Kennis is macht, kennis delen is kracht

ctr FIN in revisie 11092014

Rapport van de Werkgroep Verkenning kaderwet gegevensuitwisseling

Versie 1.2

Prealabele opmerkingen:

De procedure

1. (Ambtelijk) FIN heeft zich aangeboden als deelnemer aan de werkgroep Verkenning Kaderwet vanuit de veronderstelling dat in een brede, open discussie een analyse van knelpunten bij gegevensuitwisseling zou worden verricht en nagedacht over mogelijke oplossingsrichtingen. Helaas constateren wij dat inmiddels eenzijdig en blijkbaar vanuit een van tevoren reeds vastgelegde doelstelling thans teksten voorliggen die ook al breed buiten de werkgroep om worden afgestemd. Dit achten wij jammer en een gemiste kans omdat daarmee een gedegen analyse van de knelpunten die zich op het brede terrein van gegevensuitwisseling voordoen ontbreekt en direct wordt toegewerkt naar de (deel) problematiek van (bepaalde) samenwerkingsverbanden. Een en ander wreekt zich oi ook omdat ook de proeve ervan blijk geeft dat zonder een principiële en structurele discussie echte oplossingen helaas nog steeds ver weg zijn.

2. Eea zo zijnde willen wij ook geen spelbreker zijn en ervan zien te maken wat ervan te maken is; ons navolgend ctr dient in dat licht te worden bezien.

De inhoud

3. In het rapport wordt geconstateerd dat een beperking tot samenwerkingsverbanden ikv fraudebestrijding onwerkbaar is voor samenwerkingsverbanden die ook betrekking hebben op toezicht en handhaving. Dezelfde redenering geldt ten aanzien van overheidsoptreden rond het nemen van primaire beschikkingen ("de voorkant").

4. Vooralsnog ontbreekt in het rapport de relatie tussen de geschetste kaderwet en overige wetgeving op het gebied van gegevensverwerking (Wbp, SUWI, materiewetten, Wpg etc).

5. De kaderwet richt zich (enkel) op (bepaalde) samenwerkingsverbanden: onduidelijk echter is de afstemming tussen bedoelde samenwerkingsverbanden

heeft opmaak toegepast: Lettertype: 10 pt

heeft opmaak toegepast: Lettertype: Verdana, 10 pt, Vet

heeft opmaak toegepast: Lettertype: Verdana, 10 pt, Vet

heeft opmaak toegepast: Lettertype: Verdana, 10 pt, Vet

heeft opmaak toegepast: Lettertype: Verdana, 10 pt, Vet

heeft opmaak toegepast: Lettertype: Verdana, 10 pt, Vet

heeft opmaak toegepast: Lettertype: Verdana, 10 pt, Vet

en gegevensuitwisseling tussen overheidsdiensten en ter zake geldende regelgeving.

6. De duiding van kaderwet is onduidelijk; of de kaderwet bevat het kader voor het bestreken terrein en alle nadere uitwerking binnen dat terrein dient te passen binnen de gegeven kaders of de wet bevat de begrippen, normen, procedures etc die zonder nadere uitwerking voor het terrein gelden (a la Awb). Deze "kaderwet" voldoet noch aan de ene noch aan de andere definitie.

7. Onduidelijk is wat het in de kaderwet geregelde samenwerkingsverband doet/is. Gaat het bijvoorbeeld om gegevensuitwisseling binnen de context van het samenwerkingsverband of gaat het om het behalen van een van de vier in de kaderwet genoemde doeleinden? Dit klemt temeer nu rond het verschijnsel samenwerkingsverband zich vele vragen voordoen in de praktijk waar de kaderwet in het geheel niet op ingaat. Te denken valt bijvoorbeeld aan: leveren de deelnemers aan elkaar (en steeds aan alle deelnemers) of leveren de deelnemers aan het samenwerkingsverband als zodanig (dat op zijn beurt weer doorlevert), hoe is de Wbp verantwoordelijkheid geregeld (wat is het verschil tussen gezamenlijke verantwoordelijkheid en gedeelde verantwoordelijkheid, kan een samenwerkingsverband als verwerker optreden, maakt het een verschil wat voor soort werkzaamheden binnen een samenwerkingsverband worden verricht en door wie, wat is de rol van een eventueel bureau/secretariaat, maakt het verschil of het samenwerkingsverband eigen bestanden creëert en aanhoudt, kan een samenwerkingsverband uit meer deelsamenwerkingsverbanden bestaan waarin het eigenlijke werk gebeurt (denk aan LIEC/RIEC), is denkbaar dat deelnemers verschillende rollen vervullen dan wel dient ieder per definitie gelijkelijk te worden behandeld, hoe gaat het samenwerkingsverband om met de gegevens wanneer deze eenmaal zijn verwerkt, kunnen gegevens die zijn uitgewisseld binnen het samenwerkingsverband ten behoeve van het doel van het samenwerkingsverband vervolgens door de deelnemers ook voor eigen doeleinden worden gebruikt, etc, etc.

8. Het rapport gaat sterk uit van fraudebestrijding terwijl wat ons betreft de invalshoek dient te zijn de problemen bij gegevensuitwisseling (bv op het gebied van fraudebestrijding maar niet alleen).

9. Het lijkt de bedoeling te zijn dat de kaderwet niet betrekking heeft op bestaande samenwerkingsverbanden; dan biedt de kaderwet dus alleen "oplossingen" voor nieuwe gevallen. Bijvoorbeeld voor de BD geldt dat die dienst als beleid heeft geen nieuwe samenwerkingsverbanden aan te gaan buiten de bestaande waarmee de vraag opkomt voor welke samenwerkingsverbanden de kaderwet moet gaan gelden?

10. Als de kaderwet alleen voor eventuele nieuwe gevallen gaat gelden, ontstaat dan niet het probleem dat er nog weer een regime bij alle al bestaande regimes wordt gevoegd waarmee de onduidelijkheid alleen maar groter wordt?

11. Ingevolge het door het kabinet ingevoerde IAK behoort ieder beleidsstuk een gedegen analyse van de probleemstelling te bevatten waarvoor het

voorstel een oplossing moet bieden. De probleemstelling wordt naar onze mening, ondanks aanzetten daartoe, onvoldoende uitgewerkt in het rapport.

12. De verschillende door FIN ingebrachte analyses, inzake "zorgvuldigheid", "scope" en "principiële karakter van de problematiek" zijn ondergesneeuwd geraakt in de voorliggende rapportage.

13. Dit wreekt zich bijvoorbeeld op het punt van de zorgvuldigheid. Hoewel lippendienst wordt bewezen aan het belang daarvan bij gegevensverwerking, gaat het rapport ervan uit dat met het opnemen van ruime doelstellingen in de kaderwet daarmee iedere afweging in zake "verenigbaarheid met " niet langer nodig is. Dit zou een van de grote winstpunten van het voorstel moeten zijn. De FIN analyse inzake de mogelijke rol van het begrip zorgvuldigheid bij gegevensverwerking komt nu juist tot de conclusie dat op ieder niveau van gegevensverwerking (wet, lagere regelgeving en uitvoering) dit begrip iedere keer op dat niveau een rol speelt.

14. De rapportage ontbeert vooralsnog node een stevige paragraaf inzake de waarborgen vanuit privacy overwegingen.

15. Bij een verkenning naar omgaan met verwerking van persoonsgegevens binnen het overheidsdomein zou op zijn minst een aanbeveling passen hier een rechtsvergelijkend onderzoek naar te doen. Het schijnt namelijk dat de problematiek van het uitwisselen van persoonsgegevens binnen het overheidsdomein (samenwerkingsverbanden) met name in Nederland speelt. Dit kan te maken hebben met de sterk verkokerde wet- en regelgeving ten aanzien van gegevensverwerking binnen Nederland.

16. De passage inzake het laten vallen van de vorderingsverplichting door het OM, achten wij zeer ongelukkig in het licht van de lopende principiële discussie ter zake. Hier worden twee zaken door elkaar gehaald; aan de ene kant speelt het onschuldige punt van het kunnen verkrijgen van gegevens door het OM binnen het samenwerkingsverband, aan de andere kant speelt het principiële punt of gegevens die eenmaal zijn verkregen door het OM binnen het samenwerkingsverband (en – enkel - met het oog op het doel van het samenwerkingsverband) zonder nadere vordering door het OM kunnen worden aangewend voor doeleinden buiten het samenwerkingsverband. FIN acht het ten principale niet juist dat de verantwoordelijkheid voor de beoordeling of gegevens ten behoeve van opsporing en vervolging mogen dienen verschuift van de OvJ die als enige de feiten van de casus kent (is sprake van een vermoeden/ een verdachte en rechtvaardigt de ernst van de overtreding een gegevensopvraag) naar het gegevensverstrekkende bestuursorgaan dat die kennis niet in huis heeft.

17. Normaliter bevat een dergelijk rapport een paragraaf over de door de werkgroep gevolgde aanpak, maar dat is in dit geval onder de gegeven omstandigheden een beetje lastig.

18. Er bestaat spanning in het feit dat deze kaderwet zich richt op gegevensuitwisseling binnen en in het kader van samenwerkingsverbanden, terwijl bij bestaande samenwerkingsverbanden de onderlinge gegevensuitwisseling nu juist is gebaseerd op bepalingen inzake bilaterale

gegevensuitwisseling (dus ook ten aanzien van samenwerkingsverbanden). Dit roept bv de vraag op of nu de kaderwet geldt dan wel die bestaande bilatreale gegevensuitwisselingsbepalingen.

19. Onduidelijk is ten aanzien van welke samenwerkingsverbanden de kaderwet geldt. Gesuggereerd is dat dit een kwestie van keuze is van het betrokken samenwerkingsverband die dat dan zou moeten aangeven in de desbetreffende onderlinge afspraak (het convenant). Dit lijkt een zwakke basis en een novum qua rechtskracht voor een wet. Zolang een dergelijke keuze niet wordt gemaakt geldt de wet, die in het Staatsblad staat, dus per saldo nergens voor.

PM

FIN had graag het bestaan van de werkgroep en dit jaar gebruikt om te komen tot een gedegen beoordeling van de knelpunten rond gegevensverwerking binnen het overheidsdomein zoals ervaren door tal van overheidsdiensten bij de toenemende wens tot gegevensdeling. Een dergelijke analyse had van groot nut kunnen zijn bij de komende discussie rond vervanging van de Wbp en de daarbij te nemen principiële besluiten. De huidige beperkte insteek maakt die ambitie onmogelijk.

In dit kader vinden wij het onverstandig in dit rapport opnieuw een aantal in het verleden gedane ongelukkige (regerings)uitspraken rond het niet bestaan van de behoefte aan een principiële en structurele heroriëntatie op het gebruik van beschikbare informatie binnen het overheidsdomein opnieuw te benadrukken, nu steeds duidelijker wordt dat die brede discussie er op korte termijn toch aankomt!

Het vervolg van ons ctr is in revisie de tekst zelf aangegeven

heeft opmaak toegepast: Lettertype: 10 pt

heeft opmaak toegepast: Lettertype: +Hoofdtekst (Calibri), 11 pt, Niet Vet

heeft opmaak toegepast: Lettertype: 10 pt

Den Haag, 27 augustus 2014

heeft opmaak toegepast: Lettertype: 10 pt

heeft opmaak toegepast: Lettertype: Verdana, 10 pt, Vet

heeft opmaak toegepast: Lettertype: 10 pt

Inhoudsopgave

Samenvatting ..... 8~~8~~5

1. Inleiding ..... 12~~12~~9

2. Context ..... 13~~13~~10

2.1 Aanleiding ..... 13~~13~~10

2.2 Samenwerkingsverbanden ..... 16~~16~~10

2.3 Verschillende categorieën gegevens ..... 18~~18~~13

2.4 Verschillende typen gegevensuitwisseling ..... 19~~19~~14

2.5 Belang van zorgvuldigheid bij gegevensuitwisseling ..... 21~~21~~16

2.6 Betere gegevensuitwisseling: zaak van meer dan wetgeving alleen ..... 22~~22~~16

2.7 Relevante andere ontwikkelingen ..... 23~~23~~18

3. Knelpunten ..... 27~~27~~21

3.1 Inleiding ..... 27~~27~~21

3.2 Verschillende wettelijke kaders ..... 27~~27~~21

3.3 Rechtvaardigingsgronden ..... 28~~28~~22

3.4 Verenigbaarheidstoets ..... 29~~29~~23

3.5 Geheimhoudingsplicht ..... 30~~30~~24

3.6 Gegevensverstrekking aan politie en OM ..... 33~~33~~27

3.7 Verstrekking van strafrechtelijke gegevens ..... 35~~35~~29

3.8 Typen van verwerking ..... 35~~35~~29

3.9 Kwaliteit gegevens en zorgvuldigheid bij verwerking ..... 36~~36~~30

3.10 Verantwoordelijke ..... 37~~37~~31

3.11 Informatieplicht ..... 37~~37~~31

3.12 Vertrouwen in het gebruik van gegevens door andere partijen ..... 38~~38~~32

4. Contouren kaderwet ..... 40~~40~~33

4.1 Inleiding ..... 40~~40~~33

4.2 Reikwijdte kaderwet ..... 41~~41~~34

4.3 Regeling doel samenwerkingsverband ..... 42~~42~~35

4.4 Verplichte uitwisseling van gegevens ..... 43~~43~~36

4.5 Specifieke vastlegging van soorten gegevens ..... 44~~44~~37

4.6 Legitimatie typen van gegevensverwerking ..... 45~~45~~38

4.7 Zorgvuldigheid bij verwerking ..... 45~~45~~38

4.8 Verantwoordelijke ..... 47~~47~~40

4.9 Informatieplicht ..... 47~~47~~40

Met opmerkingen : Ik vind de structuur van het rapport niet echt helder en een beetje een samenraapsel; wat mi node ontbreekt is een helder verhaal over de verschillende knelpunten die thans ten dele zo hier en daar al dan niet terloops zijn opgenomen. Tav samenvatting, inleiding, context bijvoorbeeld vind ik niet duidelijk of dat nu slaat op het werk van de werkgroep, fraudebestrijding, gegevensuitwisseling of de kaderwet. Ik zou er de voorkeur aan geven te beginnen met de aanleiding, te weten de reden voor de instelling en de context van de werkgroep. Dan de ruime taakomschrijving, de discussie daarover binnen de wekgroep, de constatering dat tav gegevensverwerking binnen het overheidsdomein zich tal van knelpunten en onduidelijkheden voordoen, dat voor een structurele oplossing daarvan een brede, maatschappelijke en politieke discussie nodig is nu het verschijnsel van gegevnsuitwisseling vanwege allerlei maatschappelijke ontwikkelingen steeds meer belang krijgt en dat de werkgroep in dat kader bij wijze van vingeroefening getracht heeft binnen de bestaande context te bezien in hoeverre een kaderwet toch nog oplossingen kan bieden al is het maar op een deelgebied. Vandaar de focus op gegevensuitwisseling alleen in kader van samenwerkingsverbanden. Naar de conclusie van de werkgroep leert die exercitie dat die deeloplossing zelfs lastig is te realiseren.

heeft opmaak toegepast: Lettertype: 10 pt

heeft opmaak toegepast: Lettertype: Verdana, 10 pt, Vet

heeft opmaak toegepast: Lettertype: Verdana, 10 pt

4.10 Informatieprotocol 484841
4.11 Toezicht 494942
4.12 Toetsing aan het EVRM 494942
4.13 Toetsing aan regelgeving van de EU 505043
5. Slotbeschouwing 525245
Bijlage 1 Overzicht samenwerkingsverbanden 535346
Bijlage 2 Proeve van een Wet gegevensuitwisseling samenwerkingsverbanden 545447

Met opmerkingen

In de inhoudsopgave ontbreekt een paragraaf over convenanten en dan zijn volgens de kaderwet nu net de plekken waar de inns en outs van de voorziene samenwerkingsverbanden moeten worden geregeld.

Punt 3 (knelpunten) levert nu niet direct het overzicht van de knelpunten bij gegevensuitwisseling op zoals een lezer dat zou verwachten.

Samenvatting

Het kabinet wil een verkenning naar een kaderwet voor de gegevensuitwisseling op het terrein van fraudebestrijding. Zo'n kaderwet zou generieke knelpunten met betrekking tot de gegevensuitwisseling in de bestaande wetgeving moeten oplossen in plaats van het aanbrengen van afzonderlijke wijzigingen in specifieke wetten. Deze notitie bevat het resultaat van deze verkenning. Zij spitst zich toe op gegevensuitwisseling in samenwerkingsverbanden. Gebleken is dat zich vooral in dergelijke verbanden knelpunten voordoen, zoals hierna aan de orde komen.

De oprichting van samenwerkingsverbanden wordt ingegeven door de behoefte aan een brede, integrale aanpak van problemen waarmee de effectiviteit van het overheidshandelen kan worden vergroot. We zien dat niet alleen gebeuren bij de aanpak van fraude, maar ook op andere beleidsterreinen. Wat daarbij opvalt, is dat slechts enkele samenwerkingsverbanden zich uitsluitend met de aanpak van fraude bezighouden. Veel samenwerkingsverbanden hebben een bredere taak, die mede de aanpak van fraude omvat. Naast samenwerkingsverbanden waaraan uitsluitend overheidspartijen deelnemen, ontstaan in toenemende mate samenwerkingsverbanden waarin ook private partijen participeren.

Om tot een efficiënte en doeltreffende samenwerking te komen is goede uitwisseling van informatie essentieel. Alleen dan kunnen partijen tot zo effectief mogelijke en op elkaar afgestemde interventies komen. Daarbij valt in de praktijk een toenemende inzet op "intelligence" en een risico-gestuurde benadering waar te nemen. Dat draagt bij aan de identificatie van personen en organisaties die achter de schermen de regie over zware vormen van fraude voeren, en aan een effectieve inzet van de beschikbare capaciteit om fraude te voorkomen en bestrijden.

Samenwerkingsverbanden verwerken daartoe verschillende categorieën gegevens. De categorie die daarbij doorgaans de meeste aandacht krijgt, betreft persoonsgegevens. Die aandacht vloeit voort uit het feit dat het bij persoonsgegevens om gegevens gaat die grondrechtelijke bescherming genieten op basis van internationale verdragen, regelingen van de Europese Unie en onze eigen Grondwet. Naast persoonsgegevens verwerken samenwerkingsverbanden ook andere gegevens, zoals bedrijfsgegevens.

Bij een verkenning naar een kaderwet gegevensuitwisseling kan het niet alleen gaan om het verkennen van mogelijkheden om knelpunten weg te nemen die op dit moment met betrekking tot het uitwisselen van gegevens bestaan. ~~Integendeel, E~~een verbetering en uitbreiding 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. Het begrip "zorgvuldigheid", uitgewerkt in een aantal waarborgen, zou het centrale ijkpunt bij iedere vorm en fase van gegevensverwerking (in samenwerkingsverbanden) moeten zijn.

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

De knelpunten bij de gegevensuitwisseling in samenwerkingsverbanden hangen voor een belangrijk deel samen met het feit dat regelingen met betrekking tot verwerking van gegevens ~~uit hun aard~~van oudsher primair een "verticaal" karakter hebben: zij regelen de gegevensverwerking *binnen* de desbetreffende sector dan wel overheidsdienst. Gegevensuitwisseling in samenwerkingsverbanden heeft echter een "horizontaal" karakter: zij heeft betrekking op gegevensverwerking *tussen* verschillende sectoren en overheidsdiensten. Gelet op de specifieke context waarin overheidsorganisaties moeten opereren, is de systematiek van de bestaande wetgeving voor iedere individuele organisatie wellicht nog te begrijpen en te billijken. Deze systematiek van de wetgeving is voor samenwerkingsverbanden echter ~~wel erg complex~~niet wel toegesneden op gebruik van binnen de

Met opmerkingen : Mi te lang en niet duidelijk waarvan dit een samenvatting is.

Met opmerkingen Met deze zin wordt de toonzetting van het rapport wel erg gezet en beperken we onszelf wel heel erg; aanvankelijk gingen we ervan uit dat de werkgroep veel ruimte had de verkenning zelf in te richten.

Met opmerkingen Dit is verwarrend; in feite draait het om persoonsgegevens; het zou heel verhelderend zijn als de justitiewetgeving begrippen als politiegegevens etc. zou laten vervallen nu met al die verschillende categorieën gegevens het zicht wel erg wordt beneveld.

overheid beschikbare gegevens door andere overheidsdiensten. ~~Zo complex dat het~~daarnaast is 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~~de verschillende regelingen niet goed op elkaar zijn afgestemd.

Voor gegevensverstrekking aan ~~alle~~ de deelnemers van een samenwerkingsverband of aan een ondersteunend bureau, als dat voor een effectief functioneren van het verband als geheel ten goede ~~zou komen~~komt, bestaat vaak geen adequate grondslag. ~~Het vinden daarvan ligt vaak nog een slag lastiger, als~~bij deelname van private partijen aan een samenwerkingsverband ligt dit nog een slag lastiger~~ook private partijen deelnemen~~.

Het doel van de gegevensuitwisseling in een samenwerkingsverband is in het algemeen een ander dan het doel waarvoor een deelnemer aan het verband de gegevens oorspronkelijk heeft verkregen. De Wet bescherming persoonsgegevens (Wbp) brengt mee dat voor deze gegevensuitwisseling dan moet worden getoetst of ~~zij~~ dat nieuwe doel al dan niet verenigbaar is met de doeleinden waarvoor de gegevens oorspronkelijk zijn verkregen. Het is echter de vraag of het noodzakelijk is ook voor samenwerkingsverbanden met een publiek belang steeds een verenigbaarheidstoets te moeten uitvoeren. Dat klemt te meer, nu de uitvoering van de verenigbaarheidstoets in de praktijk een lastige hindernis blijkt te zijn en bij tijd en wijle een juridische rem zet op de bereidheid om gegevens uit te wisselen.

Met opmerkingen ☐ Dit kan volgens ons niet omdat dat in strijd is met de privacy regelgeving (internationaal en nationaal; de afweging naar verenigbaarheid blijft steeds noodzakelijk op ieder niveau en in het licht van de feitelijke situatie).

De mate waarin gegevens binnen samenwerkingsverbanden kunnen worden uitgewisseld, wordt sterk bepaald door de geheimhoudingsplichten in verschillende wetten. Deze wetten bevatten ook bepalingen die het mogelijk maken de geheimhoudingsplicht te doorbreken. Wat al deze mogelijkheden echter gemeen hebben, is dat zij weliswaar voor gegevensverstrekking aan samenwerkingsverbanden in verschillende mate enige ruimte geven, maar in de praktijk toch nog wel de nodige drempels opleveren. Wat zich hier wreekt, is dat de verschillende mogelijkheden tot verstrekking van gegevens aan andere partijen hoofdzakelijk zijn geformuleerd vanuit het perspectief van de verschillende sectoren en niet met het oog op een overkoepelend publiek belang van samenwerkingsverbanden. De geheimhoudingsbepalingen in die sectorwetten gaan voor verstrekking aan dergelijke verbanden uit van "nee, tenzij". Een kaderwet zou dit paradigma kunnen doen kantelen naar "ja, tenzij". Het "nee, tenzij" leidt in de praktijk ertoe dat de discussie vooral gaat over wat mag en wat niet mag en daarmee primair een juridische discussie is. De kanteling naar "ja, tenzij" zal meebrengen dat de discussie een meer beleidsmatig karakter krijgt.

Met opmerkingen ☐ Ook binnen het overheidsdomein is een afweging noodzakelijk en mag niet alles! Het ware interessant – geweest – na te gaan waar in de jurisprudentie de grenzen worden gelegd.

~~Juist de S~~samenwerking tussen bestuursrechtelijke toezichthouders en strafrechtelijke opsporingsinstanties kan bij uitstek meerwaarde hebben bij fraudebestrijding en andere activiteiten op het terrein van de rechtshandhaving en criminaliteitsbestrijding. Het Wetboek van Strafvordering kent evenwel een systeem voor het vorderen van informatie door politie en OM, dat een barrière voor een efficiënte vorm van gegevensuitwisseling in samenwerkingsverbanden opwerpt. Zo is het bij voorbeeld onduidelijk of in het kader van samenwerkingsverbanden gegevens mogen worden verstrekt aan het OM zonder dat daar een vorderingsrecht vanuit het OM aan ten grondslag ligt. Daarnaast bestaat in de praktijk grote behoefte aan betere en ruimere mogelijkheden voor politie, bijzondere opsporingsdiensten en OM om strafrechtelijke gegevens aan andere partijen binnen het samenwerkingsverband te verstrekken. De bestaande mogelijkheden op dit punt zijn niet optimaal.

Met opmerkingen ☐ Die bepalingen zijn er toch niet voor niets?

De praktijk worstelt ook met de vraag of en, zo ja, in hoeverre de huidige regelgeving allerlei typen van gegevensverwerking binnen samenwerkingsverbanden toestaan. Dat geldt vooral voor het gebruik van geavanceerde analysemethoden waarmee mogelijk relevante patronen in beeld kunnen worden gebracht die een samenwerkingsverband kan gebruiken voor het opstellen van risico-analyses en profielen.

In de praktijk blijkt dat samenwerkingsverbanden zich ook de vraag stellen of en, zo ja, in hoeverre zij moeten voldoen aan de informatieplicht van artikel 34 Wbp. 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. Belangrijk is ook dat het in samenwerkingsverbanden op het terrein van de fraudebestrijding al gauw gaat om gegevensverwerking die, als zij bij betrokkenen bekend wordt, tot calculerend gedrag bij hen kan leiden.

Bij gegevensuitwisseling in samenwerkingsverbanden geldt dat geen enkele partij graag gegevens verstrekt, als niet duidelijk is wat ermee gebeurt. Dat geldt vooral als het om gevoelige gegevens gaat. Het bestaan van onduidelijkheid op dit punt kan een belemmering vormen voor de gegevensuitwisseling.

Een kaderwet kan mogelijk helpen d~~D~~e hiervóór genoemde knelpunten weg te nemen. ~~kunnen worden weggenomen door een kaderwet voor de gegevensuitwisseling in samenwerkingsverbanden.~~ Een kaderwet zal niet voor ieder samenwerkingsverband in detail kunnen regelen waaraan dat samenwerkingsverband zich heeft te houden. Dat zou ook niet goed mogelijk zijn zonder te vervallen in een rigide structuur die onvoldoende ruimte voor maatwerk voor ieder afzonderlijk samenwerkingsverband biedt. De praktijk van samenwerkingsverbanden is te veelvormig om die vast te kunnen leggen in wetgeving in formele zin.~~Wel zal een~~De kaderwet zal het~~een~~ raamwerk bieden waarbinnen de deelnemers aan een samenwerkingsverband hun samenwerking nader uitwerken in een convenant en in een informatieprotocol, dat de nodige waarborgen voor de bescherming van persoonsgegevens bevat. Een kaderwet zal aldus niet alleen legitimerend en faciliterend, maar ook normerend zijn.

Met opmerkingen [ ]: Ik blijf een gestructureerd overzicht van knelpunten missen!

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 onwerkbare situatie opleveren. Los van deze overweging kan worden vastgesteld dat een kaderwet voor veel meer samenwerkingsverbanden in de publieke sfeer betekenis kan hebben dan alleen de verbanden die (mede) op het terrein van de fraudebestrijding bezig zijn. Het ligt dan ook voor de hand te kiezen voor een kaderwet op het brede terrein van de uitoefening van toezicht op de naleving van wettelijke voorschriften, de handhaving van de openbare orde en veiligheid en de voorkoming, opsporing en vervolging van strafbare feiten. Het is immers dit brede terrein waarop zich allerlei samenwerkingsverbanden manifesteren die gegevens binnen het bestuursrecht en tussen het bestuursrechtelijke en strafrechtelijke domein willen uitwisselen. Verder wordt bepleit de kaderwet ook betrekking te laten hebben op samenwerkingsverbanden waaraan private partijen deelnemen. Ook private partijen beschikken immers over informatie die voor het voorkomen en bestrijden van fraude en andere vormen van criminaliteit van belang is. Daarvoor zullen uiteraard extra waarborgen dienen te worden ingebouwd.

Met opmerkingen [ ]: Moet dus nog breder: ook de voorkant van het bestuursrechtelijke gebeuren.

De kaderwet zou moeten bepalen dat de deelnemers aan het samenwerkingsverband in een convenant nauwkeurig het specifieke doel van de samenwerking en de daarvoor noodzakelijke gegevensuitwisseling vastleggen. Dit doel moet passen binnen de reikwijdte van de bredere wettelijke doelomschrijving. De verenigbaarheidstoets van de Wbp kan dan achterwege blijven.

De deelname aan een samenwerkingsverband kan niet vrijblijvend zijn. De kaderwet zou dan ook moeten voorschrijven dat de deelnemers verplicht zijn de voor het samenwerkingsverband noodzakelijke gegevens aan de andere deelnemers te verstrekken, voor zover zij daarop geen uitzonderingen mogelijk hebben gemaakt.

Met opmerkingen [ ]: Dit lijkt ons een brug te ver: de facto kan dan immers alle info worden gedeeld.

Met opmerkingen [ ]: Is dit de reden om dit op te nemen of gaat het om het creëren van de juridische grondslag voor gegevensverstrekking?

Uit een oogpunt van transparantie is het wenselijk in een onder de kaderwet vallende AMvB aan te geven welke soorten van gegevens door de samenwerkingsverbanden kunnen worden gewisseld. Om de bestaande onduidelijkheid over welke typen van gegevensverwerking zijn toegestaan weg te nemen, zal een kaderwet kunnen expliciteren dat de door deze kaderwet gereguleerde

gegevensuitwisseling binnen samenwerkingsverbanden betrekking kan hebben op alle in die wet beschreven doeleinden voor zover nader uitgewerkt in het desbetreffende convenant.

Wil een kaderwet gegevensuitwisseling een integrale verbetering van de gegevensuitwisseling in samenwerkingsverbanden opleveren, dan zal deze kaderwet niet alleen een verbetering van de mogelijkheden van gegevensuitwisseling moeten bieden, maar ook voorzieningen moeten bevatten die bijdragen aan de kwaliteit van de gegevens en de zorgvuldigheid bij de verwerking daarvan. Daarbij kan onder meer worden gedacht aan opneming van het vereiste van noodzakelijkheid en de daaruit voortvloeiende beginselen van proportionaliteit en subsidiariteit, waarborgen die de transparantie van de gegevensverwerking dienen en het uitvoeren van een Privacy Impact Assessment.

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

De verwerking van persoonsgegevens onder de werking van een kaderwet voor gegevensuitwisseling in samenwerkingsverbanden zal plaatsvinden onder toezicht van het College bescherming persoonsgegevens.

De beschreven kaderwet, waarvan een proeve is bijgevoegd, voldoet aan de voorwaarden die het EVRM stelt, en past binnen de grenzen van de huidige en komende regelgeving van de EU op het terrein van de bescherming van persoonsgegevens.

Met opmerkingen Dit vragen wij ons allemaal ten stelligste af!

Iets over bewaartermijnen?

Iets over transparantie mede in licht van passages blz. 32, 41 en 42

1. Inleiding

~~Op 20 december 2013 heeft het kabinet~~ook hier weer zouden wij niet beginnen met de relatie en verslaglegging Mc fraude en TK maar om de interne opdracht vanuit de mc fraude aan de wg. de Tweede Kamer een brief gezonden over de aanpak van fraude met publieke middelen. In die brief kondigt het kabinet onder meer een verkenning aan naar een kaderwet voor de gegevensuitwisseling op het terrein van fraudebestrijding. Zo'n kaderwet zou generieke knelpunten met betrekking tot de gegevensuitwisseling in de bestaande wetgeving moeten oplossen in plaats van het aanbrengen van afzonderlijke wijzigingen in specifieke wetten.[1]

Deze notitie bevat het resultaat van deze verkenning. In § 2 wordt eerst de context geschetst waarbinnen de verkenning heeft plaatsgevonden. In § 3 wordt een aantal knelpunten in de huidige praktijk van gegevensuitwisseling op een rijtje gezet die tijdens de verkenning naar voren zijn gekomen. Vervolgens worden in § 4 de contouren van een mogelijke kaderwet geschetst waarmee deze knelpunten zouden kunnen worden opgelost. Als bijlage is bij de notitie een proeve van een kaderwet gevoegd.

De notitie is opgesteld door een werkgroep, bestaande uit vertegenwoordigers van de ministeries van Veiligheid en Justitie, Sociale Zaken en Werkgelegenheid en Financiën, van het openbaar ministerie en van de gemeente Tilburg.[2] De werkgroep heeft daarbij in de eerste plaats gebruik gemaakt van ervaringen die zijn opgedaan bij de ontwikkeling van samenwerkingsverbanden waarin partijen gegevens uitwisselen. Verder heeft de werkgroep in april 2014 een brainstormsessie met verschillende genodigden gehouden over knelpunten in de gegevensuitwisseling en de mogelijkheden die een kaderwet ~~biedt~~ zou kunnen bieden om deze op te lossen. Ook heeft de werkgroep voor haar verkenning gebruik gemaakt van de in eerdergenoemde kabinetsbrief aangekondigde inventarisatie van de behoefte aan gegevensuitwisseling in een viertal casussen: gefingeerde dienstverbanden, faillissementsfraude, identiteitsfraude en notoire fraudeurs/subjectgerichte fraudebestrijding. Bij deze inventarisatie is ook naar eventuele knelpunten bij de gegevensuitwisseling gekeken. Voor de notitie heeft uiteraard ook raadpleging plaatsgevonden van relevante literatuur, officiële publicaties en websites. PM Verdere verantwoording

In deze notitie wordt ervan uitgegaan dat de gegevensuitwisseling in enigerlei vorm van samenwerkingsverband plaatsvindt. Daarmee wordt gedoeld op de situatie dat twee of meer partijen voor een bepaald doel in een georganiseerd verband samenwerken en om dat doel te bereiken gegevens uitwisselen. Het is vooral in dergelijke samenwerkingsverbanden dat zich knelpunten laten gevoelen als in § 3 zijn beschreven. De gerichtheid op samenwerkingsverbanden sluit overigens niet uit dat een eventuele kaderwet ook betekenis kan hebben voor gegevensuitwisseling in "reguliere processen". Gegevensuitwisseling in dergelijke processen kan immers zeer wel vorm krijgen in samenwerkingsverbanden. De gerichtheid op samenwerkingsverbanden brengt wel mee dat verstrekking van gegevens met een incidenteel karakter buiten de reikwijdte van deze notitie vallen. Daar komt bij dat een kaderwet zich minder goed leent voor de oplossing van een eventueel knelpunt bij dat type verstrekking. Zo'n kaderwet zal namelijk al gauw een aantal randvoorwaarden voor gegevensuitwisseling bevatten (zie nader § 4) die niet bij incidentele verstrekkingen passen.

[1] Kamerstukken II 2013-2014, 17050, nr. 450, blz. 7-8.

[2] Samenstelling werkgroep: ~~(OM)~~ ~~(SZW)~~ ~~(VenJ)~~ ~~(Fin)~~ ~~(SZW)~~ ~~(VenJ)~~ ~~(VenJ)~~ ~~(Fin)~~ ~~(Tilburg)~~ ~~(SZW)~~ ~~(SZW)~~. Vooralsnog geef ik de voorkeur aan vertegenwoordigers van de volgende departementen en organisaties:.

Met opmerkingen Staat dit echt ergens?

Met opmerkingen Uit die brief: Ten tweede wordt voor generieke knelpunten waarvan wordt vastgesteld dat die alleen met wetgeving zijn op te lossen een verkenning uitgevoerd naar een kaderwet voor de gegevensuitwisseling op het bredere terrein van fraudebestrijding, in plaats van de noodzakelijke maar steeds afzonderlijke wijzigingen van specifieke wetten. (...)

Met opmerkingen Interessant is welke generieke knelpunten geïnventariseerd zijn.

Met opmerkingen Moet dit niet: Dit rapport zijn?

Met opmerkingen Zijn dit de generieke knelpunten die alleen door middel van een kaderwet kunnen worden opgelost.

Met opmerkingen Vooalsnog nog niet!

Met opmerkingen Hij geschiedt thans juridisch slechts in bilaterale verbanden en uiteraard geschiedt veel gegevensuitwisseling louter unilateraal in bilaterale relaties.

Met opmerkingen Individueel of gezamenlijk?

Met opmerkingen Wanneer is sprake van een samenwerkingsverband? Aan welke kenmerken/vereisten moet een 'samenwerkingsverband' voldoen?

Met opmerkingen Wordt hier nu bedoeld dat de kaderwet ook geldt voor reguliere processen (wat die dan ook zijn) als die processen (voortaan?) geschieden in de vorm van samenwerkingsverbanden? Zo ja waar ligt dan de grens?

Met opmerkingen Mi zijn de unilaterale gegevensuitwisselingen niet incidenteel maar structureel van aard en liggen die vast in wet- en regelgeving; zelfs de huidige samenwerkingsverbanden opereren veelal onder die noemer.

Met opmerkingen Wat zijn dan de verschillende knelpunten in beide vormen (incidentele verstrekking versus verstrekking aan een samenwerkingsverband)

Met opmerkingen ?

2. Context van wat (rapport, gegevensuitwisseling, fraudebestrijding?)

2.1 Aanleiding van/voor wat?

Onderstaand een tekstsuggestie/inlas van FIN (waarbij het eerdere FIN memo inzake het structurele en principiële karakter van bestaande knelpunten bij gegevensverwerking enigszins wordt aangestipt) in het rapport zodat die analyse mogelijk in een volgende ronde kan worden opgepakt tbv de alsdan te voeren brede discussie over hoe we als rijksoverheid aankijken tegen nut en noodzaak van een bredere gegevensverwering binnen het overheidsdomein. FIN beschouwt deze bevindingen als een belangrijk resultaat van het werk van de werkgroep gedurende de eerste helft dit jaar en ziet graag eea vastgelegd in dit rapport zodat hier later op kan worden voortgeborduurd.

Met opmaak: Standaard

De aanleiding voor de instelling van een werkgroep Verkenning Kaderwet gegevensverstrekking is het bredere mc-project inzake fraudebestrijding. In het kader van dit brede project zijn tal van werkgroepen ingesteld die ieder bepaalde onderwerpen en aspecten van fraudebestrijding als focus en taakopdracht hebben waarover zij zullen rapporteren. Bij een aantal van deze werkgroepen speelt gegevensverwerking en gegevensuitwisseling een belangrijke rol. Dit is niet verwonderlijk nu in toenemende mate in de praktijk via samenwerking en gegevensuitwisseling tussen overheidsdiensten nieuwe, effectieve methoden worden ontwikkeld in het kader van de bestrijding van fraude op verschillend gebied. Gegevensuitwisseling en het kunnen beschikken over elders binnen de overheid beschikbare relevante informatie wordt meer en meer een conditio sine qua non voor een verantwoord en effectief overheidsbeleid. De werkgroep Verkenning Kaderwet constateert dat de problemen bij gegevensuitwisseling ten behoeve van fraudebestrijding niet principieel verschillen van gegevensuitwisseling tussen overheidsdiensten ten behoeve van andere doeleinden die ook geschieden in het kader van het algemeen belang. Dit betekent dat de problemen die spelen bij het op grotere schaal gebruik kunnen maken van op enige plek binnen het overheidsdomein aanwezige informatie ook spelen bij het willen delen van informatie ten behoeve van fraudebestrijding. De hiervoor bedoelde samenwerking en gegevensuitwisseling zijn, naar de ervaringen van de praktijk leert, evenwel niet eenvoudig te realiseren. Hieraan ligt een complex van factoren ten grondslag. Uiteraard is een belangrijk element daarbij dat de rechten van de burger op een rechtmatig en verantwoord gebruik van persoonsgegevens grenzen stelt aan gegevensverwerking en –uitwisseling. Het werk van de werkgroep is evenwel erop gericht om binnen de bestaande kaders, waaronder met name de wet- en regelgeving inzake waarborging van de privacy na te gaan, in hoeverre andere zich voordoende knelpunten bestaan en kunnen worden weggenomen.

Ook de werkgroep heeft ervaren dat het in kaart brengen van die knelpunten en het opstellen van een inventarisatie daarvan niet een eenvoudige zaak is. Er zijn inmiddels een fors aantal pogingen ondernomen in de vorm van studies, evaluaties en praktijkbeoordelingen die knelpunten eenduidig vast te stellen. Ook dit rapport doet daartoe weer een poging. Toch is de materie weerbarstig, vluchtig en niet wel grijpbaar. Het is niet gemakkelijk precies de vinger op de verschillende knelpunten te leggen en daarmee de basis te scheppen voor het oplossen van die knelpunten. De werkgroep heeft zich afgevraagd wat de reden is dat wel het algemene gevoelen bestaat bij alle betrokkenen dat gegevensuitwisseling binnen het overheidsdomein binnen het huidige kader tal van vragen oproept die de praktijk van gegevens fors parten speelt, terwijl toch het eenduidig definiëren van die knelpunten geen eenvoudige zaak is.

Een belangrijke factor hiervoor is, naar de mening van de werkgroep, dat de behoefte aan en praktijk van gegevensuitwisseling tussen overheidsdiensten steeds minder past binnen het bestaande wettelijk kader. Er is met andere woorden sprake van toenemende spanning tussen de geldende wet- en regelgeving en de behoefte aan en noodzaak van een groter gebruik van gegevens binnen het overheidsdomein als geheel. De praktijk doet zijn best en probeert zo goed mogelijk binnen de bestaande wettelijke kaders de mogelijkheden te benutten. Die wettelijke

kaders stammen evenwel enerzijds deels uit het verleden en vormen anderzijds, denk aan de privacy wetgeving, recente toevoegingen.

De gegevenshuishouding binnen de overheid is vanouds per domein, per overheidssector of organisatie, verticaal georganiseerd. Iedere overheidsdienst regelde de eigen informatiebehoefte op de eigen wijze en binnen de eigen materiewetgeving. Aan gegevensuitwisseling tussen overheidsdiensten bestond tot voor kort geen grote behoefte en voor zover dat wel het geval was werd een verstrekking tussen de ene overheidsdienst aan een andere overheidsdienst apart geregeld. De privacywetgeving betekende voor het eerst dat sprake was van begrippen die horizontaal bij iedere gegevensverwerking dienden te worden geharmoniseerd. Naast de opkomst van de privacywetgeving ziet het recente verleden de opkomst van de behoefte in de praktijk tussen overheidsdiensten te gaan samenwerken en in dat kader optimaal gebruik te maken van bij de verschillende deelnemende partijen aanwezige informatie. Samen sta je uiteraard sterker en de technologische ontwikkelingen maken het anders dan vroeger toen het om uitwisseling ging van gegevens die betrekking hebben op een individueel geval, mogelijk grootschalige bestanden op efficiënte wijze snel en gemakkelijk te vergelijken. Staat de opportuniteit en wenselijkheid van deze ontwikkeling buiten kijf, mits een en ander in voldoende mate rekening houdt met de gerechtvaardigde privacy belangen van de burger, anders ligt het met de kijk op en de juridische inbedding van gegevensuitwisseling binnen het overheidsdomein. Zoals gezegd gaat de geldende wetgeving, enkele uitzonderingen daargelaten, in zijn algemeenheid uit van op zich zelf staande individuele gegevenshuishoudingen waarbij het wettelijk uitgangspunt zelfs veelal is, via het bestaan van geheimhoudingsbepalingen, dat gegevens juist niet tussen de verschillende kolommen binnen het overheidsdomein worden uitgewisseld. Een bijzondere situatie neemt de opkomst van basisregistraties in deze in. Zoals bekend is daarbij het verklaarde uitgangspunt dat op een plaats binnen de overheid de desbetreffende gegevens worden geregistreerd en dat die gegevens vervolgens verplicht de bron zijn voor iedere overheidsdienst die gebruik moet maken van dit soort gegevens. De recente wetgeving inzake de verschillende basisregistraties staat dan ook haaks op het uitgangspunt dat ten grondslag ligt aan de informatiehuishoudingen binnen de overheid bij de verschillende individuele overheidsdiensten. Dit (verouderde?) uitgangspunt verklaart naar de mening van de werkgroep voor een fors deel de spanning die optreedt wanneer toch wordt gezocht naar wegen om gegevensuitwisseling tussen overheidsdiensten te bewerkstelligen.

De remedie hiervoor is niet zo eenduidig. Wat in feite nodig is, is dat een nieuwe visie wordt ontwikkeld op het gebruik van gegevens die beschikbaar zijn binnen het overheidsdomein. Anders dan thans het geval is, zou die visie uit moeten gaan van de erkenning dat het in beginsel een goede zaak is, wanneer daar aanleiding dan wel noodzaak toe bestaat, om op enige plek binnen de overheid aanwezige beschikbare informatie te delen met een andere overheidsdienst. In deze tijd zijn de technologische mogelijkheden voorhanden om een dergelijk gebruik van gegevens mogelijk te maken en de complexiteit, massaliteit, snelheid en gevraagde effectiviteit anno 2014 vragen daar ook om. De uitwerking van de nieuwe visie op gebruik van gegevens binnen het overheidsdomein zou te zijner tijd dienen te worden neergelegd in wetgeving. Dat proces kan samenvallen met de noodzaak de bestaande privacywetgeving rond gegevensverwerking aan te passen in verband met de komst van nieuwe EU-regelgeving die zich binnen afzienbare termijn aandient. Ook de al voorgenomen aanpassing van de wetgeving op het gebied van gegevensverwerking in de strafrechtelijke sfeer past naadloos in dit tijdpad. Het ontwikkelen van nieuw beleid en wetgeving ten aanzien van verwerking van persoonsgegevens binnen het overheidsdomein langs de Koninklijke weg en middels een brede maatschappelijke discussie garandeert tegelijkertijd dat de noodzakelijke waarborgen voor de gerechtvaardigde privacy belangen van de burger in acht worden genomen. Het risico van de huidige ontwikkelingen waarbij de vele verschillende betrokken partijen ieder op eigen wijze volgens de beste bedoelingen trachten de verschillende vormen van samenwerking en gegevensuitwisseling vorm te geven, is dat die belangen op die wijze niet altijd optimaal zijn geborgd. Een van de eerste voorwaarden voor rechtmatige verwerking van persoonsgegevens is dat dit transparant geschiedt. Aan deze voorwaarde wordt het best voldaan wanneer de verwerking van persoonsgegevens is geregeld bij

wet in formele zin en aan de verschillende vormen van verwerking een eenduidig en transparant kader ten grondslag ligt.

De werkgroep doet hiermee een oproep voor de start van de hiervoor bedoelde brede politieke en maatschappelijk discussie. De werkgroep heeft evenwel gemeend er goed aan te doen het daar niet bij te laten maar ook een poging te doen te bezien wat mogelijk is binnen de bestaande kaders. Daartoe is een voorzet voor een beperkte kaderwet uitgewerkt. Dat die mogelijkheden beperkt zijn blijkt uit het resultaat. De werkgroep is zich terdege bewust van de beperkingen van deze benadering maar acht de poging en het in kaart brengen van de daaraan gekoppelde bezwaren verhelderend voor en een bijdrage tot de gewenste brede discussie.

PT 1: Mi zouden we ook een paragraaf moeten hebben over de bezwaren verbonden aan de proeve maar dan moeten we het eerst wel eens worden over die bezwaren!

PT 2: Voordat ik verder ga moeten we het eerst maar eens hebben over het voorlopig ctr dat in dit stuk is opgenomen!

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. Tegen die achtergrond wil het kabinet fraude zoveel mogelijk voorkomen en waar fraude ondanks alle maatregelen toch nog heeft plaatsgevonden, zo effectief mogelijk bestrijden. Dat vraagt volgens het kabinet om een brede en integrale benadering waarbij de rijksoverheid ook zal samenwerken met gemeenten en private partijen, zoals banken en curatoren.[3]

Met opmerkingen : Meer iets over belang van gegevensverwerking ikv fraudebestrijding en dan overgang naar problemen bij gegevensuitwisseling.

Om tot een efficiënte en doeltreffende samenwerking te komen is ~~goede~~ uitwisseling van informatie essentieel. Alleen dan kunnen partijen tot zo effectief mogelijke en op elkaar afgestemde interventies komen. Daarbij valt in de praktijk een toenemende inzet op "intelligence" en een risico-gestuurde benadering waar te nemen. Dat draagt bij aan de identificatie van personen en organisaties die achter de schermen de regie over zware vormen van fraude voeren, en aan een effectieve inzet van de beschikbare capaciteit om fraude te voorkomen en bestrijden.

Bij de uitwisseling van informatie worden ook persoonsgegevens gedeeld. Het delen daarvan moet uiteraard voldoen aan de wettelijke bepalingen ter bescherming van persoonsgegevens. Hetzelfde geldt voor andere gegevens die wettelijk bescherming genieten. Waar onze wetgeving in algemene zin belangrijke waarborgen voor de bescherming van dergelijke gegevens bevatten, blijken zij echter in de specifieke situatie waarin partijen in samenwerkingsverbanden gegevens willen uitwisselen, de nodige knelpunten op te leveren, terwijl de vraag rijst of deze waarborgen in die specifieke situatie ook onverkort zouden moeten blijven gelden.

Met opmerkingen Of nader uitwerken wat hier nu preceis bedoeld wordt (welke knelpunten worden door wetgeving opgeroepen?). Of: welke wetgeving staat aan de gegevensuitwisseling in samenwerkingsverbanden in de weg? En vervolgens: welke gedachten zitten daar dan achter?

Met opmerkingen : MI weg.

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

Met opmerkingen Maar de overheid moet daar ook rekening houden met grondrechten als privacy ik zou dan ook zeggen: 'en erkent ...'. De gekozen insteek lijkt wel heel pragmatisch.

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

mogelijkheden om met een kaderwet tot een betere gegevensuitwisseling te komen, moet dan ook een overheid die langs deze lijnen opereert, als uitgangspunt nemen.

2.2 Samenwerkingsverbanden

Om de effectiviteit van het overheidshandelen als geheel te vergroten, richten overheidsorganisaties in toenemende mate samenwerkingsverbanden op. We zien dat niet alleen gebeuren bij de aanpak van fraude, maar ook op andere beleidsterreinen. Wat daarbij opvalt, is dat enkele samenwerkingsverbanden zich in het bijzonder met de aanpak van fraude bezighouden en andere samenwerkingsverbanden een bredere taak hebben, die evenwel ook in enigerlei vorm mede de aanpak van fraude omvat. Dat moge blijken, als we hierna in vogelvlucht een aantal samenwerkingsverbanden de revue laten passeren.[4]
Deze lange opsomming onderbreekt behoorlijk de lijn van het verhaal; kan eea niet in een bijlage met slechts een summiere duiding vzv nodig?

De Belastingdienst, de Inspectie SZW, het UWV, de gemeenten, het OM, de SVB, de ministeries van Financiën en van Sociale Zaken en Werkgelegenheid en de politie werken samen in een interventiestructuur met het oog op het voorkomen en bestrijden van fraude. Het gaat daarbij om belasting- en premiefraude, uitkeringsfraude, illegale tewerkstelling en de daarmee samenhangende misstanden. Deze partijen hebben daartoe in 2003 een samenwerkingsovereenkomst[5] gesloten (de politie is later toegetreden). De interventiestructuur bestaat uit een landelijke stuurgroep, een analysefunctie, regionale platforms en interventieteams. In deze structuur werken de partners niet alleen op strategisch, tactisch en operationeel niveau samen, maar delen ze ook gegevens met elkaar. Het betreft niet alleen gegevensuitwisselingen die casus-gebonden zijn, maar ook gestructureerde bestandskoppelingen op basis waarvan met de inzet van het instrument Systeem Risico Indicatie (SyRI) risico-analyses worden uitgevoerd en eventuele interventies worden voorbereid.[6]

Om de integriteit van de financiële sector te versterken is in 1998 het samenwerkingsverband Financieel Expertise Centrum (FEC) opgericht. Aan dit samenwerkingsverband nemen de volgende partijen deel: de AIVD, de AFM, de Belastingdienst, DNB, de FIOD, de politie en het OM. Het FEC heeft tot taak een structurele informatie-uitwisseling tussen de partners te creëren, een kenniscentrum te realiseren en projecten uit te voeren. Het FEC richt zich als bewaker van de financiële integriteit op onder meer de volgende aandachtsgebieden: witwaspraktijken, vastgoedfraude, identiteitsfraude, hypotheekfraude, beleggingsfraude en cybercrime.[7] De manier waarop de FEC-partners samenwerken en met elkaar informatie uitwisselen is vastgelegd in een convenant, respectievelijk informatieprotocol.[8]

In 2013 hebben verschillende partijen de Infobox Crimineel en Onverklaarbaar Vermogen (iCOV) opgericht. Het betreft het OM, de politie, de Belastingdienst, de Douane, de FIOD en de Financial Intelligence Unit Nederland. Doel van iCOV is het in kaart brengen van onverklaarbaar of crimineel vermogen, het blootleggen van witwas- of fraudeconstructies en het kunnen innen van overheidsvorderingen ter ondersteuning van de publiekrechtelijke taakuitoefening van de deelnemende organisaties. Met dat doel voor ogen houdt iCOV zich onder meer bezig met het opstellen van rapportages, criminaliteitsbeeldanalyses, risico-indicatoren en groepsprofielen. Een en ander is vastgelegd in een convenant en protocollen.[9]

---

[4] Voor een uitgebreider overzicht van samenwerkingsverbanden wordt verwezen naar bijlage 1.
[5] Zie: http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/belastingdienst_interventieteams.
[6] Kamerstukken II 2012-2013, 33579,, nr. 3, blz. 3.
[7] Zie: http://www.fec-partners.nl/nl/organisatie.
[8] Zie Convenant FEC 2009, Stcrt 2009, 71, en Informatieprotocol FEC 2011, Stcrt. 2011, 21708.
[9] Zie Convenant iCOV 2013, Stcrt 2013, 24607, Protocol gegevensverwerking iCOV Productie 2013, Stcrt 2013, 24608, en Protocol gegevensverwerking iCOV Research and Development 2013, Stcrt. 2013, 24610.

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

1. een bestuurlijke en geïntegreerde aanpak van de georganiseerde criminaliteit door naast strafrechtelijke ook bestuursrechtelijke en fiscale maatregelen te treffen,
2. de identificering van gelegenheidsstructuren binnen die economische sectoren en publieke voorzieningen die vatbaar zijn voor beïnvloeding door de georganiseerde criminaliteit,
3. de bestrijding van zgn. handhavingsknelpunten en
4. de bevordering en ondersteuning van integriteitsbeoordelingen door het openbaar bestuur op grond van de Wet Bibob.

De samenwerking richt zich voor de eerste twee doelen op onderwerpen als mensenhandel, georganiseerde hennepteelt en fraude in vastgoedsector. De samenwerking is vastgelegd in een bestuurlijk akkoord en een convenant.[10] In de loop van 2014 zal de verwerking van persoonsgegevens binnen de RIEC's nader worden geregeld in een privacyprotocol.

Naast samenwerkingsverbanden waaraan uitsluitend overheidspartijen deelnemen, ontstaan in toenemende mate ook samenwerkingsverbanden waarin ook private partijen participeren. Publiek-private samenwerking levert beide kanten voordelen op. De overheid leert van de private sector. Zo zit er veel kennis bij het bedrijfsleven over nieuwe ontwikkelingen, risico's en technologieën. Omgekeerd steekt de private sector ook veel op van de overheid. De samenwerking levert niet in de laatste plaats voordeel op door gebruik te maken van elkaars informatie. Ook private partijen beschikken over informatie die voor het voorkomen en bestrijden van fraude en andere vormen van criminaliteit van belang is. Zowel de private partij als de publieke partij kan op basis van uitgewisselde informatie actie ondernemen of een interventie plegen die bijdraagt aan het voorkomen en bestrijden van criminaliteit. Om een aantal verbanden te noemen: 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.

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

1. Convenant verbetering bestrijding zorgfraude tussen de Nederlandse Zorgautoriteit, de Inspectie voor de Gezondheidszorg, Zorgverzekeraars Nederland, de Inspectie SZW, de FIOD, de Belastingdienst, het OM, het Centrum Indicatiestelling Zorg en het Ministerie van VWS[11],
2. Convenant hennepteelt Zeeland - West-Brabant 2013 tussen gemeenten, politie, OM, woningcorporaties, netbeheerders, UWV en SVB[12],
3. Convenant aanpak verzekeringsfraude tussen Verbond van Verzekeraars, zorgverzekeraars, het OM en de politie[13].

---

[10] Zie het Bestuurlijk Akkoord Geïntegreerde Decentrale Aanpak Georganiseerde Misdaad van september 2008 (kamerstukken II, 29 911, nr. 27) en het Convenant ten behoeve van bestuurlijke en geïntegreerde aanpak georganiseerde criminaliteit, bestrijding handhavingsknelpunten en bevordering integriteitsbeoordelingen (http://download.belastingdienst.nl/belastingdienst/docs/convenant_liec_riec_al11121z1ed.pdf).

[11] Zie: http://www.rijksoverheid.nl/documenten-en-publicaties/convenanten/2013/03/07/convenant-verbetering-van-bestrijding-zorgfraude.html.

[12] Zie: http://www.hetccv.nl/binaries/content/assets/ccv/dossiers/hennepteelt/13.004679-convenant-hennepteelt-zeelandwest-brabant-2013.pdf. Omdat het exploiteren van hennepkwekerijen vrijwel altijd gepaard gaat met andere strafbare feiten zoals diefstal van elektriciteit, belastingontduiking en uitkeringsfraude, richt de samenwerking zich ook op deze vormen van criminaliteit.

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

heeft opmaak toegepast: Markeren

Van de hier genoemde samenwerkingsverbanden houdt een minderheid zich uitsluitend met fraudebestrijding bezig. De meeste samenwerkingsverbanden hebben een taak die zich in meerdere of mindere mate ook tot andere terreinen uitstrekt. Met dat aspect zal rekening moeten worden gehouden bij de overwegingen rond de reikwijdte van een eventuele kaderwet. Een kaderwet die zich beperkt tot gegevensuitwisseling ten behoeve van de fraudebestrijding zal tot gevolg hebben dat verschillende samenwerkingsverbanden ten dele wel en ten dele niet onder de werking van de kaderwet vallen. Op de vraag welke consequentie daaraan verbonden zou kunnen worden, wordt hierna ingegaan in § 4.2.

heeft opmaak toegepast: Markeren

2.3 Verschillende categorieën gegevens (dit onderdeel vind ik er wat bijgesleept)

Samenwerkingsverbanden verwerken verschillende categorieën gegevens. De categorie die daarbij doorgaans de meeste aandacht krijgt, betreft *persoonsgegevens*. Die aandacht vloeit voort uit het feit dat het bij persoonsgegevens om gegevens gaat die grondrechtelijke bescherming genieten op basis van internationale verdragen, regelingen van de Europese Unie en onze eigen Grondwet.[14] De bescherming van persoonsgegevens is nader geregeld in de Wet bescherming persoonsgegevens (Wbp) als algemeen kader voor de verwerking van persoonsgegevens en daarnaast in sectorspecifieke regelingen als de Wet politiegegevens (Wpg)[15] en de Wet justitiële en strafvorderlijke gegevens (Wjsg) en sectorale wetgeving.

In de Wbp wordt een persoonsgegeven aangemerkt als elk gegeven betreffende een geïdentificeerde of identificeerbare persoon. Het gegeven dient dus informatie over een persoon te bevatten. Bij feitelijke of waarderende gegevens over eigenschappen, opvattingen of gedragingen zal dat uit de aard van de gegevens voortvloeien. Maar ook telefoonnummers, kentekens van auto's en postcodes met huisnummers dienen onder omstandigheden als persoonsgegeven te worden aangemerkt.[16]

De Wbp definieert bepaalde gegevens als *bijzondere persoonsgegevens*. Voor dergelijke persoonsgegevens geldt een apart regime. Het gaat om gegevens met betrekking tot iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakbond en strafrechtelijke gegevens. De verwerking van dergelijke gegevens is verboden, tenzij de wet een uitzondering schept. Zo'n uitzondering bestaat bijvoorbeeld voor strafrechtelijke persoonsgegevens, indien de verantwoordelijke de gegevens heeft verkregen krachtens de Wpg of de Wjsg (artikel 22, eerste lid, Wbp).

---

[13] Zie: https://www.verzekeraars.nl/overhetverbond/zelfregulering/Documents/Convenanten/Convenant_aanpak_verzekeringsfraude.pdf.

[14] Zie artikel 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM), het Dataprotectieverdrag uit 1981 (Trb. 1988, nr. 7), de Europese Privacyrichtlijn uit 1995 (Richtlijn 95/46/EG, Pb L 281), artikel 8 van het Handvest van de grondrechten van de Europese Unie (Pb EG 18 december 2000, C 364/3) en artikel 10 van de Grondwet.

[15] De Wpg is niet alleen van toepassing op politiegegevens. Op grond van artikel 46 Wpg is deze wet van overeenkomstige toepassing op de verwerking van persoonsgegevens door bijzondere opsporingsdiensten.

[16] Kamerstukken II 1997-1998, 25892, nr. 3, blz. 46-47.

Politiegegevens zijn persoonsgegevens die in het kader van de uitoefening van de politietaak worden verwerkt. Strafvorderlijke gegevens zijn gegevens die zijn verkregen in het kader van een strafvorderlijk onderzoek en die het OM in een strafdossier of langs geautomatiseerde weg verwerkt. Bij justitiële gegevens gaat het om bepaalde beslissingen van de rechter of het OM ten aanzien van bepaalde personen. Bij zowel strafvorderlijke als justitiële gegevens gaat het overigens niet alleen om persoonsgegevens, maar ook om gegevens over een rechtspersoon. Van belang is verder dat, wanneer gegevens op grond van de Wpg of de Wjsg aan partners in een samenwerkingsverband zijn verstrekt en vervolgens binnen dat verband worden doorverstrekt, die twee wetten niet meer van toepassing zijn en de Wbp geldt.[17]

Met opmerkingen : Kan het paradigma hier niet kantelen door voortaan ook bij de politie en justitie te spreken over persoonsgegevens (die door politie cq justitie worden verwerkt); dat geeft mi al een stuk meer duidelijkheid , er zijn al veel te veel begrippen bij gegevensverwerking .

Met opmerkingen : Maar er blijft wel weer de politiegeheimhouding op rusten?

Samenwerkingsverbanden verwerken uiteraard niet alleen persoonsgegevens. Een andere categorie gegevens waaraan gedacht kan worden, betreft *bedrijfs- of fabricagegegevens.* Het gaat hier om gegevens die bijvoorbeeld in het kader van de uitoefening van toezicht zijn verzameld. Verder valt te wijzen op gegevens die uitsluitend voorwerpen aanduiden, bijvoorbeeld gestolen goederen of identiteitsbewijzen. Dergelijke gegevens zijn geen persoonsgegevens indien deze geen informatie bevatten met behulp waarvan personen in hun maatschappelijke positie kunnen worden geraakt. Het gaat dan om zuivere *objectgegevens.* Hetzelfde geldt voor gegevens die onroerende zaken of andere registergoederen identificeren. Het feit dat deze zaken via een openbaar register zoals de kadastrale registratie tot een individuele natuurlijke persoon kunnen worden herleid, doet hieraan op zichzelf niet af.[18]

2.4 Verschillende typen gegevensuitwisseling (gaat het bij dit en het volgende punt nu om aspecten bij gegevensuitwisseling?)

Bij het inventariseren van knelpunten in de gegevensuitwisseling en de verkenning van de mogelijkheden om deze met een kaderwet op te lossen, is het van belang vooraf te onderkennen dat gegevensuitwisseling[19] verschillende verschijningsvormen kan hebben. Deze vormen laten zich categoriseren naar niveau van uitwisseling, naar vorm van verwerking, naar de aard van de uitwisseling, naar de vraag of van unilaterale, bilaterale dan wel multilaterale verstrekking sprake is, naar herkomst en – tot slot - naar de adressant van de gegevens.

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

1. *Strategisch.* Het gaat hierbij om verwerking van gegevens, veelal van statistische aard, met het oog op het signaleren van trends en ontwikkelingen. Hiervoor worden in beginsel geen persoonsgegevens gebruikt.
2. *Tactisch.* Het gaat hierbij om verwerking van gegevens om tactische analyses te maken die uitmonden in mogelijke interventiestrategieën. Voorbeelden hiervan op het bredere terrein van criminaliteitsbestrijding en handhaving zijn de Bestuurlijke Criminaliteitsbeeldanalyses (BCBA's) die de RIEC's opstellen[20], en de gebiedsscans die de Omgevingsdiensten uitvoeren. Voor het opstellen van dergelijke analyses kan het noodzakelijk zijn ook persoonsgegevens te

[17] Dat is bijvoorbeeld het geval wanneer de politie op grond van artikel 20 Wpg gegevens verstrekt aan de reclassering en de reclassering in het kader van een publiekrechtelijk samenwerkingsverband deze gegevens wil doorverstrekken aan de gemeente. Met het oog op een dergelijke situatie bepaalt artikel 22, zesde lid, Wbp dat het verbod om strafrechtelijke persoonsgegevens te verwerken, niet van toepassing is op verwerkingen door of ten behoeve van publiekrechtelijke samenwerkingsverbanden van verantwoordelijken of groepen van verantwoordelijken, indien de verwerking noodzakelijk is voor de uitvoering van de taak van deze verantwoordelijken of groepen van verantwoordelijken en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad (Kamerstukken II 2008-2009, 31 841, nr. 3, blz. 9).

[18] Kamerstukken II 1997-1998, 25892, nr. 3, blz. 47.

[19] Onder gegevensuitwisseling wordt hier in termen van de Wbp verstaan: de verstrekking van gegevens aan het samenwerkingsverband en de verdere verwerking van die gegevens binnen het samenwerkingsverband.

[20] Zie: http://www.riec.nl/instrumenten/bcba.

gebruiken. Daarbij kunnen zo mogelijk vormen van pseudonimisering of anonimisering worden toegepast.[21]

3. *Operationeel/zaaksgericht.* Het gaat hierbij om gegevensuitwisseling in een concrete casus met als doel het verkrijgen van een goede informatiepositie op basis waarvan gezamenlijk kan worden bezien welke aanpak het meest effectief is. Voorbeelden hiervan zijn de gegevensuitwisseling binnen het FEC voor het opstellen van adviezen aan de FEC-partners voor het uitvoeren van bepaalde interventies[22] en de inkomens- en vermogensrapporten van de iCOV[23]. Het opstellen van dergelijke casusanalyses brengt uit de aard der zaak mee dat persoonsgegevens worden verwerkt. Het niveau van gegevensuitwisseling kan van invloed zijn

Met opmerkingen | Is het verschil hiertussen uit te leggen?

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

1. *Handmatig*. Te denken valt aan schriftelijke en mondelinge gegevensuitwisseling tijdens zgn. informatietafels of –pleinen in samenwerkingsverbanden.
2. *Geautomatiseerd*. Hierbij kan worden gedacht aan gegevensuitwisseling door koppeling van bestanden van verschillende partners om met behulp van geavanceerde software bepaalde patronen te ontdekken ("datamining")[24], gerichte bevragingen in databestanden van verschillende partners om bepaalde profielen vast te stellen ("profiling") en opslag van uitgewisselde gegevens in een nieuw databestand. Dergelijke verwerkingen vinden plaats met behulp van speciale beveiligde internet-applicaties, zoals het "Colleges Collaboration Tool" (CoCoTo) van het FEC, Inspectieview Milieu van de Inspectie Transport en Leefomgeving[25], het RIEC-IS van de RIEC's[26] en het Systeem Risico Indicatie (SyRI) dat de zgn. interventieteams gebruiken.[27]

Als het gaat om de *aard van de uitwisseling*, kan zowel worden gedacht aan verstrekking op ad-hoc-basis ten behoeve van een bepaalde casus als aan gegevensuitwisseling van structurele aard. Bij het laatste valt te denken aan het maandelijks aan elkaar rapporteren van controles in een bepaald gebied en aan bepaalde periodieke producten, zoals de iCOV-rapportage Inkomen en Vermogen.

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

De herkomst van de gegevens kan divers zijn. Een belangrijke, zo niet belangrijkste bron van de gegevens zal bij samenwerkingsverbanden uiteraard gelegen zijn in verstrekking door de deelnemers zelf. De samenwerking zal immers mede gestoeld zijn op de gedachte dat de deelnemers over gegevens beschikken die voor de andere deelnemers met het oog op het doel van het samenwerkingsverband van belang zijn. De gegevens kunnen echter ook een andere herkomst

---

[21] Bij pseudonimisering wordt een identificerend gegeven vervangen door een ander identificerend gegeven. Bij anonimisering worden gegevens omgezet naar een vorm die identificatie niet langer mogelijk maakt.
[22] Zie het FEC-jaarverslag 2012-2014, voor het jaar 2014, blz. 9 (http://www.fec-partners.nl/media/76/42/705631/123/fec-jaarverlag_2012_-_2014_voor_het_jaar_2012.pdf).
[23] Zie Convenant iCOV 2013, Stcrt. 2013, 24607 (https://zoek.officielebekendmakingen.nl/stcrt-2013-24607.html). .
[24] Bij deze vorm van gegevensverwerking doet de computer in feite zelf het werk. Mits de te verwerken data voldoende gestructureerd worden aangeboden, kunnen bepaalde computertools zelf uit deze data mogelijk relevante patronen halen. Daarmee kunnen modellen worden gemaakt waarmee niet alleen actuele risico's in beeld kunnen worden gebracht, maar ook voorspellingen doen omtrent risico's die zich mogelijk in de toekomst gaan voordoen ("predictive modelling").
[25] Zie http://www.informatieuitwisselingmilieu.nl/pagina.php?id=3.
[26] Zie het jaarverslag 2012 van het LIEC, blz. 28 (http://www.liec.nl/doc/130136_RIEC-LIEC-Jaarverslag_web.pdf).
[27] Zie artikel 65 van de Wet structuur uitvoeringsorganisatie werk en inkomen (Wet Suwi).

hebben. Daarbij kan worden gedacht aan gegevens uit openbare registers, gegevens uit andere openbare bronnen, gegevens uit registraties met authentieke gegevens, zoals de Basisregistratie personen, en gegevens die van bedrijfsinformatiebureaus als Dunn & Bradstreet afkomstig zijn.[28]

Tot slot de *adressant van de gegevens*. Bij samenwerkingsverbanden kan de gegevensuitwisseling in de eerste plaats bestaan uit directe verstrekking van gegevens aan één of meer andere partners in het verband, zonder dat deze gegevens in een apart bestand worden opgeslagen.[29] Voor deze vorm van gegevensuitwisseling zijn alleen de wettelijke regelingen van belang die voor de betrokken partijen gelden voor het verstrekken van gegevens aan het samenwerkingsverband, voor de politie de Wpg, voor het OM de Wjsg en voor de overige betrokken partners de Wbp (tenzij voor hen ook een bijzondere wet geldt). De gegevensuitwisseling kan ook bestaan uit verstrekking aan het samenwerkingsverband zelf, waarbij een organisatie die het verband ondersteunt, de verstrekte gegevens verwerkt tot specifieke informatieproducten als een casusanalyse, een gebiedsscan of profielen van bepaalde personen of bedrijven. Deze informatieproducten worden dan vervolgens weer ter beschikking gesteld van de deelnemers aan het samenwerkingsverband. De verwerking van gegevens tot dergelijke informatieproducten valt onder de Wbp. Zo'n verwerking zal in beginsel moeten worden aangemeld bij het College bescherming persoonsgegevens (art. 27 Wbp e.v.).

Met opmerkingen Dit is mi veel te kort door de bocht. Als het erom gaat de verschillende modaliteiten en gegevensverstrekkingen binnen samenwerkingsverbanden te schetsen kan dit anders.

2.5 Belang van zorgvuldigheid bij gegevensuitwisseling

Met opmerkingen Deze paragraaf zegt niet wat hij beoogt en beoogt niet wat hij zegt (of juist wel?). Wat ik bedoel is dat het FIN-verhaal over zorgvuldigheid nu net beoogde op ieder niveau en in iedere fase wel o.a. ook de verenigbaarheidstoets toe te passen hoe lastig dat wellicht ook is omdat dat nu eenmaal voortvloeit uit de internationale regelingen.

Bij een verkenning naar een kaderwet gegevensuitwisseling kan het niet alleen gaan om het verkennen van mogelijkheden om knelpunten weg te nemen die op dit moment met betrekking tot het uitwisselen van gegevens bestaan. 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 een goede balans moeten worden gevonden tussen enerzijds de met een kaderwet beoogde verbetering van de mogelijkheden van gegevensuitwisseling en anderzijds de behoefte aan zorgvuldigheid bij die uitwisseling. Beide kunnen hand in hand gaan, als een kaderwet niet alleen knelpunten wegneemt, maar ook de nodige waarborgen voor een zorgvuldige gegevensverwerking bevat. Zo'n kaderwet kan dan ook een nieuwe impuls geven aan een zorgvuldige omgang met gegevens in de al bestaande praktijk van gegevensuitwisseling.

Met opmerkingen Klinkt mooi maar deze wet kapt dus juist iedere zorgvuldigheid af!

Dat bij iedere vorm van gegevensverwerking zorgvuldigheid voorop dient te staan, is op zich niets nieuws. De Wbp schrijft in artikel 6 nu al voor dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt. Waar het bij een verruiming van mogelijkheden van gegevensuitwisseling in samenwerkingsverbanden evenwel om gaat, is dat het principe van een zorgvuldige omgang met persoonsgegevens nog meer dan nu een algemeen erkende en aanvaarde praktische toetssteen bij de inrichting van deze gegevensuitwisseling zou kunnen vormen.

Zo'n toetssteen zou uiteraard in de eerste plaats gestoeld kunnen worden op een aantal bestaande waarborgen, zoals het principe van doelbinding, het noodzakelijkheidsvereiste en de beginselen van proportionaliteit en subsidiariteit. Dergelijke waarborgen vloeien al uit internationale verdragen, EU-richtlijnen en de daarop gebaseerde nationale wetten ter bescherming van persoonsgegevens voort. Wil het principe van een zorgvuldige omgang met persoonsgegevens in samenwerkingsverbanden een voldoende praktische toetssteen kunnen vormen, dan is het wenselijk dat een eventuele kaderwet een aantal aanvullende, meer specifieke waarborgen bevat. Welke waarborgen dat kunnen zijn, komt hierna in § 4.7 aan de orde.

Met opmerkingen Kan hier al een klein doorkijkje worden gegeven?

[28] Vgl. artikel 7 Protocol gegevensverwerking iCOV Productie 2013, Stcrt. 2013, 24608.

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

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

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

Met opmerkingen | Welke?

2.6 Betere gegevensuitwisseling: zaak van meer dan wetgeving alleen

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

De bereidheid tot samenwerking hangt in de praktijk meestal af van de vraag of betrokken partijen belang in samenwerking zien. Vaak is het belang daarvan evident en soms is de samenwerking zelfs verankerd in wetgeving.[30] Intussen dringt wel steeds meer het besef bij overheidsorganisaties door dat het belang van samenwerking niet uitsluitend gelegen hoeft te zijn in een specifiek belang dat een individuele organisatie bij een eigen goede taakuitvoering heeft, maar dat met samenwerking ook een breder, overkoepelend overheids belang kan en mag dienen. Als organisaties dat niet al uit zichzelf zijn gaan beseffen, is het wel de publieke opinie die daartoe een stimulans geeft. Zoals ook al in § 2.1 naar voren kwam, verwachten burgers en bedrijven immers in toenemende mate dat de overheid als één georganiseerd geheel optreedt.

Een en ander neemt niet weg dat samenwerking waar dat mogelijk en zelfs nodig zou zijn, niet steeds vanzelfsprekend is. Het komt nog voor dat cultuurverschillen en verkokerd denken samenwerking in de weg staan.[31] Hier ligt vooral een bestuurlijke opgave om deze drempels tot samenwerking te slechten. Een kaderwet gegevensuitwisseling kan in dit verband helpen, omdat het niet langer mogelijk is zich te verschuilen achter het argument dat bepaalde wettelijke voorschriften het uitwisselen van gegevens belemmeren en daarmee de mogelijkheden tot samenwerking beperken.

Met opmerkingen | Dat is maar de vraag.

De bereidheid tot het uitwisselen van gegevens zal ook zijn ingegeven door het belang dat men daarbij heeft. Het directe belang bij de verstrekking van gegevens zal doorgaans bij de ontvangende partij liggen. Deze zal immers mede op basis van de ontvangen informatie een analyse kunnen uitvoeren, een interventie kunnen plegen dan wel daarop een andere handeling kunnen baseren. Doch ook de verstrekkende partij kan indirect belang bij de verstrekking hebben. Zo kan verstrekking van gegevens door de politie aan een gemeente ertoe leiden dat de gemeente een maatregel neemt die een bepaalde vorm van criminaliteit voorkomt, zodat de politie niet zelf hoeft op te treden. In dit licht bezien hoeft samenwerking niet te betekenen dat er altijd van een

[30] Een voorbeeld daarvan is de samenwerking tussen het UWV, de SVB en de gemeenten bij de uitvoering van de Wet structuur uitvoeringsorganisatie werk en inkomen (Wet Suwi) enige andere wetten. Zie daarvoor art. 9 Wet Suwi.

[31] Zie in dit verband ook: A.J.C. de Moor-van Vugt, Gegevensuitwisseling door Toezichthouders; onderzoek uitgevoerd in opdracht van het WODC, 2012, blz. 56.

bilaterale of multilaterale verstrekking van gegevens sprake moet zijn; ook een unilaterale verstrekking van gegevens kan de belangen van beide betrokken partijen dienen.

In het geval dat er bij een partij geen taken of belangen zijn aan te wijzen die tot verstrekking van gegevens aan een andere partij nopen, kan een goede taakuitvoering door die andere partij toch aanleiding tot verstrekking zijn. Uitgaande van een kaderwet die in zo'n geval verstrekking mogelijk maakt, is ook dan vooral sprake van een bestuurlijke opgave om deze mogelijkheid te benutten door daarover afspraken te maken. Als deze opgave niet wordt opgepakt, resteert slechts het middel van een wettelijke verplichting tot verstrekking.

Met opmerkingen | Mi weg.

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

Voordat tot gegevensuitwisseling wordt overgegaan, dienen betrokken partijen daarover goede afspraken te maken. Afspraken over het doel van de samenwerking, de aansturing van het samenwerkingsverband en de hoofdlijnen van de gegevensuitwisseling worden vaak – zie ook § 2.2 - in een convenant vastgelegd. Afspraken over de gegevensuitwisseling worden dan meestal uitgewerkt in een informatie- of privacyprotocol. Daarbij is van belang een heldere beschrijving te geven van de inrichting van de gegevensuitwisseling: welke partijen wisselen welke gegevens in welk proces uit om tot welk resultaat of product te komen? Bij de inrichting daarvan moet uiteraard acht worden geslagen op de vorm en mate waarin hiervoor relevante regelgeving de gegevensuitwisseling toelaten.

Ter ondersteuning van het samenwerkingsverband wordt vaak een bureau in het leven geroepen die voor de feitelijke gegevensuitwisseling zorgdraagt, analyses en rapportages opstelt en adviezen geeft. Afhankelijk van de gemaakte afspraken beheert zo'n organisatie vaak ook een informatiesysteem waarin de uitgewisselde gegevens worden verwerkt. Een heldere beschrijving van de inrichting van de gegevensuitwisseling is niet alleen nodig om die uitwisseling goed te laten verlopen, maar ook een randvoorwaarde voor het opzetten van een dergelijk informatiesysteem. Daarmee wordt voorkomen dat een systeem wordt ontwikkeld dat naderhand gegevens blijkt te verwerken op een wijze die niet strookt met de geldende regelgeving, en dan tegen wellicht hoge kosten moet worden aangepast.

2.7 Relevante andere ontwikkelingen

Bij deze verkenning is mede acht geslagen op verschillende ontwikkelingen die relevant zijn voor gegevensverwerking in het algemeen~~relevantie voor de verkenning hebben~~.

Een eerste ontwikkeling die hier wordt genoemd, betreft het onderzoek dat in het verleden naar gegevensuitwisseling door toezichthouders is verricht. In 2008 heeft een interdepartementale werkgroep herijking toezichtregelgeving onderzocht wat de mogelijke juridische belemmeringen zijn voor de voortzetting en intensivering van de samenwerking tussen de rijksinspecties en welke mogelijkheden er zijn deze belemmeringen weg te nemen. De werkgroep kwam tot de conclusie dat een algemene wettelijke regeling voor de informatie-uitwisseling tussen inspecties die een gelijk regime voor alle inspecties zou creëren, niet goed mogelijk en niet wenselijk is. De werkgroep voerde daartoe aan dat er immers sprake is van nogal uiteenlopende toezichthoudende organen, die gegevens van allerlei aard uitwisselen waarvoor diverse regimes gelden. Het zou volgens de werkgroep zeer de vraag zijn of het zou lukken deze regimes in een overkoepelende regeling onder te brengen. Bovendien zou een algemeen geldende doelomschrijving voor de overdracht van gegevens voor inspectiedoeleinden op problemen kunnen stuiten in relatie tot de eis uit artikel 6 van de Europese privacyrichtlijn dat het doel van de verwerking van

persoonsgegevens welbepaald moet zijn.[32] Het toenmalige kabinet nam deze conclusie over.[33] Bij de behandeling van het kabinetsstandpunt inzake het advies van de Commissie Brouwer-Korf en de evaluatie van de Wbp is op aandringen van de Tweede Kamer toegezegd de mogelijkheid van een dergelijke algemene regeling toch te bezien.[34] Het toenmalige kabinet heeft in dat verband gewezen op de mogelijkheid van een algemene wettelijke bepaling die inhoudt dat gegevens in het kader van een structurele samenwerking kunnen worden uitgewisseld, mits de afspraken tot samenwerking op een wettelijk voor te schrijven wijze zijn bekendgemaakt.[35] De toezegging van het kabinet heeft geleid tot een onderzoek in opdracht van het WODC naar gegevensuitwisseling door toezichthouders. Dat onderzoek heeft geleid tot een rapport waarin wordt aanbevolen om – mede ten behoeve van een vereenvoudiging en verduidelijking van de eis van doelbinding – de huidige Wbp om te vormen tot een brede kaderwet, eventueel met nadere uitwerking in sectorale wetgeving. Ook bevat het rapport aanbevelingen voor het gebruik van convenanten ten behoeve van structurele gegevensverstrekking in publiekrechtelijke samenwerkingsverbanden.[36] Het kabinet heeft in reactie op dat rapport zich op het standpunt gesteld dat de herziening van de Europese regelgeving inzake de verwerking en bescherming van persoonsgegevens (zie hierna) een goed moment is voor een meer algemene bezinning op het huidige nationale kader, waarin het zwaartepunt ligt bij de sectorale wetgeving.[37] Al deze aspecten zullen in deze verkenning moeten worden meegewogen, meer in het bijzonder bij een bespreking van de mogelijke contouren van een eventuele kaderwet (zie § 4).

Met opmerkingen | Is dat niet de context voor ons werk?

Een ontwikkeling waarmee ook rekening moet worden gehouden, is de inwerkingtreding op 1 januari 2014 van de Wet tot wijziging van de Wet structuur uitvoeringsorganisatie werk en inkomen (Suwi) en enige andere wetten in verband met fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekende zijnde gegevens (Stb. 2013, 405). Deze wet introduceert nieuwe mogelijkheden van gegevensuitwisseling voor de aanpak van fraude op het terrein van sociale zekerheid en inkomensafhankelijke regelingen, belastingen, premies en arbeidswetten. Zij geeft tevens een wettelijke verankering van het instrument Systeem Risico Indicatie (SyRI). SyRI omvat de technische infrastructuur en bijbehorende procedures om in een beveiligde omgeving op een zorgvuldige manier gepseudonimiseerde data te koppelen en te analyseren, zodat op basis daarvan risicomeldingen met betrekking tot mogelijke fraude kunnen worden gegenereerd. SyRI kan worden gebruikt door samenwerkingsverbanden waaraan in ieder geval de gemeenten, de Belastingdienst, het UWV, de SVB en de Inspectie SZW deelnemen. In zekere zin kan deze wet tot wijziging van de Wet Suwi worden gezien als inspiratiebron voor de onderhavige verkenning naar een kaderwet gegevensuitwisseling. Immers, verschillende elementen van deze wijzigingswet en het daarop gebaseerde uitvoeringsbesluit[38] zijn in enigerlei vorm terug te vinden in § 4 van deze notitie, waarin de contouren van een mogelijke kaderwet gegevensuitwisseling worden beschreven. Te denken valt aan de ruime doelbinding, de toepasselijkheid op meerdere samenwerkingsverbanden en een aantal waarborgen, zoals de noodzakelijke expliciete toets aan de beginselen van proportionaliteit en subsidiariteit.

Met opmerkingen | Of liever doelstelling?

Met opmerkingen | Zit al in Wbp

Een ander relevant traject wordt gevormd door de beleidsvisie van het kabinet met richtlijnen voor het zorgvuldig omgaan met persoonsgegevens in de gemeentelijke praktijk in het kader van de zgn. drie decentralisaties. Bij het opstellen van die visie is uitgegaan van het belang dat gemeenten op een soepele manier informatie over burgers kunnen opvragen en uitwisselen, zonder dat er nodeloos of overmatig gegevens worden opgevraagd, gedeeld of anderszins

[32] Rapport van de werkgroep herijking toezichtregelgeving, 2008, § 4.2.2.
[33] Kamerstukken II 2008-2009, 31700 VI, nr. 70.
[34] Kamerstukken II 2009-2010, 31051, nr. 7, blz. 19.
[35] Kamerstukken II 2008-2009, 31700 VI, nr. 118, blz. 9.
[36] De Moor-van Vugt, a.w., blz. xiv.
[37] Kamerstukken II 2012-2013, 32761, nr. 43.
[38] Besluit van PM tot wijziging van het Besluit SUWI in verband met regels voor fraudeaanpak door gegevensuitwisseling en het effectief gebruik van binnen de overheid bekend zijnde gegevens met inzet van SyRI (Stb. PM).

verwerkt. Bij de totstandkoming van die visie is vooralsnog geconcludeerd dat er voor het mogelijk maken van de gewenste gegevensdeling geen noodzaak is voor een nieuw juridisch kader voor gegevensverwerking en privacy in het sociaal domein.[39] Dit impliceert dat de onderhavige verkenning, voor zover zij al op een breder terrein dan fraudebestrijding betrekking heeft, in ieder geval niet het sociaal domein omvat waarop de drie decentralisaties zich afspelen.

Deze verkenning vertoont ook samenhang met het rapport "Dienstbaar en transparant" van het project SGO-3. In dat rapport adviseert de stuurgroep SGO-3 een programma te starten voor het ontwikkelen van een kaderwet die de hanteerbaarheid van de huidige privacywet- en regelgeving verbetert. De stuurgroep adviseert om dit traject af te stemmen met de onderhavige verkenning naar de mogelijkheden van een kaderwet voor de gegevensuitwisseling ten behoeve van de fraudebestrijding. Het traject zou volgens de stuurgroep een plaats moeten krijgen in het wetgevingsprogramma dat op dit moment wordt ontwikkeld door de ministeries van BZK, EZ en VenJ.[40]

Met opmerkingen Weer een ons onbekend traject.

Voor deze verkenning is ook relevant dat op dit moment in Brussel onderhandelingen plaatsvinden over voorstellen van de Europese Commissie voor een Algemene verordening gegevensbescherming[41] en een Richtlijn gegevensbescherming opsporing en vervolging[42]. De beoogde verordening moet de Europese privacyrichtlijn uit 1995[43] vervangen. Als verordening zal zij directe werking in Nederland hebben en tot gevolg hebben dat de Wet bescherming persoonsgegevens en bepalingen ter bescherming van persoonsgegevens in specifieke wetten overbodig worden dan wel aanpassing behoeven. De beoogde richtlijn gegevensbescherming opsporing en vervolging zal geen directe werking hebben en moeten worden omgezet in nationale wetgeving. Als gevolg daarvan zullen de Wet bescherming persoonsgegevens, de Wwet politiegegevens en de Wet justitiële en strafvorderlijke gegevens aanpassing behoeven. Beide voorstellen van de Europese Commissie bevatten geen bepalingen die specifiek op gegevensuitwisseling in samenwerkingsverbanden betrekking hebben. Dat neemt niet weg dat bij de verdere voorbereiding van een eventuele kaderwet met de komende verordening en richtlijn rekening moet worden gehouden. In § 4.12 wordt daaraan al een eerste beschouwing gewijd.

Met opmerkingen MI: moet passen binnen.

Een laatste relevante ontwikkeling waarop in deze verkenning wordt gewezen, is de evaluatie van de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Deze evaluatie heeft geleid tot een brief van de Minister van Veiligheid en Justitie van 23 juni 2014 aan de Tweede Kamer, waarin hij een perspectief schetst op de toekomstige omgang met politiële, justitiële en strafvorderlijke gegevens. In de brief wordt de conclusie getrokken dat deze wetten moeten worden gemoderniseerd, waarbij de verschillende regimes die van toepassing zijn op politiële, justitiële en strafvorderlijke gegevens, moeten worden geharmoniseerd, het gebruik van gegevens en niet de bewaartermijnen het uitgangspunt van de nieuwe regelgeving moet zijn en het toezicht op het gebruik en de verstrekking van gegevens moet worden versterkt. Deze modernisering van de regelgeving en de uitvoering is volgens de Minister ambitieus en zal de nodige tijd kosten.[44] Met betrekking tot samenwerkingsverbanden merkt hij in de brief op dat in verschillende verbanden, waarin ook politiële, justitiële en strafvorderlijke gegevens worden uitgewisseld, in toenemende mate met convenanten en privacyprotocollen wordt gewerkt. Hij stelt daarbij dat hij deze werkwijze krachtig verder zal bevorderen.[45] Bij de voorbereiding van een

Met opmerkingen Het zou heel goed zijn wanneer die operatie gelijk wordt ondernomen met de aanpassing van de Wbp zodat de verschillende ontwikkelingen dit keer wel zo veel mogelijk op elkaar worden afgestemd. De verschillende kaderwetten voor het bestuursrecht en het strafrecht in een wet onderbrengen zou de ideale oplossing zijn want dan wordt met een begrippenarsenaal gewerkt! Ook in het buitenland geschiedt dat!

[39] Kamerstukken II 2013-2014, 32761, nr. 62, blz. 1.
[40] Eindrapport project SGO-3 "Versnelde effectieve inzet van basisregistraties", mei 2014, blz. 45 (http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2014/05/22/de-basisregistraties-van-de-nederlandse-overheid-dienstbaar-en-transparant.html).
[41] Zie voorstel van de Europese Commissie van 25 januari 2012, COM(2012)11.
[42] Zie voorstel van de Europese Commissie van 25 januari 2012, COM(2012)10.
[43] Richtlijn 95/46/EG van het Europees parlement en de Raad van 24 oktober 1995, betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, Pb L 281.
[44] Kamerstukken II 2013-2014, 33842, nr. 2, blz. 1-2.
[45] Idem, blz. 8.

eventuele kaderwet gegevensuitwisseling zal met dit moderniseringstraject rekening moeten worden gehouden en zal ook het belang van convenanten en privacyprotocollen moeten worden meegewogen.

Basisregistraties, digitalisering etc?

3. Knelpunten

3.1 Inleiding

In § 1 van deze verkenning is naar voren gebracht dat de werkgroep haar verkenning van knelpunten bij de gegevensuitwisseling in samenwerkingsverbanden gebaseerd heeft op bestaande ervaringen, een brainstormsessie met experts, de bestudering van een viertal casussen en van literatuur, officiële publicaties en websites. De werkgroep merkt in dit verband op dat zij weliswaar primair aandacht heeft besteed aan gegevensuitwisseling ten behoeve van de fraudebestrijding, maar zich niet tot dat terrein heeft beperkt. Dat heeft twee redenen. De eerste is dat bestaande samenwerkingsverbanden zich maar zeer ten dele met uitsluitend fraudebestrijding bezighouden (zie § 2.2). De tweede reden is dat knelpunten bij gegevensuitwisseling ten behoeve van andere doeleinden evenzeer van belang kunnen zijn, zeker in het geval voor een kaderwet met een bredere reikwijdte dan alleen fraudebestrijding zou worden gekozen (zie nader § 4.2).

Met opmerkingen [ ]: Breder opzetten: van opdracht naar analyse knelpunten van gegevensverwerking en dan beperken tot samenwerkingsverbanden.

Met opmerkingen [ ]: Het ligt anders: gegevensuitwisseling ikv fraudebestrijding of ikv samenwerkingsverbanden is niet anders dan gegevensuitwisseling voor andere doeleinden, maw als je je dus al wil richten of die beperkte vorm van gegevensuitwisseling loop je onherroepelijk aan tegen de algemene probelematiek bij gegevensuitwisseling.

3.2 Verschillende wettelijke kaders

Met opmerkingen [ ]: Plus onduidelijke wettelijke kaders en probleem wettelijke kaders niet toegesneden op huidige behoefte aan grootschalige gegevensuitwisseling.

Gegevensverwerking heeft altijd een centrale plaats gehad bij de interne werkprocessen van veel overheidsorganisaties en in de verhouding overheid-burger. Gegevensverwerking is immers een belangrijk onderdeel van en dienstbaar aan de opgedragen taak van praktisch iedere overheidsinstelling. Iedere overheidsinstelling heeft zijn eigen taak en oefent een eigen gegevenshuishouding uit bij de uitvoering van die taak. Zolang de gegevensverwerking plaats vindt binnen het kader van de eigen taak, wordt de bevoegdheid tot dergelijke gegevensverwerking geacht op te gaan in de algemene taakomschrijving nu die dienstig is aan die taakinvulling en daarvoor noodzakelijk is. In deze situatie is het opnemen van bepalingen rond gegevensverwerking beperkt tot het opnemen van informatieverplichtingen voor burgers die met de betrokken overheidsinstelling te maken hebben. Ook is meestal sprake van een geheimhoudingsbepaling voor de betrokken overheidsdienst zodat de burger of het bedrijf erop kan vertrouwen dat zijn gegevens in veilige handen zijn (zie ook § 3.5). Daarmee is sprake van geïsoleerde, 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 juridische noodzaak een dergelijke uitwisseling van gegevens juridisch in te kaderen c.q. van een adequate juridische grondslag te voorzien. De bevoegdheid gegevens uit te wisselen met een ander valt in beginsel buiten de taakomschrijving van de betrokken overheidsdienst, zoals die 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 bilaterale verstrekking en niet op verstrekking aan meerdere partijen tegelijk die in een samenwerkingsverband opereren.[46]

[46] 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

Gelet op de specifieke context waarin overheidsorganisaties moeten opereren, is de systematiek van de bestaande wetgeving voor iedere individuele organisatie wellicht nog te begrijpen en te billijken. Deze systematiek van de wetgeving is voor samenwerkingsverbanden echter wel erg complex. Zo complex dat het ook voor deskundigen lastig is door de bomen het bos te zien. Het gaat dan nog niet eens zozeer om het grote aantal normen dat in acht moet worden genomen, maar meer nog om het feit dat die normen in relatie tot samenwerkingsverbanden in bepaalde gevallen niet goed te duiden zijn. Het kan dan bijvoorbeeld gaan om de vraag of en, zo ja, in hoeverre bepalingen die bilaterale verstrekking mogelijk maken, ook kunnen worden benut voor gegevensuitwisseling binnen het samenwerkingsverband.[47] 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.

Met opmerkingen ☐ Anders, zie hiervoor.

Tegen deze achtergrond is meer in het bijzonder bij de evaluatie van de Wpg en de Wjsg gebleken dat bij verstrekking van strafrechtelijke gegevens aan samenwerkingsverbanden zich verschillende knelpunten voordoen. De belangrijkste knelpunten die in dit verband bij de evaluatie van de Wpg zijn genoemd, zijn onduidelijkheid over wanneer verstrekken begint, wat je mag verstrekken, de soms tegenstrijdige wettelijke kaders, de plaats en positie van convenanten en hoe het staat met de informationele privacy nadat verstrekt is.[48] De evaluatie van de Wjsg laat zien dat het bij samenwerkingsverbanden zelfs voor goed ingelichte betrokkenen vaak niet duidelijk is of gegevens nu via de Wpg, de Wjsg of zelfs via de Wbp moeten worden verwerkt. Daar komt bij dat, als gegevens onder de werking van zowel de Wjsg als de Wpg (lijken te) vallen, men voor verstrekking van gegevens aan samenwerkingsverbanden voor het ruimere regime van de Wpg kiest boven dat van de Wjsg.[49]

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 een kaderwet een oplossing zou kunnen bieden.

Met opmerkingen ☐ Innerlijk tegenstrijdig.

3.3 Rechtvaardigingsgronden

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

Persoonsgegevens mogen ingevolge artikel 7 Wbp alleen worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Wanneer sprake is van

---

met betrekking tot verstrekking van strafrechtelijke gegevens door en ten behoeve van samenwerkingsverbanden.

[47] Zo merkte de Raad van State in zijn advies over het voorstel tot wijziging van de Wet op het financieel toezicht en enige andere wetten (Wijzigingswet financiële markten 2014) op dat toezichthouders toezichtvertrouwelijke informatie slechts mogen verstrekken in één-op-één relatie met in de wet genoemde partijen. Deze eis stond volgens de Raad in de weg aan hetgeen met het voorstel wordt beoogd, namelijk het mogelijk maken van informatie-uitwisseling binnen het FEC. De regering heeft de desbetreffende bepaling vervolgens zo aangepast dat de informatie slechts mag worden verstrekt als dat voor de ontvangende partij dienstig is voor de uitoefening van haar wettelijke taak (kamerstukken II 2012-2013, 33632, nr. 4, blz. 18-19).

[48] WODC, Glazen privacy. Knelpuntenonderzoek uitvoering Wet politiegegevens (Wpg), 2013, blz. 89.

[49] WODC, Onderzoeksrapport Evaluatie Wet justitiële en strafvorderlijke gegevens, 2013, blz. 84, 91.

"gerechtvaardigde doeleinden", valt af te leiden uit artikel 8 Wbp. Dat artikel bepaalt in een limitatieve opsomming van gronden wanneer de verwerking – dus ook het verzamelen - van persoonsgegevens gerechtvaardigd is. Dat is het geval wanneer de betrokkene uitdrukkelijk toestemming heeft verleend (a) of wanneer de verwerking noodzakelijk is ter uitvoering van een overeenkomst (b), ter nakoming van een wettelijke verplichting (c), ter vrijwaring van een vitaal belang van de betrokkene (d), voor de goede vervulling van een publiekrechtelijke taak door een bestuursorgaan (e) of ter behartiging van het gerechtvaardigde belang van de verantwoordelijke, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert (f).

Voor gegevensuitwisseling in samenwerkingsverbanden op het terrein van de fraudebestrijding geldt dat deze uiteraard niet afhankelijk kan zijn van toestemming van betrokkenen. Fraudeurs hebben er eerder belang bij dat hun gegevens niét worden uitgewisseld, als daardoor de kans groter wordt dat zij gepakt worden. Dat de gegevensuitwisseling noodzakelijk is ter uitvoering van een overeenkomst, zal zich bij dergelijke samenwerkingsverbanden ook niet voordoen. Op een wettelijke verplichting tot gegevensverstrekking kan ~~veelal ook geen~~lang niet altijd een beroep worden gedaan.[50] Daarbij moet worden bedacht dat een eventuele bevoegdheid tot gegevensverstrekking nog geen wettelijke verplichting impliceert. Ook van een vitaal belang van betrokkenen zal geen sprake zijn. Zo resteren de gronden e en f.

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

Met opmerkingen : Deze voorwaarde staat er dus aan in de weg gegevens te delen wanneer de doelstelling niet specifiek tot het taakgebied van de individuele deelnemers behoort.

Met opmerkingen : ism richtlijn/Wbp?

Kan aldus het vinden van een rechtvaardigingsgrond voor gegevensuitwisseling tussen bestuursorganen in een samenwerkingsverband al problemen opleveren, het ligt nog een slag lastiger, als aan een samenwerkingsverband ook private partijen – zie § 2.2 - deelnemen. Tenzij een sectorspecifieke wet voor dat geval gegevensverstrekking mogelijk maakt, zal de verstrekking uitsluitend kunnen worden gebaseerd op eerdergenoemde grond f. Een beroep op die grond brengt echter mee dat steeds een afweging voor het individuele geval moet worden gemaakt. Dat belemmert een structurele uitwisseling van gegevens. Als een eventuele kaderwet voor gegevensuitwisseling bij fraudebestrijding ook op uitwisseling met private partijen betrekking zou hebben, zou deze kaderwet die belemmering kunnen wegnemen.

Met opmerkingen : Geloof ik niet!

3.4 Verenigbaarheidstoets

Aan de rechtvaardigingsgronden van artikel 8 voegt artikel 9 Wbp de algemene eis toe dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (principe van doelbinding). Het doel van de gegevensuitwisseling in een samenwerkingsverband is in het algemeen een ander dan het doel waarvoor een deelnemer aan het verband de gegevens oorspronkelijk heeft verkregen. Dit brengt

[50] Een uitzondering hierop wordt gevormd door artikel 64, derde lid, Wet Suwi, waarin de deelnemers aan een samenwerkingsverband worden verplicht elkaar de noodzakelijke gegevens te verstrekken.

mee dat voor deze gegevensuitwisseling moet worden getoetst of zij al dan niet verenigbaar is met de doeleinden waarvoor de gegevens oorspronkelijk zijn verkregen.[51]

Aan het beginsel van doelbinding en daarmee aan de verenigbaarheidstoets moet – ook in het licht van de Europese privacyregelgeving – in algemene zin grote waarde worden toegekend. Het is echter de vraag of het noodzakelijk is ook voor samenwerkingsverbanden met een publiek doel als fraudebestrijding steeds een verenigbaarheidstoets te moeten uitvoeren. Deze vraag wordt ingegeven door de paradoxale situatie dat de taken en belangen van organisaties die aan een samenwerkingsverband deelnemen, veelal van dien aard zijn dat zij op beleidsmatige gronden graag de samenwerking aangaan, maar de uitvoering van de verenigbaarheidstoets in de praktijk een lastige hindernis blijkt te zijn en bij tijd en wijle een juridische rem zet op de bereidheid om gegevens uit te wisselen.[52] Dat uit zich onder meer in de vraag of strafrechtelijke gegevens, gelet op hun gevoeligheid, wel mogen worden gebruikt voor bestuurlijke doeleinden, als daarvoor niet een expliciete wettelijke grondslag bestaat.

Met opmerkingen Voor mij geen vraag!

Omdat de verenigbaarheidstoets niet enkel door de vastlegging van het doel van een samenwerkingsverband in een convenant achterwege kan worden gelaten, is een wettelijke voorziening nodig om dat mogelijk te maken. Het huidige artikel 43 Wbp biedt die mogelijkheid niet. Weliswaar geeft dat artikel voor bepaalde doeleinden de mogelijkheid om af te wijken van het principe van doelbinding, maar uit de zeer casuïstische jurisprudentie over artikel 43 Wbp kan worden afgeleid dat toepassing slechts is weggelegd voor uitzonderlijke gevallen en niet gebruikt kan worden als een grondslag voor permanente of anderszins structurele overdracht van gegevens.[53] In samenwerkingsverbanden is echter wel behoefte aan permanente, structurele uitwisseling van gegevens. Om dat mogelijk te maken zonder dat daarvoor eerst een verenigbaarheidstoets moet worden uitgevoerd, is derhalve een afzonderlijke wettelijke voorziening nodig. Zo'n voorziening zou kunnen inhouden dat in een kaderwet een breed doel voor gegevensuitwisseling in samenwerkingsverbanden wordt geformuleerd, waarbij wordt bepaald dat een specifiek samenwerkingsverband het meer bijzondere doel waarvoor zij gegevens uitwisselt, nader vastlegt.

Met opmerkingen Helpt niet nu de wettelijke doelstelling veel te algemeen is voor een verantwoorde afweging; wet zou de facto vrijbrief worden voor iedere gegevensdeling en dat gaat niet.

Met opmerkingen Dan geen afweging meer en dus geen waarborgen meer!

3.5 Geheimhoudingsplicht

De mate waarin gegevens binnen samenwerkingsverbanden kunnen worden uitgewisseld, wordt ook sterk bepaald door de bestaande geheimhoudingsplichten. Deze plichten kunnen zijn ingegeven met het oog op verschillende belangen. Daarbij kan het 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).[54]

---

[51] Voor het toetsen of er sprake is van verenigbaar gebruik draagt het tweede lid van artikel 9 Wbp de volgende vijf criteria aan:
1. de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen,
2. de aard van de gegevens,
3. de gevolgen van de beoogde verwerking voor de betrokkene,
4. de wijze waarop de gegevens zijn verkregen, en
5. de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

[52] Zie in dit verband ook: De Moor-van Vugt, a.w., blz. 35, 59.

[53] Vgl. kamerstukken II 2008-2009, 29911, nr. 23, blz. 8. Zie ook HR 31 januari 2012 (LJN: BT7126, pag. 19) en de Leidraad afstemmen van wetgeving op de Wet bescherming persoonsgegevens, 2010, blz. 68.

[54] 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.

Bij gegevensuitwisseling in samenwerkingsverbanden zijn de bescherming van private belangen en de zorg voor de goede werking van het openbaar bestuur het belangrijkst. 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.[55]

Een algemene geheimhoudingsplicht is opgenomen in de Algemene wet bestuursrecht (Awb). Artikel 2:5 Awb bepaalt dat een ieder die betrokken is bij de uitvoering van de taak van een bestuursorgaan en daarbij de beschikking krijgt over gegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden, verplicht is tot geheimhouding van die gegevens. Deze geheimhoudingsplicht is aanvullend: zij geldt niet voor wie reeds uit hoofde van ambt, beroep of wettelijk voorschrift ter zake van die gegevens een geheimhoudingsplicht geldt. Verder wijkt deze plicht voor een wettelijk voorschrift dat tot mededeling verplicht, terwijl ook uit de taakuitoefening een noodzaak tot mededeling kan voortvloeien. Tot de gegevens met een vertrouwelijk karakter kunnen onder meer bedrijfs- en fabricagegegevens en gegevens die betrekking hebben op de persoonlijke levenssfeer, worden gerekend.[56]

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

Naast deze algemene geheimhoudingsplichten bestaan ook tal van bijzondere geheimhoudingsbepalingen. Voor samenwerkingsverbanden op het terrein van de fraudebestrijding zijn vooral de geheimhoudingsbepalingen in de volgende wetten relevant: de Wjsg (art. 52), de Wpg (art. 7), de Algemene wet inzake rijksbelastingen (Awr, art. 67), de Wet op het financieel toezicht (Wft, art. 1:89 e.v.) en de Wet Suwi (art. 74). Deze wetten bevatten ook bepalingen die het mogelijk maken de geheimhoudingsplicht te doorbreken, maar daaraan zijn dan vaak wel de nodige voorwaarden verbonden.

Zo kent de Wjsg in de artikelen 8a en 39f het College van procureurs-generaal de mogelijkheid toe om, voor zover dat nodig is met het oog op een zwaarwegend algemeen belang, justitiële, respectievelijk strafvorderlijke gegevens aan derden te verstrekken ten behoeve van specifiek omschreven doeleinden. Artikel 8a ziet daarbij op de justitiële documentatie waarover het OM de beschikking heeft gekregen in het kader van de behandeling van een strafzaak.[57] Het biedt dus geen grondslag om het OM justitiële gegevens te vragen waarover het zelf niet beschikt. Daarvoor zal, zo nodig, op grond van artikel 9 Wjsg een voorziening kunnen worden getroffen in het Besluit justitiële en strafvorderlijke gegevens (Bjsg).

Met opmerkingen Welke partij wordt hier bedoeld?

Ook de Wpg biedt de mogelijkheid om politiegegevens aan derden te verstrekken. Op grond van artikel 18 Wpg kan in het Besluit politiegegevens (Bpg) worden vastgelegd aan welke instellingen voor welke doeleinden politiegegevens kunnen worden verstrekt. Artikel 18 kent daarnaast aan de Minister van Veiligheid en Justitie de bevoegdheid toe in bijzondere gevallen toestemming of

[55] De Moor-van Vugt, a.w. blz. 31.
[56] Kamerstukken II 1988-1989, 21221, nr. 3 blz. 57.
[57] Aanwijzing wet justitiële en strafvorderlijke gegevens, blz. 15-16.

opdracht te geven tot het verstrekken van daarbij door hem te omschrijven politiegegevens, voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang.[58] Verder biedt artikel 20 Wpg de korpschef de mogelijkheid in overeenstemming met het bevoegd gezag bepaalde politiegegevens aan samenwerkingsverbanden te verstrekken, voor zover dat noodzakelijk is met het oog op een zwaarwegend algemeen belang en voor bepaalde doeleinden, zoals het voorkomen en opsporen van strafbare feiten.

Een mogelijkheid om de geheimhoudingsplicht van artikel 67 Awr te doorbreken ten behoeve van de gegevensuitwisseling in samenwerkingsverbanden, ligt opgesloten in artikel 43c, eerste lid, onder m en w, van de Uitvoeringsregeling Awr. Ingevolge die bepaling kunnen gegevens worden verstrekt aan bepaalde bestuursorganen, voor zover deze gegevens nodig zijn om de samenwerking in het kader van de integrale toepassing en handhaving van overheidsregelingen effectief en efficiënt te laten verlopen en een convenant is gesloten met deze bestuursorganen.

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

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

Wat al deze mogelijkheden gemeen hebben, is dat zij weliswaar voor gegevensverstrekking aan samenwerkingsverbanden in verschillende mate enige ruimte geven, maar in de praktijk toch nog wel de nodige drempels opleveren. Zo geeft artikel 8a Wjsg toegang tot maar een deel van de justitiële gegevens. Verder lijkt de toetsing aan het criterium "zwaarwegend algemeen belang" bij de politie tot een zekere schroom te leiden om de mogelijkheden van artikel 20 Wpg te benutten. Het alternatief is gebruik maken van de mogelijkheid die artikel 9 Wjsg en 18 Wpg bieden om de verstrekking van gegevens aan samenwerkingsverbanden te regelen in het Bjsg, respectievelijk Bpg. De aard van die mogelijkheden brengt evenwel mee dat dit een regeling vergt voor ieder afzonderlijk samenwerkingsverband. Artikel 43c van de Uitvoeringsregeling Awr biedt op het eerste gezicht veel ruimte voor verstrekking van belastinggegevens, althans aan de met name genoemde partijen , maar stuit in de praktijk op toenemende terughoudendheid om deze ruimte te benutten gezien d ewel erg algemeen geformuleerde doelstelling van de samenwerkingsverbanden. ~~Met de invoering van het huidige artikel 67 Awr in 2008 is als lijn neergezet dat nieuwe gevallen die in de uitvoeringsregeling worden opgenomen zoveel mogelijk worden beperkt en dat~~Daarnaast wordt ernaar ~~wordt~~ gestreefd om gegevensverstrekking zo veel mogelijk bij wettelijk voorschrift te gaan regelen.[59] Ingeval van samenwerkingsverbanden zou dat evenwel kunnen impliceren dat voor ieder verband apart een wettelijke voorziening moet worden getroffen. ~~Er lijkt inmiddels wel ruimte te bestaan voor verstrekking van gegevens door de Belastingdienst aan het OM, zonder dat daarvoor een vordering van het OM op grond van artikel 126nd Wetboek van Strafvordering (WSv) nodig is.[60] Die ruimte is echter nog niet bevestigd door~~

[58] Van deze mogelijkheid is gebruik gemaakt om politiegegevens te verstrekken aan de RIEC's ten behoeve van de zgn. integrale casusanalyse. Zie Wpg-machtigingsbesluit RIEC's/werkproces integrale casusanalyse (Stcrt. 2013, nr. 6711).

[59] De Moor-van Vugt, a.w., blz. 33.

~~[60] Zie Hof Arnhem-Leeuwarden 8-11-2013, ECLI:NL:GHARL:2013:8478. In dit arrest heeft het Hof uitgemaakt dat verstrekking van gegevens door de belastingdienst aan het OM zonder vordering mogelijk is, voor zover dit zijn basis vindt in een convenant tussen betrokken partijen. Tenzij het convenant dat zou uitsluiten, is verstrekking ook mogelijk in het geval dat de persoon om wiens gegevens het gaat, als verdachte wordt~~

~~de Hoge Raad.~~ De mogelijkheden om op grond van de Wft gegevens aan andere partijen te verstrekken, is vanwege het ingrijpende karakter van de informatieverplichtingen van financiële ondernemingen aan de toezichthouders aan strenge voorwaarden verboden.[61] De Wet Suwi, tot slot, biedt een goede basis voor gegevensuitwisseling, maar doet dat niet voor alle vormen van fraudebestrijding, laat staan voor andere doeleinden op het terrein van rechtshandhaving en criminaliteitsbestrijding.

Wat zich hier wreekt, is dat, zoals ook hierv~~óó~~or al is gesignaleerd, de verschillende mogelijkheden tot verstrekking van gegevens aan andere partijen hoofdzakelijk zijn geformuleerd vanuit het perspectief van de verschillende sectoren en niet met het oog op een overkoepelend publiek belang van samenwerkingsverbanden. De geheimhoudingsbepalingen in die sectorwetten gaan voor verstrekking aan dergelijke verbanden uit van "nee, tenzij". Een kaderwet zou dit paradigma kunnen doen kantelen naar "ja, tenzij". Het "nee, tenzij" leidt in de praktijk ertoe dat de discussie vooral gaat over wat mag en wat niet mag en daarmee primair een juridische discussie is. De kanteling naar "ja, tenzij" zal meebrengen dat de discussie een meer beleidsmatig karakter krijgt. Zij zal zich toespitsen op de vraag "Willen wij met elkaar samenwerken en de daartoe noodzakelijke gegevens uitwisselen en welke gegevens menen wij eventueel daarvan te moeten uitzonderen?".

Een en ander heeft niet tot doel de betekenis van geheimhoudingsbepalingen als zodanig ter discussie te stellen. Integendeel, geheimhoudingsbepalingen dienen, zoals aan het begin van deze paragraaf naar voren is gebracht, zeer legitieme belangen. Dit impliceert ook dat naar de mate waarin deze belangen meer gewicht hebben, de prudentie des te groter dient te zijn bij het benutten van de ruimte die een eventuele kaderwet zou bieden om in het specifieke geval van een samenwerkingsverband gegevens te verstrekken die in andere gevallen onder de werking van een geheimhoudingsplicht (blijven) vallen.

3.6 Gegevensverstrekking aan 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 ontplooien 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

---

~~aangemerkt. Daaraan doet volgens het Hof niet af dat in dit geval ook toepassing had kunnen worden gegeven aan de regeling van artikel 126nd WSv. Zie in dit verband ook § 3.6.~~

[61] De Moor-van Vugt, a.w. blz. 33-34.

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 WSv 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 WSv om, zonder de waarborgen die het WSv 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 bewijskeer 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.[62]

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 toekomt 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.[63] 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 bij verstrekking door bestuursorganen dan ook niet nodig de verantwoordelijkheid voor het vergaren van gegevens uitsluitend neer te leggen bij de met opsporing belaste instanties.

Met opmerkingen | Mi weg.

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.[64]

---

[62] EHRM 25-2-1993, NJ 1993, 485 (Funke), EHRM 17-12-1996, NJ 1997, 699 (Saunders) en EHRM 3-5-2001, BNB 2002/26 (J.B. vs Zwitserland).

[63] Kamerstukken II, 2003-2004, 29 441, nr. 3, blz. 2.

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

Weliswaar lijkt er op grond van een arrest van het Hof Arnhem-Leeuwarden inmiddels ruimte te zijn voor verstrekking van gegevens door de Belastingdienst aan het OM zonder dat daarvoor een vordering van het OM op grond van artikel 126nd WSv nodig is[65], 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.[66] 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. Een eventuele kaderwet zou zo kunnen worden ingericht dat deze barrière verdwijnt.

Met opmerkingen : Mi weg.

3.7 Verstrekking van strafrechtelijke gegevens

In § 2.3 is naar voren gekomen dat de verwerking van bijzondere persoonsgegevens in beginsel verboden is (art. 16 Wbp). Wel bevat de Wbp een aantal uitzonderingen op dat verbod. Zo is het verbod om strafrechtelijke persoonsgegevens te verwerken, niet van toepassing, indien de verantwoordelijke heeft verkregen krachtens de Wpg of de Wjsg (art. 22, eerste lid, Wbp).

In de praktijk bestaat grote behoefte bij partijen die aan samenwerkingsverbanden deelnemen, aan betere mogelijkheden om strafrechtelijke gegevens door politie, bijzondere opsporingsdiensten en OM aan andere partijen binnen het samenwerkingsverband te laten verstrekken. Uit § 3.5 komt het beeld naar voren dat de mogelijkheden die de Wpg en de Wjsg bieden om strafrechtelijke persoonsgegevens aan samenwerkingsverbanden te verstrekken, echter niet optimaal zijn. Ook een recente wijziging van de Wet Suwi heeft daarin voor samenwerkingsverbanden op het terrein van de fraudebestrijding geen verandering gebracht.[67]

De mogelijkheden om strafrechtelijke persoonsgegevens te verstrekken, kunnen worden verbeterd door gebruik te maken van de mogelijkheid die artikel 23, eerste lid, onder f, Wbp biedt. Daarin wordt bepaald dat het in artikel 16 neergelegde verbod om bijzondere persoonsgegevens te verwerken, niet van toepassing is voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en dit bij wet wordt bepaald. Indien de wetgever van oordeel is dat gegevensuitwisseling binnen samenwerkingsverbanden voor een door de wetgever bepaald doel noodzakelijk is met het oog op een algemeen zwaarwegend algemeen belang en voor een zodanige uitwisseling in een kaderwet een uitdrukkelijke wettelijke basis creëert, behoeft bij de toepassing van de regeling niet steeds opnieuw in concreto aan de desbetreffende norm te worden getoetst.[68] Een kaderwet zou aldus voor alle samenwerkingsverbanden die onder de reikwijdte van die wet zouden vallen, de mogelijkheid tot verstrekking van strafrechtelijke persoonsgegevens creëren. Dat zou uit een oogpunt van wetgevingseconomie de voorkeur verdienen boven de mogelijkheid om de verstrekking in het Bpg en het Bjsg te regelen, nu de aard van die mogelijkheid meebrengt dat dit voor ieder samenwerkingsverband afzonderlijk dient te geschieden.

3.8 Typen van verwerking

---

gegevensverstrekking binnen een samenwerkingsverband mogelijk is zonder dat daaraan een vordering op grond van het stelsel van strafvorderlijke bevoegdheden ten grondslag ligt.

[65] Zie Hof Arnhem-Leeuwarden 8-11-2013, ECLI:NL:GHARL:2013:8478. Zie ook § 3.5.

[66] HR 27-11-2012, LJN BY0215.

[67] Zie kamerstukken II 2012-2013, 33579, nr. 3, blz. 22.

[68] Zie kamerstukken II 1997-1998, 25982, blz. 124-125.

De behoefte aan gegevensuitwisseling bestond in het verleden vooral uit informatie in een concreet geval. Deze behoefte bestaat nog steeds, maar wordt langzamerhand overvleugeld door de behoefte aan gegevens ten behoeve van grootschalige bestandsvergelijkingen voor het onderkennen van trends en patronen en het opstellen van profielen. De ontwikkeling van geavanceerde analysetechnieken onder de noemer van "big-data-analytics" is daar mede debet aan. Met het oog op deze ontwikkeling wordt in de kabinetsbrief van 20 december 2013 over de aanpak van fraude ervan uitgegaan dat de verkenning mede betrekking heeft op de mogelijkheden om op verkennende wijze fraudepatronen te onderkennen.[69]

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

De thans bestaande onduidelijkheid op dit punt belemmert de ontwikkeling en het gebruik van diensten en producten die met moderne analysemethoden geleverd kunnen worden. Dit vloeit niet alleen voort uit het veelal ontbreken van bepalingen in de huidige regelgeving die specifiek betrekking hebben op samenwerkingsverbanden[70], maar ook uit het ontbreken van bepalingen over de wijze van gegevensverwerking. Er zijn slechts enkele wettelijke bepalingen die iets zeggen over geautomatiseerde gegevensverstrekking of het geautomatiseerd zoeken in de eigen systemen op verzoek van een derde waarna de gegevens separaat (door tussenkomst van een medewerker) worden verstrekt.[71]

Een kaderwet gegevensuitwisseling zou de bestaande onduidelijkheid kunnen wegnemen door uitdrukkelijk te bepalen dat de door deze wet gereguleerde gegevensuitwisseling binnen samenwerkingsverbanden betrekking kan hebben op alle in die wet beschreven typen van verwerking. Deze typen zouden in beginsel alle typen gegevensuitwisseling moeten beslaan die in § 2.4 zijn beschreven. In § 4.6 wordt dit nader uitgewerkt.

3.9 Kwaliteit gegevens en zorgvuldigheid bij verwerking

De Wetenschappelijke Raad voor het Regeringsbeleid heeft in haar rapport iOverheid uit 2011 aangegeven dat voor het bewaken van de kwaliteit van gegevens rekening dient te worden gehouden met een drietal ontwikkelingen:

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

Deze ontwikkelingen brengen mee dat gegevens die uit bronnen met verschillende, soms zeer uiteenlopende doeleinden worden geput, eerst worden gedecontextualiseerd om vervolgens te worden gehercontextualiseerd, wanneer zij worden gecombineerd met andere gegevens in een andere beleidscontext. Daaraan kleven risico's voor de kwaliteit van de gegevens in termen van betrouwbaarheid en kenbaarheid. Dat geldt voor de professionals die met deze gegevens moeten werken (en informatie uit een andere professionele context moeten interpreteren) en wordt nog

[69] Kamerstukken II 2013-2014, 17050, nr. 450, blz. 7.
[70] Uitzonderingen zijn te vinden in artikel 22, zesde lid, Wbp, artikel 20 Wpg, artikel 28, tweede lid, onder d, Wet Bibob en artikel 64 Wet Suwi. Zie ook § 3.2.
[71] Voorbeelden hiervan zijn artikel 23 Wpg, artikel 107c Kadasterwet en artikel 28 Handelsregisterwet 2007.

versterkt wanneer het gaat om informatie die het resultaat is van technische bewerkingen, zoals "profiling" en "datamining". Aandacht voor de kwaliteit van informatie vereist ook gedegen aandacht voor technische en organisatorische randvoorwaarden zoals beveiliging, werkprocessen en een betrouwbare authenticatie- en identificatie-infrastructuur.[72]

De hier geschetste ontwikkelingen doen zich vooral ook voor bij gegevensuitwisseling in samenwerkingsverbanden. Bij een onderzoek naar gegevensuitwisseling door toezichthouders brachten experts naar voren dat onder andere politiegegevens niet altijd even hard zijn. Welke hardheidsgraad de gegevens hebben, is vaak niet bekend. De gegevens kunnen uit meerdere bronnen komen, of het relaas kan onvolledig zijn. Dat is niet goed te controleren. Databestanden kunnen daardoor "vervuild" zijn met zachte informatie. Verder blijkt uit het onderzoek het risico dat gegevens niet helemaal betrouwbaar zijn wanneer deze binnen een gegevensverzameling worden verrijkt met subjectieve informatie. Dit leidt tot kleuring van de gegevens, die in een andere context en binnen een andere gegevensverzameling verkeerd of onjuist kan worden opgevat. Omgekeerd kunnen gegevens worden gefilterd alvorens zij worden verstrekt aan een andere partij, waardoor belangrijke elementen verloren kunnen gaan.[73]

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

3.10 Verantwoordelijke

Het is uit een oogpunt van privacybescherming van belang duidelijk vast te stellen wie met betrekking tot de gegevensverwerking als verantwoordelijke in de zin van de Wbp is aan te merken. Op deze verantwoordelijke rusten immers verschillende verplichtingen, zoals de informatieplicht, 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, roept dat discussie op over de vraag wie verantwoordelijke is voor de gegevensverwerking binnen het samenwerkingsverband. In een kaderwet zou, in navolging van artikel 64, tweede lid, van de Wet Suwi, als uitgangspunt kunnen worden gekozen 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.[74] Met het oog op deze mogelijkheden zal een kaderwet ruimte dienen te bevatten om van het in die wet gekozen uitgangspunt af te wijken.

3.11 Informatieplicht

In de praktijk blijkt dat samenwerkingsverbanden vaak worstelen met de vraag of en, zo ja, in hoeverre zij moeten voldoen aan de informatieplicht van artikel 34 Wbp. 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 de betrokkenen door de verantwoordelijke worden geïnformeerd over de verwerking van hun persoonsgegevens. Deze plicht is niet van toepassing, indien de vastlegging of de verstrekking bij

[72] Wetenschappelijke Raad voor het Regeringsbeleid, iOverheid, 2011, blz. 214-217.
[73] De Moor-van Vugt, a.w., blz. 51-57 en 75.
[74] Kamerstukken II 1997-1998, 25892, nr. 3, blz. 58.

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).

De keuze voor een kaderwet zou het mogelijk maken van deze uitzondering op de informatieplicht gebruik te maken. Daarvoor zou dan wel nodig zijn dat uit die kaderwet blijkt dat, indien partijen een samenwerkingsverband oprichten, zij – uitzonderingen daargelaten – verplicht zijn de noodzakelijke gegevens aan dat samenwerkingsverband te verstrekken en, zo nodig, vast te leggen.[75] Het zou de transparantie voor de burger bevorderen, als in de kaderwet ook zou worden bepaald dat bij de oprichting van een samenwerkingsverband ervoor wordt gezorgd dat er algemene informatie wordt gegeven over de gegevensverwerking door het desbetreffende samenwerkingsverband. Deze informatie zou dan bijvoorbeeld op een website kunnen worden geplaatst.

Met opmerkingen : Wat moet hier eventueel worden vastgelegd?

Met opmerkingen : Mi sterker aanzetten als een echte waarborg!

Een dergelijke regeling in een kaderwet zou dus meebrengen dat niet iedere betrokkene afzonderlijk zou moeten worden geïnformeerd over de verwerking van gegevens over hem of haar. Dat heeft het voordeel dat alle inspanningen die hiervoor nodig zijn, achterwege kunnen blijven, zonder dat het noodzakelijk is precies na te gaan of die inspanningen zijn aan te merken als een onevenredige inspanning, die ingevolge het vierde lid van artikel 34 eveneens kan leiden tot het buiten toepassing laten van de informatieplicht. Belangrijker is dat het in samenwerkingsverbanden op het terrein van de fraudebestrijding al gauw gaat om gegevensverwerking die, als zij bij betrokkenen bekend wordt, tot calculerend gedrag bij hen kan leiden.[76]

3.12 Vertrouwen in het gebruik van gegevens door andere partijen

Bij gegevensuitwisseling in samenwerkingsverbanden geldt dat geen enkele partij graag gegevens verstrekt, als niet duidelijk is wat ermee gebeurt. Dat geldt vooral als het om gevoelige gegevens gaat. Het bestaan van onduidelijkheid op dit punt kan een belemmering vormen voor de gegevensuitwisseling. Het gaat hier vooral om de vraag of verstrekking aan derden buiten het samenwerkingsverband mogelijk moet zijn en, zo ja, onder welke voorwaarden. Als hierover onduidelijkheid bestaat, wordt mogelijk in strijd gehandeld met het zorgvuldigheidsbeginsel dat in artikel 6 Wbp is verankerd.[77]

Om voldoende vertrouwen in het gebruik van gegevens door andere partijen te kunnen hebben, wordt soms het "gazo"-principe gehanteerd: geen actie zonder overleg. Dit gebeurt bijvoorbeeld bij samenwerkingsverbanden die te maken hebben met meldingen op grond van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft), zoals het FEC. Verder is denkbaar dat expliciet wordt vastgelegd dat doorverstrekking aan een derde alleen plaatsvindt met instemming van de partner van wie de persoonsgegevens oorspronkelijk afkomstig zijn.[78] Met het oog daarop kan het zinvol zijn doorverstrekking aan derden te "loggen". In een kaderwet kunnen op dit punt bepaalde voorzieningen worden getroffen.

Ik mis hier de notie dat gegevensverstrekking in samenwerkingsverband geschiedt met het oog op het doel van het samenwerkingsverband en dus niet met het oogmerk dat de in het hiervoor genoemde kader gewisselde gegevens vervolgens door de ontvangende partijen voor eigen doeleinden worden gebruikt dan zit je veeleer in een bilaterale gegevensuitwisselingssituatie met een heel ander doel nl het doel waarvoor de ontvangende partij de gegevens nodig heeft.

Dit zou nog wel eens een cruciaal verschil kunnen zijn tussen gegevensuitwisseling in samenwerkingsverbanden en de bestaande reguliere gegevensuitwisseling. In het eerste geval

[75] Vgl. artikel 64, tweede lid, Wet Suwi.
[76] Zie ook kamerstukken II 2012-2013, 33579, nr. 3, blz. 26.
[77] Vgl. ABRvS 4 juli 2007, overweging 2.4.5, LJN: BA8742, 200608203/1.
[78] Zie de artikelen 4 en 18 Informatieprotocol FEC 2011, Stcrt. 2011, 21708.

gaat het echt om de situatie van 1 plus 1 is 3, terwijl in d etweede situatie daarvan niet sprake is maar d eontvangende partij de gegevens nodig heeft voor de uitvoering van zijn eigen taak!

Dit punt verdient nadere uitwerking want is van belang voor het denken rond en definiëren van samenwerkingsverbanden.

4. Contouren kaderwet

4.1 Inleiding

In de vorige paragraaf is aangegeven dat de daarin genoemde knelpunten kunnen worden weggenomen door een kaderwet voor de gegevensuitwisseling in samenwerkingsverbanden. In deze paragraaf worden de contouren van zo'n kaderwet geschetst. Daarvoor is mede gebruik gemaakt van elementen uit een recente wet tot wijziging van de Wet Suwi.[79] Deze wijzigingswet bevat een nieuw artikel 64 Wet Suwi, waarin een regeling voor de gegevensverstrekking ten behoeve van samenwerkingsverbanden is opgenomen.

Een belangrijk kenmerk van het nieuwe artikel 64 Wet Suwi is dat het niet geschreven is voor één specifiek samenwerkingsverband. Daarmee heeft dit artikel al enigszins het karakter van een kaderregeling. Een verschil met een kaderwet, zoals bedoeld in deze notitie, is dat de reikwijdte van artikel 64 beperkter is dan van zo'n kaderwet. Dat artikel bestrijkt maar een – overigens niet onbelangrijk - deel van de mogelijke vormen van fraude en bevat vanwege die relatief beperkte reikwijdte een aantal elementen, zoals de (gedeeltelijke) samenstelling van een samenwerkingsverband[80], die in een kaderwet uit een oogpunt van flexibiliteit geheel aan regeling bij convenant zouden moeten worden overgelaten. Een ander verschil is dat artikel 64 blijkens de toelichting uitsluit dat aan het samenwerkingsverband ook strafrechtelijke persoonsgegevens worden verstrekt.[81]

Een kaderwet (of raamwet) is een wet die de algemene principes, verantwoordelijkheden en procedures regelt, maar geen gedetailleerde regels bevat. Een belangrijke eigenschap van kaderwetten lijkt dan ook dat zij doorgaans niet zelf beleidsinhoudelijke regulatieve keuzes vastleggen, maar vooral randvoorwaarden scheppen waarbinnen bijvoorbeeld lagere regelgevers, beleidsmakers of uitvoerders dienen te opereren.[82] Een kaderwet zal in dat licht bezien niet voor ieder samenwerkingsverband in detail regelen waaraan dat samenwerkingsverband zich heeft te houden. Dat zou ook niet goed mogelijk zijn zonder te vervallen in een rigide structuur die onvoldoende ruimte voor maatwerk voor ieder afzonderlijk samenwerkingsverband biedt.[83] Wel zal een kaderwet een raamwerk bieden waarbinnen de deelnemers aan een samenwerkingsverband hun samenwerking nader uitwerken in een convenant en in een informatieprotocol, dat de nodige waarborgen voor de bescherming van persoonsgegevens bevat. Een kaderwet kan daarbij de knelpunten wegnemen die nu in de praktijk bij het opstellen van zo'n convenant en protocol worden ervaren. Een kaderwet zou echter niet alleen legitimerend en faciliterend, maar ook normerend moeten zijn.[84] Zij zou de hoofdlijnen moeten bevatten voor een aantal waarborgen voor een zorgvuldige gegevensuitwisseling, die in het convenant en het informatieprotocol van een samenwerkingsverband nader moeten worden uitgewerkt.

Gelet op het kabinetsstandpunt over het WODC-rapport "Gegevensuitwisseling door toezichthouders" zal een kaderwet ook niet het karakter kunnen krijgen van een wet waarin de huidige Wbp wordt omgevormd tot een brede kaderwet, eventueel met nadere uitwerking in

Met opmerkingen Ik vind het niet verstandig dit soort oude en verouderde standpunten opnieuw in dit rapport zo te benadrukken nu steeds duidelijker wordt dat op korte termijn de gegevensuitwisseling in Nederland binnen het overheidsdomein voor een principiële heroriëntatie staat.

[79] Wet van 9 oktober 2013 tot wijziging van de Wet structuur uitvoeringsorganisatie werk en inkomen en enige andere wetten in verband met fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekende zijnde gegevens, Stb. 2013, 405.

[80] Artikel 64, eerste lid, van de Wet Suwi noemt de colleges van burgemeester en wethouders, het UWV, de SVB, toezichthouders op het terrein van SZW, de Belastingdienst en andere bestuursorganen en personen, voor zover zij zijn belast met een publieke taak en daartoe bij regeling van de Ministers van SZW en Financiën zijn aangewezen.

[81] Kamerstukken II 2012-2013, 33579, nr. 3, blz. 22.

[82] R.A.J. van Gestel en A. Vleugel, Herijking van het primaat van de wetgever: de betekenis van de kaderwetgeving en delegatie, 2012, blz. 19.

[83] De werkgroep herijking toezichtregelgeving kwam in 2008 met betrekking tot de gegevensuitwisseling tussen toezichthouders tot dezelfde conclusie. Zie § 2.7.

[84] De Moor-van Vugt, a.w., blz. 59.

sectorale wetgeving. Het kabinet heeft in reactie op dat rapport zich immers – zie § 2.7 - op het standpunt gesteld dat een meer algemene bezinning op het huidige nationale kader beter kan wachten op de uitkomst van de herziening van de Europese regelgeving inzake de verwerking en bescherming van persoonsgegevens. Dat impliceert dat het nu niet opportuun is voor een kaderwet te pleiten waarin de Wbp opgaat. Het kabinetsstandpunt laat wel ruimte voor een meer bescheiden opzet van een kaderwet, waarbij de Wbp, de Wpg, de Wjsg en de bepalingen over gegevensverwerking in sectorale wetten, op mogelijk een enkele kleine aanpassing na, in stand blijven. Deze opzet zou niet alleen het voordeel hebben dat de voorbereiding van een dergelijke kaderwet niet of nauwelijks zou interfereren met de lopende herziening van de Europese regelgeving inzake de verwerking en bescherming van persoonsgegevens en het vervolg op de evaluatie van de Wpg en Wjsg. Zij zou ook de voorkeur verdienen, omdat bij een keuze voor een brede kaderwet waarin de Wbp opgaat, voorbij zou worden gegaan aan het feit dat de Wbp ook betekenis heeft voor al die vormen van gegevensverwerking die buiten samenwerkingsverbanden plaatsvinden. Hetzelfde geldt met betrekking tot de Wpg en Wjsg en bepalingen over gegevensverwerking in sectorale wetten, voor zover de gedachte zou bestaan deze regelgeving of delen daarvan eveneens in zo'n brede kaderwet op te nemen.

Met opmerkingen : Ik zie niet hoe het thans al onduidelijke veld rond gegevensverwerking gediend wordt met een nieuw onderscheid bij gegevensverwerking, namelijk of dit al dan niet plaatsvindt in samenwerkingsverband, integendeel!

Tot slot valt erop te wijzen dat een kaderwet voor gegevensuitwisseling een algemene aanvulling zou vormen op wettelijke regelingen die in specifieke gevallen samenwerking voorschrijven en daarbij regels over gegevensuitwisseling geven, zoals de in artikel 9 van de Wet Suwi voorgeschreven samenwerking tussen het UWV, de SVB en de gemeenten bij de uitvoering van die wet en enige andere wetten. Deze aanvulling impliceert niet dat ook de kaderwet samenwerking tussen overheidsorganisaties voorschrijft. Dat zou, gelet op de vele, soms zeer uiteenlopende belangen van deze organisaties, niet kunnen. De aanvullende betekenis van een kaderwet zal wel zijn gelegen in het feit dat, àls partijen tot samenwerking besluiten, de kaderwet de uitwisseling van gegevens in zo'n samenwerkingsverband legitimeert, faciliteert en normeert.

Met opmerkingen ?

Met opmerkingen Dit is in feite de enige positieve bijdrage die de kaderwet biedt, echter dit is theoretisch want het positieve effect van het creëren van een juridische grondslag voor gegevensverstrekking (ikv samenwerkingsverbanden, vallend onder de kaderwet) wordt teniet gedaan door alle vragen die deze kaderwet oproept en de nieuwe onduidelijkheden die het schept.

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

4.2 Reikwijdte kaderwet

In de brief van het kabinet van 20 december 2013 over de aanpak van fraude wordt de verkenning naar een kaderwet toegespitst op fraudebestrijding. De aard van de kabinetsbrief brengt dat begrijpelijkerwijs mee. De vraag rijst evenwel of een kaderwet gegevensuitwisseling in samenwerkingsverbanden zich tot dat domein zou moeten beperken.

Zoals in § 2.2 al naar voren is gekomen, houdt van de samenwerkingsverbanden die zich met fraudebestrijding bezighouden, in feite een minderheid zich uitsluitend met fraudebestrijding bezig. De meeste samenwerkingsverbanden hebben een taak die zich in meerdere of mindere mate ook tot andere terreinen uitstrekt. Een kaderwet die zich beperkt tot gegevensuitwisseling ten behoeve van de fraudebestrijding zou tot gevolg hebben dat samenwerkingsverbanden ten dele wel en ten dele niet onder de werking van de kaderwet vallen. Dat zou voor die samenwerkingsverbanden een onwerkbare situatie opleveren. Het zou al lastig zijn, als gegevens in een exclusieve één-op-één-relatie tot een bepaald doel zouden staan. Gegevens die samenwerkingsverbanden verwerken, kunnen echter meerdere doelen tegelijk dienen. Zo kunnen de RIEC's bepaalde persoonsgegevens verwerken met het oog op tegelijkertijd georganiseerde hennepteelt èn fraude in de vastgoedsector. Het is dan niet doenlijk deze verwerking te laten plaatsvinden onder de gelijktijdige werking van de kaderwet en van daarvan afwijkende bepalingen in andere wetgeving.

Met opmerkingen Erg moeilijk te duiden zin!

Los van deze overweging kan worden vastgesteld dat een kaderwet voor veel meer samenwerkingsverbanden in de publieke sfeer betekenis kan hebben dan alleen de verbanden die (mede) op het terrein van de fraudebestrijding bezig zijn. 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. Dat pleit voor een kaderwet die een breder domein dan fraudebestrijding bestrijkt. Het ligt dan in zekere zin voor de hand te kiezen voor een kaderwet op het brede terrein van de uitoefening van toezicht op de naleving van wettelijke voorschriften en de handhaving van de openbare orde en veiligheid ("bestuursrechtelijke

Met opmerkingen :

handhaving") en de voorkoming, opsporing en vervolging van strafbare feiten ("strafrechtelijke handhaving"). Het is immers dit brede terrein waarop zich allerlei samenwerkingsverbanden manifesteren die gegevens tussen het bestuursrechtelijke en strafrechtelijke domein willen uitwisselen.

Met opmerkingen [ ]: Zelfde argumentatie geldt dus tav de behoefte aan gegevens van andere bestuursorganen in de voorfase van bestuurlijke beschikkingen.

Erkend zij dat ook een kaderwet op dit bredere terrein het probleem kan oproepen van de toepasbaarheid op samenwerkingsverbanden die op zowel het terrein van de kaderwet als daarbuiten opereren. Naarmate het terrein dat de kaderwet beslaat, groter is, zal dit probleem zich naar verwachting evenwel minder snel 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.[85]

Een andere vraag die de reikwijdte van een eventuele kaderwet bepaalt, is de vraag of deze wet alleen voor samenwerkingsverbanden zou moeten gelden die op nationaal niveau 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 beperking tot samenwerkingsverbanden op nationaal niveau niet voor de hand. Juist op lokaal en regionaal niveau bestaan samenwerkingsverbanden die maatwerk vergen, waarvoor een kaderwet een legitimerende, faciliterende en normerende functie kan uitoefenen.

Voor de reikwijdte van een kaderwet is tot slot van belang of aan samenwerkingsverbanden die onder de kaderwet vallen, ook private partijen mogen deelnemen. Om de redenen die in § 2.2 zijn genoemd, valt daar veel voor te zeggen. Omdat het delen van informatie tussen publieke en private partijen gevoelig ligt, is het wenselijk dat de kaderwet voldoende waarborgen bevat dat de gegevensuitwisseling een te rechtvaardigen doel dient. De belangrijkste waarborg is dat dit doel een publiek belang dient te zijn; verstrekking van gegevens aan private partijen met het oog op bijvoorbeeld commerciële belangen van die partijen is ongewenst. Met een kaderwet die betrekking heeft op gegevensuitwisseling met als doel de bestuursrechtelijke en strafrechtelijke handhaving te bevorderen, is dat publieke belang verzekerd. Een andere waarborg is dat de kaderwet voorschrijft dat private partijen alleen dan aan een samenwerkingsverband onder de reikwijdte van deze wet kunnen deelnemen, indien zij voorkomen op een lijst die bij ministeriële regeling is vastgesteld. Daarmee dragen ook de ministers op wier beleidsterrein het desbetreffende samenwerkingsverband functioneert, verantwoordelijkheid voor de samenstelling van het verband en kunnen zij daarop door het parlement worden aangesproken. Dit kan vooral van belang zijn bij regionale of lokale samenwerkingsverbanden waarvoor de ministeriële verantwoordelijkheid, afhankelijk van de deelnemers van overheidszijde, niet of slechts in beperkte mate aanwezig zou zijn.

Met opmerkingen [ ]: Een lijst per minister?

Met opmerkingen [ ]: Dit wordt toch wel een erg lastige want de minister heeft geen enkel zicht op noch verantwoordelijkheid voor wat private partijen met decentrale overheden aan gegevens uitwisselen en dit moet mi ook niet het geval zijn.

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

4.3 Regeling doel samenwerkingsverband

Een kaderwet gegevensuitwisseling in samenwerkingsverbanden zou in de eerste plaats moeten bepalen dat bestuursorganen en private partijen aan een samenwerkingsverband kunnen deelnemen ten behoeve van een integraal optreden met betrekking tot de uitoefening van toezicht op de naleving van wettelijke voorschriften, de handhaving van de openbare orde en veiligheid en de voorkoming, opsporing en vervolging van strafbare feiten. Hiermee zou een kaderwet het

Met opmerkingen [ ]: Dit klinkt goed maar geeft geen duiding wat in feite gebeurt c.q. de bedoeling is.

[85] Zie voor het doel en de opzet van veiligheidshuizen: http://veiligheidshuizen.nl/achtergrond.

bredere doel omschrijven waarbinnen samenwerkingsverbanden voor een meer specifiek doel kunnen worden aangegaan.

De kaderwet zou vervolgens moeten bepalen dat de deelnemers aan het samenwerkingsverband in een convenant nauwkeurig het specifieke doel van de samenwerking en de daarvoor noodzakelijke gegevensuitwisseling vastleggen. Dit doel moet passen binnen de reikwijdte van de bredere wettelijke doelomschrijving. Als aan die voorwaarde is voldaan, is het niet meer nodig om nog apart te toetsen of het doel van de gegevensuitwisseling verenigbaar is met het doel waarvoor de gegevens oorspronkelijk door de verstrekkende partij zijn verkregen. Anders gezegd: de verenigbaarheidstoets van artikel 9 Wbp (zie § 3.4) kan achterwege blijven. Met de bredere doelomschrijving in de kaderwet en de concretisering daarvan in het convenant ontstaat een getrapte vorm van doelbinding: de gegevensuitwisseling in een samenwerkingsverband moet vallen binnen zowel de bredere doelomschrijving van de kaderwet als het meer gespecificeerde doel dat in het convenant is vastgelegd. Daarmee wordt in voldoende mate voldaan aan het principe van doelbinding.[86]

Met opmerkingen Dit is dus een belangrijk punt waarop de kaderwet het doel mist; die verenigbaarheidstoets is niet afgedekt met de ruime doelstellingen van de kaderwet.

4.4 Verplichte uitwisseling van gegevens

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

Met opmerkingen Welk vereiste is dit en is dit hetzelfde begrip noodzakelijk als in de vorige zin?

De verplichting tot gegevensverstrekking in een kaderwet voor specifieke samenwerkingsverbanden zou als een "lex specialis" kunnen worden gezien ten opzichte van de generieke geheimhoudingsbepalingen in sectorwetten en zou aldus voorrang hebben boven die bepalingen. Om op dit punt echter geen misverstand te laten ontstaan verdient het de voorkeur in de kaderwet uitdrukkelijk te bepalen dat geheimhoudingsbepalingen in andere wetten buiten toepassing blijven. Daarmee kan een kaderwet knelpunten als omschreven in § 3.5 wegnemen.

Met opmerkingen Dit gaat veel te ver tav de strenge fiscale geheimhoudingsbepaling temeer waar de doeleinde zeer ruim en vaag zijn omschreven. Tevens is de vraag hoe de kaderwet zich verhoudt tot bestaande bilaterale gegevensuitwisselingsbepalingen die veelal veel specifieker zijn geformuleerd dan de doeleinden van de kaderwet. Dus het lex specialisverhaal ligt eerder omgekeerd!

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

Onder de verplichting tot gegevensverstrekking zou ook de verstrekking aan politie, andere opsporingsdiensten en OM vallen. In § 3.6 is in dit verband bepleit dat gegevens in samenwerkingsverbanden voortaan aan de politie, andere opsporingsdiensten of het OM kunnen worden verstrekt, zonder dat daarvoor een vordering als bedoeld in artikel 126nc of 126nd WSv nodig is. Daartoe zou de kaderwet moeten bepalen dat voor de verstrekking in een samenwerkingsverband van gegevens aan de politie, andere opsporingsdiensten of het OM deze artikelen niet van toepassing zijn. 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 hiervóór beschreven mogelijkheid in het convenant vast te leggen dat het van verstrekking kan afzien. In

Met opmerkingen

[86] Met de voorgestelde getrapte vorm van doelbinding wordt het bezwaar weggenomen dat de werkgroep herijking toezichtregelgeving destijds had tegen een wettelijke regeling met een algemeen geldende doelomschrijving (zie § 2.7). Een getrapte vorm van doelbinding ligt ook opgesloten in artikel 64 Wet Suwi (kamerstukken II 2012-2013, 33579, nr. 3, blz. 36).

dat geval zal de politie, de opsporingsdienst of het OM buiten het samenwerkingsverband, zo nodig, alsnog een vordering op grond van artikel 126nc, respectievelijk 126nd kunnen instellen.

Met opmerkingen Deze passage miskent de mogelijkheid van gegevensverstrekking aan politie/OM alleen ikv de doeleinden van het samenwerkingsverband en niet tbv verder gebruik door politie/OM waarvoor de vordering geldt.

4.5 Specifieke vastlegging van soorten gegevens

Uit een oogpunt van transparantie zou het wenselijk kunnen zijn in de kaderwet of een daaronder vallende AMvB aan te geven welke soorten van gegevens door de samenwerkingsverbanden kunnen worden gewisseld. Daarbij zou het de voorkeur verdienen dat bij AMvB te doen teneinde voldoende flexibel te kunnen inspelen op een eventueele behoefte de lijst van soorten gegevens aan te passen.

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

a. arbeidsgegevens, zijnde gegevens waarmee een door een persoon verrichte werkzaamheden vastgesteld kunnen worden;
b. gegevens inzake bestuursrechtelijke maatregelen en sancties, zijnde gegevens waaruit blijkt dat een natuurlijke persoon of een rechtspersoon een bestuursrechtelijke boete opgelegd heeft gekregen dan wel dat een andere bestuursrechtelijke maatregel is getroffen;
c. strafrechtelijke gegevens, zijnde gegevens als bedoeld in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens;
d. fiscale gegevens, zijnde gegevens waarmee de fiscale verplichtingen van een natuurlijk persoon of rechtspersoon kunnen worden vastgesteld;
e. gegevens roerende en onroerende goederen, zijnde gegevens waarmee het bezit en het gebruik van bepaalde goederen door een natuurlijk persoon of rechtspersoon kunnen worden vastgesteld;
f. gegevens over uitsluitingsgronden van bijstand of uitkeringen, zijnde gegevens waaruit blijkt dat een persoon niet in aanmerking komt voor een uitkering;
g. handelsgegevens, zijnde gegevens waarmee de aard en werkzaamheden van een rechtspersoon kunnen worden vastgesteld;
h. huisvestingsgegevens, zijnde gegevens waarmee de (daadwerkelijke) verblijfs- of vestigingsplaats van een natuurlijk persoon of rechtspersoon kunnen worden vastgesteld;
i. identificerende gegevens, zijnde bij een natuurlijk persoon: naam, adres, woonplaats, postadres, geboortedatum, geslacht en administratieve kenmerken en bij een rechtspersoon: naam, adres, postadres, rechtsvorm, vestigingsplaats en administratieve kenmerken;
j. inburgeringsgegevens, zijnde gegevens waarmee kan worden vastgesteld of aan een persoon inburgeringsverplichtingen zijn opgelegd;
k. nalevingsgegevens, zijnde gegevens waarmee de nalevingshistorie van wet- en regelgeving van een natuurlijk persoon of rechtspersoon kan worden vastgelegd;
l. onderwijsgegevens, zijnde gegevens waarmee de financiële ondersteuning ten behoeve van de bekostiging van onderwijs kan worden vastgesteld;
m. pensioengegevens, zijnde gegevens waarmee de pensioenrechten kunnen worden vastgesteld;
n. re-integratiegegevens, zijnde uitsluitend de gegevens waarmee kan worden vastgesteld of aan een persoon re-integratieverplichtingen zijn opgelegd en of deze worden nageleefd;
o. schuldenlastgegevens, zijnde gegevens waarmee de eventuele schulden van een natuurlijk persoon of rechtspersoon kunnen worden vastgesteld;
p. uitkerings-, toeslagen- en subsidiegegevens, zijnde gegevens waarmee de financiële ondersteuning van een natuurlijk persoon of rechtspersoon kan worden vastgesteld;
q. vergunningen en ontheffingen, zijnde gegevens waarmee kan worden bepaald voor welke activiteiten een natuurlijk persoon of rechtspersoon toestemming heeft gevraagd of verkregen;
r. zorgverzekeringsgegevens, zijnde uitsluitend de gegevens waarmee kan worden vastgesteld of een persoon is verzekerd voor de Zorgverzekeringswet.

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

Met opmerkingen De combinatie van deze ruime opsomming van uit te wisselen gegevens en de ruime doelstellingen (plus het laten vervallen van de verenigbaarheidstoets) betekenen de facto dat binnen het overheidsdomein praktisch alles kan worden gewisseld; dan kan je beter de Koninklijke weg bewandelen en dit ook in de wet opnemen want dan kan je eea goed regelen en ben je transparant.

De lijst is voor het overgrote deel ontleend aan artikel 5a.1, derde lid, Besluit Suwi. De opsomming in die bepaling dekt al nagenoeg volledig de soorten van gegevens die relevant kunnen zijn voor uitwisseling in samenwerkingsverbanden. Toegevoegd zijn de strafrechtelijke gegevens (onderdeel c). Deze toevoeging houdt verband met het pleidooi in § 3.7 om in de kaderwet voor alle samenwerkingsverbanden die onder de reikwijdte van die wet zouden vallen, de mogelijkheid tot verstrekking van strafrechtelijke persoonsgegevens te creëren, zodat het niet langer noodzakelijk is dat voor ieder samenwerkingsverband afzonderlijk in het Bpg en het Bjsg te regelen. Deze mogelijkheid zou kunnen worden gerealiseerd door gebruik te maken van de ruimte die artikel 23, eerste lid, onder f, Wbp biedt. Daartoe zou in de kaderwet uitdrukkelijk moeten worden bepaald dat de verplichting tot gegevensverstrekking mede betrekking heeft op strafrechtelijke persoonsgegevens als bedoeld in artikel 16 Wbp. De toepasselijkheid van deze verplichting op strafrechtelijke persoonsgegevens is overigens niet absoluut: partijen kunnen juist met het oog op bij hen beschikbare strafrechtelijke persoonsgegevens desgewenst gebruik maken van de uitzonderingsmogelijkheid die in § 4.4 is beschreven.

4.6 Legitimatie typen van gegevensverwerking

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

1. het opstellen van rapporten waarin inzichten worden geboden of trends worden gesignaleerd die voor het bereiken van het doel van het samenwerkingsverband relevant zijn,
2. het opstellen van adviezen over acties om het doel van het samenwerkingsverband te bereiken, en het uitvoeren daarvan,
3. het uitvoeren van analyses om de hiervóór bedoelde rapporten en adviezen te kunnen opstellen,
4. het opstellen van profielen van groepen van personen, organisatie of bedrijven die met het oog op het doel van het samenwerkingsverband een verhoogd risico laten zien,
5. het koppelen van deze profielen aan gegevens waarover het samenwerkingsverband rechtmatig de beschikking heeft, 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,
6. het signaleren van patronen en het opstellen van risico-indicatoren voor het uitvoeren van analyses en het opstellen van profielen, of
7. het delen van informatie, inzicht en kennis in andere dan de hiervóór bedoelde vormen, voor zover dat voor het bereiken van het doel van het samenwerkingsverband relevant is.

De kaderwet zou tevens moeten bepalen dat samenwerkingsverbanden ten behoeve van het signaleren van patronen en het opstellen van risico-indicatoren bestanden kunnen koppelen die zijn geselecteerd op basis van veronderstelde relevantie voor het signaleren van deze patronen of het opstellen van deze indicatoren. Aldus zou de kaderwet ook op dit punt de bestaande twijfel met betrekking tot de toelaatbaarheid van bepaalde typen van gegevensverwerking kunnen wegnemen.

Met opmerkingen [ ] Ligt het niet voor de hand dat de kaderwet aparte regels bevat voor de verschillende typen bewerkingen?

4.7 Zorgvuldigheid bij verwerking

Wil een kaderwet gegevensuitwisseling een integrale verbetering van de gegevensuitwisseling in samenwerkingsverbanden opleveren, dan zal deze kaderwet op grond van de overwegingen in § 2.5, 3.9 en 3.12 niet alleen een verbetering van de mogelijkheden van gegevensuitwisseling moeten bieden, maar ook voorzieningen moeten bevatten die bijdragen aan de kwaliteit van de gegevens en de zorgvuldigheid bij de verwerking daarvan.

Met opmerkingen [ ] De uitwerking van dit begrip in deze paragraaf verwoordt hoegenaamd niet het gedachtegoed van het FIN memo ter zake.

Met opmerkingen [ ] Dit is een ander begrip integraal dan in de formulering integraal optreden?

Met het oog daarop is het wenselijk in de kaderwet de volgende voorzieningen te treffen, die deels al eerder aan de orde zijn gekomen:

a. De gegevensuitwisseling moet betrekking hebben op gegevens waarvan kan worden aangetoond dat de uitwisseling noodzakelijk is voor het doel van het samenwerkingsverband.
b. Een mogelijke aantasting van de belangen van de natuurlijke personen of rechtspersonen op wie de uitwisseling van gegevens betrekking heeft, mag niet onevenredig zijn in verhouding tot het doel dat met de uitwisseling wordt beoogd.
c. Het doel dat met de uitwisseling wordt beoogd, kan in redelijkheid niet op minder ingrijpende wijze voor de betrokken personen of rechtspersonen worden bereikt.
d. Gelet op de vereisten a tot en met c, vindt de verwerking van gegevens zoveel mogelijk versleuteld plaats, waarbij een afweging wordt gemaakt met de inspanningen die de versleuteling vergt, en de invloed van de versleuteling op de effectiviteit van de gegevensuitwisseling.
e. De onderbouwing van de wijze waarop bij een eventuele koppeling van bestanden de selectie van deze bestanden plaatsvindt, en de eventueel gehanteerde risico-indicatoren zijn openbaar gemaakt op een voor het publiek toegankelijke wijze.
f. Bij de verstrekking van gegevens aan andere deelnemers wordt, waar nodig en mogelijk, aangegeven wat de graad van juistheid en betrouwbaarheid van de gegevens is, en of de gegevens zijn gebaseerd op feiten dan wel een persoonlijk oordeel.[87]
g. Voordat de deelnemers aan het samenwerkingsverband tot verwerking van persoonsgegevens overgaan, voeren zij een zgn. "Privacy Impact Assessment" (PIA) uit.
h. De deelnemers voeren, behoudens spoedeisende gevallen, acties op grond van de uitgewisselde gegevens slechts uit na overleg met de deelnemers van wie de gegevens afkomstig zijn.
i. De deelnemers aan het samenwerkingsverband stellen een informatieprotocol vast waarin in ieder geval de in § 4.10 genoemde onderwerpen zijn geregeld.

De eisen onder a, b en c vloeien, voor zover zij op persoonsgegevens betrekking hebben voort uit artikel 8 EVRM. Daarin liggen het vereiste van noodzakelijkheid en de daaruit voortvloeiende beginselen van proportionaliteit en subsidiariteit verankerd. Hoewel deze eisen al rechtstreekse gelding op basis van het EVRM hebben, lijkt het wenselijk deze in de kaderwet te expliciteren. Hiermee wordt benadrukt dat ook het gebruik van de ruimere mogelijkheden van gegevensverwerking die de kaderwet biedt, moet worden getoetst aan deze eisen.[88]

De eis onder d ziet op de toepassing van vormen van anonimisering en pseudonimisering. Waar dat met een redelijke inspanning mogelijk is, dienen dergelijke vormen conform het principe van "Privacy by Design" te worden ingepast in het proces van gegevensverwerking. Een goed voorbeeld hiervan is de pseudonimisering die in het proces van gegevensverwerking met behulp van SyRI plaatsvindt. Dit proces houdt in dat aan de hand van gepseudonimiseerde gegevens en met behulp van vooraf bepaalde risico-indicatoren potentiële treffers worden bepaald ten aanzien van (gepseudonimiseerde) personen die een verhoogd risico laten zien dat zij fraude plegen. De potentiële treffers worden vervolgens ontsleuteld voor een nader analyse op naam.[89]

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

Met opmerkingen | Zijn die er dan?

Bij gegevensuitwisseling in samenwerkingsverbanden is het bij uitstek van belang dat de context waarbinnen een gegeven is verzameld of ontstaan, zo nodig en mogelijk wordt meegegeven aan

[87] Deze waarborg is ook terug te vinden in artikel 6 van het voorstel voor een Europese Richtlijn gegevensbescherming opsporing en vervolging van 25 januari 2012, COM(2012)10.
[88] De kaderwet volgt in dit opzicht dezelfde lijn als onlangs in het nieuwe artikel 5a.1, vierde lid, Besluit Suwi is neergelegd.
[89] Vgl. kamerstukken 2012-2013, 33579, nr. 3, blz. 3 e.v. Zie ook artikel 5a.2 Besluit SUWI.

de andere deelnemers aan het samenwerkingsverband. Met het oog daarop is de onder f beschreven eis opgenomen.[90]

Met het onder g bedoelde "Privacy Impact Assessment" (PIA) kan op gestructureerde en transparante wijze zichtbaar worden gemaakt wat de eventuele effecten van de gegevensuitwisseling voor de bescherming van persoonsgegevens zijn. Tijdens het proces waarin de PIA wordt uitgevoerd, kunnen bepaalde elementen van de gegevensuitwisseling zo nodig worden heroverwogen om tot een betere bescherming van persoonsgegevens te komen. De eis van een PIA vloeit voort uit het regeerakkoord.[91] Voor het uitvoeren van een PIA op rijksniveau heeft het kabinet een toetsmodel vastgesteld, dat sinds 1 september 2013 verplicht moet worden toegepast.[92]

Onder h is het "gazo"-principe vastgelegd. Opneming van dit principe moet – zie § 3.12 - bijdragen aan het vertrouwen dat deelnemers hebben in het gebruik van hun gegevens door andere deelnemers. Bij acties waaraan voorafgaand overleg moet plaatsvinden, kan worden gedacht aan bijvoorbeeld het intrekken van een vergunning. Als het voorgenomen intrekken daarvan mede op gegevens van de politie wordt gebaseerd, kan overleg met de politie aanleiding zijn om bijvoorbeeld de intrekking uit te stellen, omdat dit in verband met een lopend politieonderzoek de voorkeur verdient.

4.8 Verantwoordelijke

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

Met opmerkingen Er wordt ook wel gesproken over gedeelde verantwoordelijkheid, is dit wat anders?

De gezamenlijke verantwoordelijkheid geldt uitsluitend voor de verwerking van gegevens binnen het samenwerkingsverband. De deelnemers zijn en blijven ieder voor zich verantwoordelijke in de zin van de Wbp voor het verstrekken van gegevens aan het samenwerkingsverband.

Het uitgangspunt dat partners gezamenlijk verantwoordelijke zijn, kan 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.[93] Het gaat hier om een louter ondersteunende rol; zij neemt de gezamenlijke verantwoordelijkheid van de partners niet weg. In een eventuele kaderwet behoeft zij dan ook geen expliciete regeling.

4.9 Informatieplicht

In § 4.4 is aangegeven dat in de kaderwet wordt bepaald dat de deelnemers aan een samenwerkingsverband verplicht zijn de noodzakelijke gegevens aan dat samenwerkingsverband te verstrekken. Zoals in § 3.11 al is beschreven, maakt een dergelijke bepaling het mogelijk dat niet iedere betrokkene afzonderlijk zou moeten worden geïnformeerd over de verwerking van gegevens over hem of haar. Op basis van de kaderwet en het op grond van die wet verplichte

[90] Zie ook § 3.9, alsmede De Moor-van Vugt, a.w., blz. 75.
[91] Regeerakkoord VVD-PvdA van 29 oktober 2012, "Bruggen slaan", blz. 28.
[92] Kamerstukken II 2012-2013, 26643, nr. 282 herdruk.
[93] Vgl. de regisseur die in artikel 10 Informatieprotocol FEC 2011 is aangewezen.

convenant en informatieprotocol (zie nader § 4.10) is in algemene zin al genoegzaam af te leiden welke gegevens ten behoeve van welk doel worden verwerkt. De kaderwet dient in verband daarmee voor te schrijven dat convenant en informatieprotocol worden gepubliceerd. De kenbaarheid van de gegevensverwerking kan verder worden vergroot via de gebruikelijke voorlichtingsactiviteiten op websites en door middel van brochures.

Met opmerkingen : Hoe/waar?

4.10 Informatieprotocol

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

De kaderwet zal moeten bepalen welke elementen dit informatieprotocol in ieder geval dient te bevatten. Daarbij kan worden gedacht aan de volgende elementen:
a. een beschrijving van de (soorten van) gegevens die worden uitgewisseld;
b. een verantwoording van de wijze waarop aan de eisen a tot en met g uit § 4.7 uitvoering is c.q. zal worden gegeven;
c. de inrichting van het proces van gegevensuitwisseling en de waarborgen die hierin zijn opgenomen met het oog op de bescherming van persoonsgegevens;
d. uitzonderingen op de verplichting tot gegevensuitwisseling (zie § 4.4);
e. de beveiliging van de gegevens (art. 13 Wbp);
f. geheimhouding (art. 12 Wbp),
g. informatieverstrekking over de gegevensuitwisseling aan het publiek en aan betrokkenen;
h. de rechten van betrokkenen: inzage, correctie, verzet (artt. 35, 36, 40 Wbp);
i. verstrekking aan derden;
j. bewaartermijnen (art. 13 Wbp);
k. de verwijdering en vernietiging van bewaarde gegevens.

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

Bij de inrichting van het proces van gegevensuitwisseling gaat het om een beschrijving van het proces van gegevensverwerking en van het eventuele gebruik van een informatiesysteem 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 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. Informatieverstrekking aan betrokkenen doelt op uitvoering van de verplichting 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).

Voor de beveiliging van gegevens is het wenselijk in het informatieprotocol de richtsnoeren die het Cbp daartoe heeft opgesteld, als uitgangspunt te nemen.[94]

[94] Zie Stcrt. 2013, 5174.

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

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

4.11 Toezicht

Het College bescherming persoonsgegevens (Cbp) houdt ingevolge artikel 51 Wbp toezicht op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde. Deze taak is niet beperkt tot het terrein van de Wbp, maar strekt zich ook uit tot andere wetten, AMvB's en andere wettelijke regelingen op grond waarvan persoonsgegevens worden verwerkt. Dat geldt dus ook voor wetten waarin in aanvulling op de Wbp nadere regels zijn gesteld.[95] Dit impliceert dat de verwerking van persoonsgegevens onder de werking van een kaderwet voor gegevensuitwisseling in samenwerkingsverbanden onder toezicht van het Cbp plaatsvindt.

4.12 Toetsing aan het EVRM

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

Het toezicht op de naleving van wettelijke voorschriften draagt, afhankelijk van de inhoud van deze voorschriften, bij aan het economisch welzijn van ons land, de bescherming van de gezondheid of de goede zeden en aan de bescherming van de rechten en vrijheden van burgers. De handhaving van de openbare orde en veiligheid dient de openbare veiligheid en het voorkomen van wanordelijkheden. De voorkoming, opsporing en vervolging van strafbare feiten staat in het teken van het voorkomen van strafbare feiten. Daarmee worden alle doeleinden waarbinnen het meer specifieke doel van een samenwerkingsverband moet vallen, afgedekt door de doeleinden die artikel 8 EVRM noemt.

De eis uit artikel 8 EVRM dat de inmenging in de uitoefening van het recht op respect voor het privéleven bij wet moet zijn voorzien, houdt in dat er sprake is van een wettelijke basis die voor de burger voldoende toegankelijk en voorzienbaar is.[96] Aan deze eis wordt voldaan met de in deze paragraaf beschreven kaderwet en de daarop berustende bepalingen in een AMvB en ministeriële regeling, die gepubliceerd worden in het Staatsblad, respectievelijk de Staatscourant. Aan de toegankelijkheid draagt bij wat uit de parlementaire stukken over een kaderwet als toelichting op deze wet kan worden afgeleid. De voorzienbaarheid neemt verder toe door de in de kaderwet opgenomen verplichtingen om bepaalde onderwerpen in het convenant en het informatieprotocol nader te regelen en deze te publiceren in de Staatscourant en overigens op een voor het publiek toegankelijke wijze openbaar te maken.

De eis dat de inmenging noodzakelijk is in een democratische samenleving, wordt in de jurisprudentie van het EVRM nader ingevuld met het vereiste van een dringende maatschappelijke behoefte ("pressing social need"). Of hiervan sprake is, wordt bepaald aan de hand van een aantal criteria. Zo moet een maatregel om noodzakelijk te zijn, relevant zijn om het beoogde doel te

[95] Kamerstukken II 1997-1998, 25892, nr. 3, blz. 177.
[96] EHRM 26 april 1979 (Sunday Times), NJ 1980, 146.

bereiken en verder moet voldaan zijn aan het proportionaliteits- en het subsidiariteitsvereiste. In algemene zin kan worden gesteld dat samenwerkingsverbanden op de terreinen die de kaderwet beslaat, effectiever en efficiënter kunnen opereren, als zij gegevens kunnen uitwisselen. Sterker nog, de primaire aanleiding om een samenwerkingsverband aan te gaan, is veelal gelegen in de behoefte aan gegevensuitwisseling. Of de gegevensverwerking in een samenwerkingsverband ook in een concreet geval aan de hier genoemde vereisten voldoet, zal moeten worden getoetst bij de oprichting van het samenwerkingsverband en de inrichting van het proces van gegevensverwerking. De kaderwet zal expliciet voorzien in de verplichting de gegevensverwerking te toetsen aan het noodzakelijkheidsvereiste en de daaruit voortvloeiende beginselen van proportionaliteit en subsidiariteit.

4.13 Toetsing aan regelgeving van de EU

Een kaderwet die een opzet kent als in de voorgaande paragrafen beschreven, past binnen de voorschriften van de Europese privacyrichtlijn. De in de kaderwet geregelde verwerking van persoonsgegevens kan worden gebaseerd op twee gronden uit deze richtlijn.

De eerste grond is te vinden in artikel 7, onder d, van de richtlijn. Daarin is bepaald dat lidstaten de verwerking van persoonsgegevens mogen toestaan, indien deze verwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de voor de verwerking verantwoordelijke is onderworpen. Deze bepaling is terug te vinden in artikel 8, onder c, Wbp. Nu in § 4.4 wordt voorgesteld in de kaderwet voor te schrijven dat deelnemers aan een samenwerkingsverband verplicht zijn de voor het samenwerkingsverband noodzakelijke gegevens te verstrekken, wordt aan deze voorwaarde voldaan. Daarmee zal ook worden voldaan aan artikel 6, eerste lid, onder c, en derde lid, van het voorstel voor een Algemene verordening gegevensbescherming[97], waarin deze voorwaarde terugkomt. Weliswaar is de activering van deze verplichting afhankelijk van een besluit van de deelnemer om aan het desbetreffende samenwerkingsverband deel te nemen, maar dat doet niet af aan het verplichte karakter van de gegevensverstrekking op zich.

Met opmerkingen [ ] Dit slaat primair op de wettelijke taken van individuele bestuursorganen; bij samenwerkingsverbanden lijkt sprake te zijn van een boven die individuele taken uitgaand publiek belang.

De tweede grond is gelegen in artikel 7, onder e, van de richtlijn. Ingevolge dat onderdeel mogen lidstaten de verwerking van persoonsgegevens toestaan, indien de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang. Met de combinatie van het doel van de gegevensuitwisseling en het noodzakelijkheidsvereiste, zoals in § 4.2, respectievelijk § 4.7 zijn beschreven, wordt aan deze voorwaarde voldaan. Daarmee zal ook worden voldaan aan artikel 6, eerste lid, onder e, en derde lid, van het voorstel voor een Algemene verordening gegevensbescherming, waarin deze voorwaarde terugkomt. De desbetreffende voorwaarde is destijds geïmplementeerd in artikel 8, onder e, Wbp. In dat onderdeel heeft een precisering plaatsgevonden tot gegevensverwerking die noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt. Daarmee valt gegevensverwerking die noodzakelijk is voor de vervulling van een taak van algemeen belang in de vorm van gegevensuitwisseling met private partijen, buiten dat onderdeel. Een kaderwet zal in zoverre een aanvulling op dat onderdeel geven dat zij – binnen de voorwaarde uit de Europese privacyrichtlijn - ook een wijze van gegevensuitwisseling met private partijen mogelijk maakt die – zie § 3.3 - de Wbp nu niet toelaat.

Met opmerkingen [ ] Ook deze Wbp bepaling lijkt dus te kort te schieten bij samenwerkingsverbanden waarbij het gaat om belangen die de individuele belangen van betrokken partijen te boven gaan.

De verstrekking van strafrechtelijke persoonsgegevens door politie en OM aan een samenwerkingsverband valt in de toekomst onder de nieuwe Richtlijn gegevensbescherming opsporing en vervolging. Ingevolge artikel 7, aanhef en onder a, van het voorstel voor deze richtlijn[98] dienen lidstaten te bepalen dat het verwerken van strafrechtelijke persoonsgegevens die onder de werking van deze richtlijn vallen, slechts rechtmatig is wanneer en voor zover die verwerking noodzakelijk is voor – onder meer – het uitvoeren van een taak door een bevoegde autoriteit, op grond van een wettelijke bepaling, voor de voorkoming, het onderzoek, de opsporing

[97] Zie de tekst van 25 januari 2012, COM(2012)11.
[98] Zie de tekst van 25 januari 2012, COM(2012)10.

en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen. Deze bepaling geeft voldoende ruimte om door middel van de kaderwet verstrekking van strafrechtelijke persoonsgegevens door politie en OM aan een samenwerkingsverband mogelijk te maken, voor zover het om het voorkomen, opsporen en vervolgen van strafbare feiten gaat. Voor zover het om de overige doeleinden van de kaderwet gaat, zal een beroep kunnen worden gedaan op artikel 7, aanhef en onder b, van het voorstel voor die richtlijn. Daarin is, in navolging van de Europese privacyrichtlijn, bepaald dat lidstaten dienen voor te schrijven dat verwerking van strafrechtelijke persoonsgegevens die onder de werking van deze richtlijn vallen, slechts rechtmatig is wanneer en voor zover de verwerking noodzakelijk is om – onder meer – een wettelijke verplichting na te komen waaraan de voor de verwerking verantwoordelijke is onderworpen. Bij die grond geldt dezelfde redenering als hiervóór met betrekking tot artikel 7, onder d, van de Europese privacyrichtlijn is gegeven.

Met opmerkingen Daar dus ook vragen.

5. Slotbeschouwing

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

Een kaderwet kan dergelijke onduidelijkheden en belemmeringen wegnemen. Het betreft in de eerste plaats de wettelijke vastlegging van een breed doel waarbinnen samenwerkingsverbanden voor een ~~meer specifiek~~nader te specificeren doel binnen de algemeen geformuleerde wettelijke doelstellingen ~~doel~~ gegevens mogen uitwisselen, zodat vragen rond de zgn. verenigbaarheidstoets tot het verleden gaan behoren. Het gaat ook om een betere legitimering van de verstrekking van gegevens aan de deelnemers en een eventueel bureau van een samenwerkingsverband en van de uitwisseling met private partijen. De kaderwet zal verder praktische barrières slechten om binnen een samenwerkingsverband gegevens aan politie en OM te verstrekken. Omgekeerd zal gaan gelden dat strafrechtelijke gegevens voortaan gemakkelijker door politie en OM aan de andere partners in een samenwerkingsverband kunnen worden verstrekt. De kaderwet zal ook een expliciete legitimatie geven aan gegevensverwerking in de vorm van "datamining" en "profiling" om daarmee de mogelijkheden voor de opbouw van "intelligence" te verbeteren. De kaderwet zal – tot slot – de noodzaak wegnemen om iedere persoon van wie gegevens worden verwerkt, daarvan afzonderlijk op de hoogte brengen, zonder dat daarvoor, zoals nu is vereist, de vraag moet worden beantwoord of dat een onevenredige inspanning zou vergen.

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

Tegenover betere mogelijkheden tot gegevensverwerking staan ook betere waarborgen voor een zorgvuldige verwerking. De kaderwet zal een aantal belangrijke beginselen met betrekking tot de bescherming van persoonsgegevens expliciteren als toetssteen voor een geoorloofde gegevensverwerking. Te denken valt aan het vereiste dat aangetoond moet kunnen worden dat de gegevensverwerking noodzakelijk is en voldoet aan de beginselen van proportionaliteit en subsidiariteit. Andere vereisten zijn het versleutelen van gegevens waar dat met een redelijke inspanning mogelijk is en de effectiviteit niet onevenredig beïnvloedt, het openbaar maken van bijvoorbeeld eventuele risico-indicatoren die men gebruikt, en het uitvoeren van een "Privacy Impact Assessment".

Zo kan een kaderwet een goede optelsom laten zien van betere mogelijkheden tot gegevensuitwisseling en de nodige waarborgen voor een zorgvuldige gegevensverwerking.

Met opmerkingen Duidelijk is dat geheimhoudingsbepalingen belemmerend werken bij gegevensuitwisseling; Niet duidelijk is waarom geheimhoudingsbepalingen – wanneer het om samenwerkingsverbanden gaat – tot onnodige belemmeringen zouden leiden.

Met opmerkingen Dit is de makke van het voorstel.

Met opmerkingen Dit is allemaal niet nieuw en wat vervalt is de verenigbaarheidstoets en daarbij komt de potentiële verruiming van gegevensuitwisseling plus de intransparantie van weer een nieuw regime.

Bijlage 1 **Overzicht samenwerkingsverbanden**

PM

***Bijlage 2* Proeve van een Wet gegevensuitwisseling samenwerkingsverbanden**

Wet houdende bepalingen met betrekking tot de uitwisseling van gegevens in samenwerkingsverbanden (Wet gegevensuitwisseling 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 de mogelijkheden te verruimen om in samenwerkingsverbanden die werkzaam zijn in het belang van toezicht op de naleving van wetten en het voorkomen, opsporen en vervolgen van strafbare feiten, gegevens uit te wisselen, dat het tevens wenselijk is het uitwisselen daarvan zo zorgvuldig mogelijk te laten plaatsvinden en het met het oog daarop wenselijk is voorschriften met betrekking tot de uitwisseling van gegevens in samenwerkingsverbanden vast te stellen;

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:

Artikel 1 *Definitiebepalingen*

1. In deze wet en de daarop rustende bepalingen wordt verstaan onder:

a. bureau: voor zover het convenant daarin voorziet, de organisatie die het samenwerkingsverband ondersteunt bij het uitvoeren van zijn werkzaamheden;

b. deelnemers: de bestuursorganen en private organisaties die aan een samenwerkingsverband deelnemen;

c. samenwerkingsverband: een samenwerkingsverband als bedoeld in artikel 2.

2. In deze wet wordt onder gegeven, verwerken van gegevens en verstrekken van gegevens mede verstaan: persoonsgegeven, verwerken van persoonsgegevens en verstrekken van persoonsgegevens als bedoeld in de Wet bescherming persoonsgegevens.

Artikel 2 *Samenwerkingsverband*

1. Bestuursorganen en private organisaties kunnen deelnemen aan een samenwerkingsverband ten behoeve van een integraal optreden voor een welbepaald doel binnen de grenzen van een of meer van de volgende doeleinden:

a. het voorkomen, opsporen en vervolgen van strafbare feiten,

b. het handhaven van de openbare orde en veiligheid,

c. het uitoefenen van toezicht op de naleving van wettelijke voorschriften.

2. Private organisaties kunnen slechts aan een samenwerkingsverband deelnemen, voor zover zij zijn aangewezen bij regeling van Onze Minister van Veiligheid en Justitie en Onze Minister wie het aangaat.

Artikel 3 *Gegevensverwerking door het samenwerkingsverband*

1. In een samenwerkingsverband worden gegevens verwerkt die noodzakelijk zijn om het doel, bedoeld in artikel 2, te bereiken.

2. Voor de verwerking van gegevens in een samenwerkingsverband komen uitsluitend de categorieën van gegevens in aanmerking die bij of krachtens algemene maatregel van bestuur zijn vastgesteld.

3. Voor de verwerking van gegevens in het samenwerkingsverband zijn de deelnemers, tenzij zij anders overeenkomen, gezamenlijk verantwoordelijke in de zin van die wet.

4. De deelnemers zijn verplicht de noodzakelijke gegevens, bedoeld in het eerste lid, aan elkaar en aan het bureau te verstrekken, tenzij een belang van een deelnemer dat zwaarder weegt dan het gemeenschappelijk belang van het samenwerkingsverband, daaraan in de weg staat. Wettelijke voorschriften die deelnemers tot geheimhouding verplichten, blijven buiten toepassing.

5. De verplichting, bedoeld in het vierde lid, heeft mede betrekking op strafrechtelijke gegevens als bedoeld in de Wet politiegegevens, de Wet justitiële en strafvorderlijke gegevens en artikel 16 van de Wet bescherming persoonsgegevens.

6. Voor de verstrekking van gegevens kan een vordering als bedoeld in de artikelen 126nc en 126nd van het Wetboek van Strafvordering achterwege blijven.

Artikel 4 *Herkomst van gegevens*

De gegevens die het samenwerkingsverband verwerkt, zijn afkomstig:

a. van de deelnemers,

b. uit bij wet ingestelde openbare registers,

c. uit openbare bronnen,

d. uit registraties met authentieke gegevens,

e. van derden, voor zover dezen aannemelijk kunnen maken dat zij rechtmatig over deze gegevens beschikken.

Artikel 5 *Typen gegevensverwerking*

1. Samenwerkingsverbanden verwerken gegevens uitsluitend ten behoeve van:

a. het opstellen van rapporten waarin inzichten worden geboden of trends worden gesignaleerd die voor het bereiken van het doel, bedoeld in artikel 2, relevant zijn,

b. het opstellen van adviezen over acties om het doel, bedoeld in artikel 2, te bereiken, en het uitvoeren daarvan,

c. het uitvoeren van analyses om rapporten en adviezen als bedoeld onder a, onderscheidenlijk b, te kunnen opstellen,

d. het opstellen van profielen van groepen van personen, organisatie of bedrijven die met het oog op het doel, bedoeld in artikel 2, een verhoogd risico laten zien,

e. het koppelen van de profielen, bedoeld onder d, aan gegevens waarover het samenwerkingsverband rechtmatig de beschikking heeft, teneinde een lijst te kunnen opstellen van personen, organisaties of bedrijven die met het oog op het doel, bedoeld in artikel 2, een verhoogd risico laten zien,

f. het signaleren van patronen en het opstellen van risico-indicatoren voor het uitvoeren van analyses en het opstellen van profielen als bedoeld onder c, onderscheidenlijk d, of

g. het delen van informatie, inzicht en kennis in andere dan de onder a tot en met e bedoelde vormen, voor zover dat voor het bereiken van het doel, bedoeld in artikel 2, relevant is.

2. Samenwerkingsverbanden kunnen ten behoeve van het signaleren van patronen en het opstellen van risico-indicatoren als bedoeld in het eerste lid, onder f, bestanden koppelen die zijn geselecteerd op basis van veronderstelde relevantie voor het signaleren van deze patronen of het opstellen van deze indicatoren.

Artikel 6 *Waarborgen bij gegevensverwerking*

1. Een verwerking van gegevens in een samenwerkingsverband is alleen dan geoorloofd, indien:

a. de verwerking is getoetst aan de noodzaak de gegevens te verwerken voor het in artikel 2 bedoelde doel,

b. een mogelijke aantasting van de belangen van de natuurlijke personen of rechtspersonen op wie de verwerking betrekking heeft, niet onevenredig is in verhouding tot het doel dat met de verwerking wordt beoogd,

c. het doel dat met de verwerking wordt beoogd, in redelijkheid niet op minder ingrijpende wijze voor de betrokken personen of rechtspersonen kan worden bereikt,

d. de verwerking zoveel mogelijk versleuteld plaatsvindt, waarbij een afweging wordt gemaakt met de inspanningen die de versleuteling vergt, en de invloed van de versleuteling op de effectiviteit van de gegevensverwerking,

e. de risico-indicatoren, bedoeld in artikel 5, eerste lid, onder f, en de selectie van bestanden, bedoeld in artikel 4, tweede lid, openbaar zijn gemaakt op een voor het publiek toegankelijke wijze,

f. bij de verstrekking van gegevens aan andere deelnemers, waar nodig en mogelijk, is aangegeven wat de graad van juistheid en betrouwbaarheid van de gegevens is, en of de gegevens zijn gebaseerd op feiten dan wel een persoonlijk oordeel, en

g. een beoordeling van de effecten van de verwerking op de bescherming van persoonsgegevens heeft plaatsgevonden, voordat tot verwerking wordt overgegaan.

2. De deelnemers voeren acties op grond van de verwerkte gegevens slechts uit na overleg met de deelnemers van wie de gegevens afkomstig zijn. Indien een spoedeisend belang zich daartegen verzet, doen de deelnemers zo spoedig mogelijk na afloop van de acties mededeling aan de desbetreffende deelnemers.

3. Artikel 40 van de Wet bescherming persoonsgegevens is van overeenkomstige toepassing op persoonsgegevens die op grond van artikel 3 worden verwerkt.

Artikel 7 *Convenant*

1. De deelnemers regelen hun samenwerking in een convenant.

2. Het convenant regelt in ieder geval:

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 inrichting van het bureau,

e. de rechten en de verplichtingen van de deelnemers,

f. de datum van inwerkingtreding en de geldingsduur van het convenant,

g. de mogelijkheden van toetreding tot en opzegging van het convenant, en

h. de wijze waarop het convenant openbaar wordt gemaakt.

3. Het convenant wordt gepubliceerd in de Staatscourant en overigens op een voor het publiek toegankelijke wijze openbaar gemaakt.

Artikel 8 *Informatieprotocol*

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

2. Het informatieprotocol bevat in ieder geval:

a. een beschrijving van de gegevens dan wel soorten daarvan die in het samenwerkingsverband worden verwerkt,

b. een verantwoording van de wijze waarop uitvoering is gegeven aan artikel 6, a tot en met g,

c. 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,

d. regels op grond waarvan een beroep kan worden gedaan op een uitzondering op de verplichting, bedoeld in artikel 3, vierde lid, eerste volzin,

e. regels over de beveiliging van de gegevens,

f. regels over de geheimhouding door de deelnemers,

g. regels over de informatieverstrekking over de gegevensverwerking aan het publiek en aan betrokkenen,

h. regels over de wijze waarop betrokkenen hun rechten, bedoeld in de artikel 35 en 36 van de Wet bescherming persoonsgegevens en artikel 5, derde lid, van deze wet, kunnen uitoefenen,

i. regels over de verstrekking van gegevens aan derden,

j. regels over de termijnen voor het bewaren van gegevens, en

k. regels over de verwijdering en vernietiging van bewaarde gegevens.

3. Het informatieprotocol wordt gepubliceerd in de Staatscourant en overigens op een voor het publiek toegankelijke wijze openbaar gemaakt.

Artikel 9 *Wijziging Wet bescherming persoonsgegevens*

In artikel 22, eerste lid, van de Wet bescherming persoonsgegevens wordt "Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens" vervangen door: Wet politiegegevens, de Wet justitiële en strafvorderlijke gegevens of de Kaderwet gegevensuitwisseling samenwerkingsverbanden.

Artikel 10 *Wijziging van de Wet politiegegevens*

In artikel 20, eerste lid, van de Wet politiegegevens worden de volgende wijzigingen aangebracht:

1. Het zinsdeel "voor de volgende doeleinden:" wordt vervangen door: voor het verlenen van hulp aan hen die deze behoeven.
2. De onderdelen a tot en met d komen te vervallen.

Artikel 11 *Inwerkingtreding*

Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip.

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

Gegeven

De Minister van Veiligheid en Justitie,

De Staatssecretaris van Veiligheid en Justitie,

De Minister van Sociale Zaken en Werkgelegenheid,

De Minister van Financiën,

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,

Toelichting

De meeste elementen van deze proeve mogen in het licht van § 4 van de notitie voor zichzelf spreken. Hierna volgen enkele opmerkingen bij artikelen die nog enige nadere toelichting behoeven.

Artikel 2

Dit artikel regelt de mogelijkheid om aan een samenwerkingsverband deel te nemen dat onder de voorwaarden die elders in de kaderwet zijn neergelegd, gebruik kan maken van de mogelijkheden die deze wet biedt om gegevens uit te wisselen.

Het feit dat in artikel 2 over bestuursorganen wordt gesproken, sluit uiteraard niet uit dat in de praktijk een door een bestuursorgaan gemachtigde persoon, dienst of instelling aan het samenwerkingsverband deelneemt en met het oog daarop ook het convenant ondertekent.

Private organisaties kunnen slechts aan een samenwerkingsverband deelnemen, voor zover zij voorkomen op een lijst die is vastgesteld door de Minister van Veiligheid en Justitie en de Minister op wiens beleidsterrein de desbetreffende organisatie werkzaam is. Bij deelname van bijvoorbeeld het Verbond van verzekeraars gaat het dan om de Minister van Financiën.

Artikel 3

In het eerste lid van dit artikel is het noodzakelijkheidsvereiste vastgelegd: in een samenwerkingsverband worden alleen gegevens uitgewisseld, voor zover dat noodzakelijk is om het doel waarvoor het samenwerkingsverband is opgericht, te bereiken.

Op grond van het tweede lid dient een lijst te worden opgesteld waarop de categorieën van gegevens zijn vermeld die in § 4.5 zijn opgesomd. Uit een oogpunt van flexibiliteit kan de lijst worden aangevuld bij ministeriële regeling.

De gezamenlijke verantwoordelijkheid voor de gegevensverwerking waarvan in het derde lid wordt uitgegaan, laat onverlet dat de deelnemers ieder voor zich verantwoordelijk zijn voor het "voortraject", d.w.z. het aanleveren van gegevens ten behoeve van het samenwerkingsverband.[99]

Voor het geval dat een deelnemer aan een samenwerkingsverband een beroep wil doen op de mogelijkheid een uitzondering te maken op de in het vierde lid vastgelegde verstrekkingsplicht, schrijft artikel 8, tweede lid, onder d, voor dat het informatieprotocol daarover nadere regels bevat die daarbij in acht moeten worden genomen.

Hoewel uit het buiten toepassing verklaren van geheimhoudingsbepalingen in het vierde lid al impliciet kan worden afgeleid dat aan samenwerkingsverbanden ook strafrechtelijke gegevens mogen worden verstrekt, wordt in het vijfde lid geëxpliciteerd dat de verstrekkingsplicht ook geldt voor strafrechtelijke gegevens als bedoeld in de Wpg, de Wjsg en artikel 16 Wbp. Daarvoor is gekozen om buiten twijfel te stellen dat het in artikel 16 Wbp neergelegde verbod om strafrechtelijke persoonsgegevens te verwerken ingeval van verstrekking aan een samenwerkingsverband niet geldt.[100] Weliswaar geldt dat verbod op grond van artikel 2, tweede lid, Wbp niet met betrekking tot gegevens die ter uitvoering van de Wpg en Wjsg worden verwerkt, maar het is wenselijk voor alle soorten van strafrechtelijke gegevens in één bepaling duidelijk te maken dat zij onder de verstrekkingsplicht vallen. Dat geldt ook voor de onder artikel 16 Wbp vallende strafrechtelijke persoonsgegevens die door buitengewone opsporingsambtenaren (Boa's) worden verwerkt. Bestuursorganen die boa's in dienst hebben, mogen derhalve op grond van het vijfde lid van artikel 3 ook gegevens aan samenwerkingsverbanden verstrekken die deze boa's hebben verzameld. Voor de verdere verwerking van strafrechtelijke persoonsgegevens in het samenwerkingsverband is in artikel 9 een wijziging van de Wbp opgenomen die het in artikel 16 Wbp neergelegde verbod daarvoor buiten toepassing verklaart.

---

[99] Vgl. Kamerstukken II 2012-2013, 33579, nr. 3, blz. 37-38.

[100] Zoals in § 3.7 is aangegeven kan met een beroep op artikel 23, eerste lid, onder f, Wbp van dat verbod worden afgeweken.

Uit het zesde lid vloeit voort dat, voor zover de politie, een bijzondere opsporingsdienst of het OM tot de deelnemers van een samenwerkingsverband behoren, voor de verstrekking van gegevens een vordering als bedoeld in de artikelen 126nc en 126nd van het Wetboek van Strafvordering achterwege kan blijven.

Artikel 4

In dit artikel is geëxpliciteerd uit welke gegevensbronnen een samenwerkingsverband mag putten. De opsomming in dit artikel dekt in voldoende mate de bronnen die in de praktijk worden gebruikt, met dien verstande dat bij gebruik van gegevens, bedoeld onder e, de eis wordt gesteld dat de verstrekker van gegevens tegenover het samenwerkingsverband in voldoende mate aannemelijk moet maken dat hij rechtmatig over deze gegevens beschikt. Deze eis wordt niet alleen ingegeven door het belang van zorgvuldig overheidsoptreden, maar ook door het belang te voorkomen dat de verantwoordelijke voor de gegevensverwerking in het samenwerkingsverband aansprakelijk wordt gesteld voor de verwerking van gegevens die de betrokken derde onrechtmatig heeft verkregen.

Artikel 5

Voor de uit § 4.6 overgenomen opsomming van doeleinden van gegevensverwerking in het eerste lid is mede acht geslagen op bestaande vormen van gegevensverwerking in samenwerkingsverbanden en op nieuwe vormen daarvan die nog in ontwikkeling zijn, maar door bijvoorbeeld twijfel over de toelaatbaarheid daarvan onder de huidige wetgeving, in de praktijk nog niet worden toegepast.

Waar met de rapporten waarop onderdeel a van het eerste lid ziet, gedoeld wordt op documenten met een louter beschrijvend karakter, wordt ervan uitgegaan dat adviezen als bedoeld in onderdeel b, aanbevelingen bevat, 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. Met betrekking tot alle acties waarop het advies betrekking heeft, stelt onderdeel b buiten twijfel dat de verwerking van gegevens zich ook uitstrekt tot het uitvoeren van deze acties.

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

De lijst, bedoeld onder e, kan het karakter van een zgn. zwarte lijst krijgen. De implicaties van plaatsing op en dergelijke lijst kunnen fors zijn. Om die reden is bij het opstellen van een dergelijke lijst extra zorgvuldigheid geboden. De checklist die het Cbp heeft opgesteld voor het opstellen van zwarte lijsten in bedrijven of bedrijfstakken, kan hierbij behulpzaam zijn.[101]

Het eerste lid heeft mede tot doel buiten twijfel te stellen dat de onder a tot en met f genoemde doeleinden toelaatbaar zijn. Omdat het eerste lid ook tot doel heeft een limitatieve opsomming van toelaatbare doeleinden te geven, bevat onderdeel g een restcategorie, die enerzijds ruimte geeft voor andere vormen van verwerking, maar deze anderzijds wel uitdrukkelijk bindt aan het doel van het samenwerkingsverband.

Het tweede lid geeft een expliciete basis voor vormen van "datamining", waarbij een computer met behulp van geavanceerde software bepaalde patronen kan signaleren die van belang zijn voor het opstellen van risico-indicatoren. Het kan hierbij niet gaan om analyses op basis van ongericht verzamelde informatie; het tweede lid schrijft voor dat het om analyses moet gaan op basis van gerichte selecties van bestanden. Uit een oogpunt van transparantie schrijft artikel 6, eerste lid, onder e, voor dat de selectie van bestanden op een voor het publiek toegankelijke wijze openbaar moet worden gemaakt.

---

[101] Zie: http://www.cbpweb.nl/downloads_overig/checklist_zwarte_lijsten.pdf.

Artikel 6

Het eerste lid en tweede lid bevatten de waarborgen voor een zorgvuldige gegevensverwerking die zijn beschreven en toegelicht in § 4.7.

Artikel 40 Wbp geeft iemand van wie de persoonsgegevens worden verwerkt op grond van artikel 8, onder e en f, Wbp, het recht daartegen bij de verantwoordelijke te allen tijde verzet aan te tekenen in verband met zijn bijzondere persoonlijke omstandigheden. Omdat de verwerking van persoonsgegevens op basis van de kaderwet geschiedt op basis van een zelfstandige, in artikel 3 neergelegde grond, die – zie § 4.12 – breder is dan de grond van artikel 8, onder e, Wbp, kan artikel 40 Wbp geen rechtstreekse toepassing bij gegevensverwerking onder de kaderwet vinden. Om die reden wordt artikel 40 Wbp in het derde lid van overeenkomstige toepassing verklaard.

Artikel 7

De regels die in het convenant worden vastgelegd, dienen uiteraard te blijven binnen de grenzen die de kaderwet, de Wbp en andere wetten stellen. Dat geldt ook voor het doel dat ingevolge het tweede lid, onder a, in het convenant wordt vastgelegd. Dat doel moet binnen de grenzen van de brede doelomschrijving uit artikel 2 vallen.

De regeling van taken en werkzaamheden, bedoeld in het tweede lid, onder b, dient tenminste een specifieke beschrijving te bevatten van de in artikel 5 genoemde typen van gegevensverwerking, voor zover het samenwerkingsverband deze typen uitvoert.

De regeling van de in het tweede lid, 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. De regeling zou ook – zie § 4.8 - een regisseur kunnen aanwijzen die de deelnemers ondersteunt bij de uitoefening van hun rol als gezamenlijk verantwoordelijke in de zin van de Wbp. In de regeling kan, tot slot, desgewenst gebruik worden gemaakt van de in artikel 3, derde lid, opgenomen mogelijkheid één van deelnemers als verantwoordelijke voor de gehele gegevensverwerking in het samenwerkingsverband aan te wijzen.

Bij de in het tweede lid, onder e, bedoelde verplichtingen kan onder meer worden gedacht aan verplichtingen op het terrein van de bekostiging van de samenwerking, inclusief een eventueel ondersteunend bureau. Denkbaar is ook dat de verplichtingen betrekking hebben op het detacheren van medewerkers bij het bureau.

De combinatie van het tweede lid, onder h, en het derde lid impliceert dat het convenant voorschrijft dat het, behalve in de Staatscourant, ook openbaar wordt gemaakt op bijvoorbeeld de website van het samenwerkingsverband.

Artikel 8

De elementen die het informatieprotocol in ieder geval dient te bevatten, zijn beschreven en toegelicht in § 4.10.

Met betrekking tot het tweede lid, onder d, kan worden opgemerkt dat een uitzondering op de verstrekkingsplicht die in artikel 3 is vastgelegd, zowel kan slaan op een individuele casus als op bepaalde, zeer bijzondere gegevens die in structurele zin niet aan het samenwerkingsverband worden verstrekt. Het doel van de regeling in het informatieprotocol moet zijn dat voor alle partijen vooraf helder is in welke gevallen op deze uitzonderingsmogelijkheid een beroep kan worden gedaan.

Het tweede lid, onder g, schrijft voor dat het informatieprotocol regels bevat over de informatieverstrekking over de gegevensverwerking aan het publiek en aan betrokkene. Het gaat hier om informatieverstrekking in aanvulling op de in het derde lid van artikel 7 en 8 voorgeschreven openbaarmaking van het convenant, respectievelijk 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

het tweede lid, onder g, vloeit voort dat het informatieprotocol ook daarover nadere regels dient te bevatten.

Artikel 9

Artikel 22 Wbp bepaalt dat het verbod om strafrechtelijke persoonsgegevens te verwerken, onder meer niet van toepassing is, indien de verwerking geschiedt door verantwoordelijken die deze hebben verkregen krachtens de Wpg en Wjsg. Nu de kaderwet in artikel 3, vijfde lid, een zelfstandige grond tot verkrijging van strafrechtelijke persoonsgegevens creëert, moet artikel 22 Wbp worden aangevuld met een verwijzing naar de kaderwet.

Artikel 10

Op grond van artikel 20 Wpg kan de korpschef van de nationale politie in overeenstemming met het bevoegd gezag bepaalde politiegegevens aan samenwerkingsverbanden verstrekken, voor zover dat noodzakelijk is met het oog op een zwaarwegend algemeen belang en voor de volgende doeleinden:
a. het voorkomen en opsporen van strafbare feiten,
b. het handhaven van de openbare orde,
c. het verlenen van hulp aan hen die deze behoeven,
d. het uitoefenen van toezicht op de naleving van regelgeving.

In het licht van artikel 2, eerste lid, van de kaderwet wordt de verstrekking voor de hiervóór aangegeven doeleinden, onder a, b en d, voortaan door de kaderwet bestreken. De korpschef behoeft voor die doeleinden geen overeenstemming met het bevoegd gezag meer te zoeken en niet te toetsen of er sprake is van een zwaarwegend algemeen belang. Die laatste toets ligt als het ware al opgesloten in de kaderwet. Een en ander impliceert dat artikel 20 Wpg zo moet worden aangepast dat de in dat artikel geregelde mogelijkheid van gegevensverstrekking alleen nog maar betrekking heeft op verstrekking voor het verlenen van hulp aan hen die deze behoeven.