronnen. Uit het tweede lid volgt dat alle vormen van data-analyse onder de in het eerste lid geëxpliciteerde bevoegdheid kunnen worden begrepen. Deze opsomming is niet limitatief omdat de toepassing van eventuele nieuwe methoden en technieken mogelijk moet zijn. In het tweede lid worden echter drie veel voorkomende vormen van data-analyse benoemd: (a) het op geautomatiseerde wijze onderling vergelijken, dan wel in combinatie met elkaar vergelijken van gegevens, (b) het doorzoeken van gegevens aan de hand van profielen en (c) het vergelijken van gegevens met het oog op het opsporen van bepaalde patronen.

Waar met de rapporten waarop onderdeel a van het derde lid ziet, bedoeld wordt op documenten met een louter beschrijvend karakter, wordt ervan uitgegaan dat adviezen als bedoeld in onderdeel b, aanbevelingen bevatten, bijvoorbeeld met betrekking tot het uitvoeren van een gezamenlijke interventiestrategie. De acties waarop onderdeel b doelt, kunnen zijn opgenomen in zo'n 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. Denkbaar is dat een interventiestrategie ook acties omvat die door andere organisaties dan de deelnemers zullen moeten worden uitgevoerd.

Gegevens kunnen op verschillende wijzen worden verwerkt. Zo kan er sprake zijn van handmatige verwerking. Daarbij valt te denken aan schriftelijke en mondelinge gegevensuitwisseling tijdens zogenaamde informatietafels of -pleinen in samenwerkingsverbanden. Maar uiteraard kan er ook sprake zijn van geautomatiseerde verwerking. Gedacht kan worden aan (beveiligde) systemen om de gegevensuitwisseling zorgvuldig te ontvangen en door te zenden en eventueel op maat vorm te kunnen geven. In dat geval is het gebruik van ICT slechts ondersteunend. Voorbeelden van dergelijke systemen zijn het "Colleges Collaboration Tool" (CoCoTo) van het FEC en het RIEC-IS van de RIEC's (Zie p. 28 van het jaarverslag 2012 van het LIEC: http://www.liec.nl/doc/130136_RIEC-LIECJaarverslag_web.pdf). Bij deze systemen vervult het secretariaat van het samenwerkingsverband een belangrijke handmatige rol bij het verdelen en uitzetten van de gegevens. Ook kan worden gedacht aan geautomatiseerde kruispuntbanken waarbij gegevens op basis van een informatie- en autorisatiemodel geheel automatisch van bronhouder naar eindgebruiker gaan. Voorbeelden hiervan zijn Inspectieview Bedrijven en Inspectieview Milieu van de Inspectie Transport en Leefomgeving en Suwi-inkijk. Tot slot zijn er samenwerkingsverbanden waar ICT-toepassingen centraal staan en voor een groot deel het primair proces beslaan. Hierbij kan worden gedacht aan gegevensuitwisseling door koppeling van bestanden van verschillende partners om met behulp van geavanceerde software bepaalde patronen te ontdekken ("datamining"), gerichte bevestigingen in databestanden van verschillende partners om bepaalde profielen vast te stellen ("profiling"). Een voorbeeld van dergelijke verwerkingen zijn verwerkingen met behulp van het Systeem Risico Indicatie (SyRI, zie art. 65 Wet SUWI).

Artikel 8

Artikel 8 bevat een aantal waarborgen dat moet bijdragen aan de kwaliteit van de gegevens en de zorgvuldige verwerking daarvan. Het heeft betrekking op zaken die moeten zijn gedaan voordat wordt overgegaan tot uitwisseling van gegevens. Op grond van het eerste lid van dit artikel onderbouwt het samenwerkingsverband in geval van een voorgenomen nieuwe uitwisseling van gegevens aan dat deze gegevensuitwisseling noodzakelijk is voor het doel van het samenwerkingsverband en dat deze gegevensuitwisseling passend is gelet op dit doel. Het doel van het samenwerkingsverband blijkt uit het convenant (zie art. 3) en ligt op het brede terrein van: a. het voorkomen en bestrijden van onrechtmatig gebruik van overheidsmiddelen en overheidsvoorzieningen, b. het

houden van toezicht op de naleving van wettelijke voorschriften, c. het handhaven van de openbare orde en veiligheid of d. het voorkomen, opsporen en vervolgen van strafbare feiten (zie art. 2). Daarnaast moet het samenwerkingsverband door middel van een Privacy Impact Assessment onderbouwen dat de privacy van de betrokkenen voldoende is gewaarborgd en de te nemen maatregelen motiveren. Deze eisen, waarvan een deel ook volgt uit artikel 8 van het Europees Verdrag voor de Rechten van de Mens, vormen een concretisering van de beginselen inzake verwerking van persoonsgegevens in artikel 5 van de Algemene verordening gegevensbescherming en artikel 4 van Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

Op grond van het tweede lid worden de onderbouwing en de PIA openbaar gemaakt op een voor het publiek toegankelijke wijze. Dit kan bijvoorbeeld geschieden door de informatie op de website van het samenwerkingsverband te plaatsen. De openbaarmaking garandeert een voor betrokkenen behoorlijke en transparantie verwerking van gegevens.

Artikel 9

Ook dit artikel bevat een aantal waarborgen dat moet bijdragen aan de kwaliteit van de gegevens en de zorgvuldige verwerking daarvan. Anders dan artikel 8, dat betrekking had op zaken die moesten zijn gedaan voordat de beslissing wordt genomen om gegevens uit te wisselen, ziet dit artikel op de gegevensverstrekking zelf. Het eerste lid gaat over de toepassing van vormen van anonimisering (de gegevens zijn niet herleidbaar tot een natuurlijke persoon) en pseudonimisering (het met een bepaald algoritme vervangen van identificerende gegevens door versleutelde gegevens). Dergelijke vormen dienen zo mogelijk in het proces van gegevensverwerking te worden ingepast conform het principe van "privacy by design". Een goed voorbeeld hiervan vormt de pseudonimisering die in het proces van gegevensverwerking met behulp van SyRi plaatsvindt. Dit proces houdt in dat aan de hand van gepseudonimiseerde gegevens het 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. De potentiële treffers worden vervolgens ontsleuteld voor een nadere analyse op naam (vgl. Kamerstukken II 2012/13, 33 579, nr. 3, p. 3 e.v. en artikel 5a.2 Besluit SUWI).

Uit een oogpunt van het waarborgen van de kwaliteit van gegevens, bepaalt het tweede lid dat bij de verstrekking van gegevens aan of door het samenwerkingsverband, inzicht wordt gegeven in de graad van juistheid en betrouwbaarheid van de gegevens. Zoals ook in paragraaf @@@ van het algemeen deel van deze toelichting is vermeld, is het van groot belang dat altijd

de context waarbinnen een gegeven is verzameld of ontstaan wordt meegegeven indien een gegeven wordt verstrekt aan een ander. Gegevens die uit bronnen met verschillende, soms zeer uiteenlopende doeleinden worden geput, worden, wanneer zij worden gecombineerd met andere gegevens in een andere beleidscontext, gedecontextualiseerd en vervolgens gehercontextualiseerd. Daaraan kleven risico's voor de kwaliteit van de gegevens in termen van betrouwbaarheid en kenbaarheid. Met het tweede lid wordt beoogd deze risico's te minimaliseren. Voorts draagt de vermelding van de context waarbinnen een gegeven verkregen of verzameld is bij aan het beginsel dat gegevens juist moeten zijn (artikel 5, eerste lid, onderdeel d, AVG).

Artikel 10

Dit artikel heeft specifiek betrekking op het koppelen van bestanden met het oog op big-data-analyses of data-mining. Dergelijke analyses kunnen, zoals de Wetenschappelijke Raad voor het Regeringsbeleid in het recente rapport "Big Data in een vrije en veilige samenleving", schreef een effectieve bijdrage leveren aan de maatschappelijke veiligheid en vrijheid (Kamerstukken II, 2016/17 @@@, p. 135). Dit artikel reguleert de analyse van aan een samenwerkingsverband verstrekte gegevens en het gebruik van de na de analyse verkregen nieuwe gegevens. De onderdelen a en b zien op de analyse en bepalen dat inzichtelijk moet worden gemaakt hoe de selectie van de te koppelen bestanden heeft plaatsgevonden en uit wat voor soort gegevens die bestanden bestaan. De verplichting om dit inzichtelijk te maken rust op het samenwerkingsverband. Bestanden kunnen uit veel verschillende soorten gegevens bestaan. Gedacht kan bijvoorbeeld worden aan ongestructureerde en ongelijksoortige data zoals video's, foto's en boeken, maar data kunnen ook het product zijn van gerichte verzameling, geautomatiseerde processen of vrijwillige verstrekking. Het samenwerkingsverband dient hierover inzicht te kunnen verschaffen.

Voorts dient het samenwerkingsverband inzicht te verschaffen over de algoritmes en methoden die bij de analyse van de verkregen gegevens worden gebruikt en over de vraag wat men van plan is te gaan doen met de door de analyse verkregen nieuwe gegevens. Met de WRR zijn wij van mening dat de algoritmes en methoden die bij data-analyses worden gebruikt deugdelijk moeten zijn en aan wetenschappelijke criteria voor goed (statisch) onderzoek voldoen.

Artikel 11

@@@

Paragraaf 4 Wijzigingen in andere wetten

PM

Paragraaf 5 Overgangs- en slotbepalingen

PM

De minister van Veiligheid en Justitie,
G.A. van der Steur