Wetsvoorstel gegevensverwerking door samenwerkingsverbanden (WGS)

MEMORIE VAN TOELICHTING – versie 3 april 2020

I. ALGEMEEN

1. Inleiding

Dit wetsvoorstel strekt er in de eerste plaats toe de verwerking van persoonsgegevens en andere gegevens door bepaalde, in deze wet aangewezen samenwerkingsverbanden voor de vervulling van een in deze wet omschreven doel van zwaarwegend algemeen belang van een adequate juridische basis te voorzien. Het betreft het Financieel Expertisecentrum (FEC), de Infobox Crimineel en Onverklaarbaar Vermogen (iCOV), de Regionale Informatie- en Expertisecentra (RIEC's) en de Zorg- en Veiligheidshuizen (ZVH's). Uit een oogpunt van flexibiliteit bevat het wetsvoorstel daarnaast de mogelijkheid om bij amvb (met een zogenoemde nahangprocedure) de verwerking van persoonsgegevens en andere gegevens door bepaalde, bij amvb aan te wijzen nieuwe samenwerkingsverbanden voor de vervulling van een nader bij amvb omschreven doel van zwaarwegend algemeen belang eveneens van een adequate juridische basis te voorzien. Het voorstel bevat in aanvulling op de Algemene verordening gegevensbescherming (AVG)[1] ook een aantal waarborgen voor een goede bescherming van persoonsgegevens die door deze samenwerkingsverbanden worden verwerkt. Met samenwerkingsverbanden wordt hier gedoeld op een verband van overheidsorganen, overheidsinstanties en soms ook private partijen die gezamenlijk gegevens verwerken voor de vervulling van het in de wet c.q. bij amvb omschreven doel van zwaarwegend algemeen belang. Het kan om een verband gaan waaraan uitsluitend overheidsorganen en overheidsinstanties deelnemen, maar ook om verbanden waaraan mede door private partijen wordt deelgenomen.

De behoefte aan dit wetsvoorstel wordt ingegeven door de wens om maatschappelijke vraagstukken meer dan voorheen van een integrale aanpak te voorzien, waarbij verschillende instanties uit de overheid maar soms ook de private sector met elkaar samenwerken om dat vraagstuk aan te pakken. Te denken valt aan de RIEC's, waarin onder meer gemeenten, de politie, het openbaar ministerie en de Belastingdienst de inzet van hun bestuurlijke, strafrechtelijke en fiscale taken en bevoegdheden op elkaar afstemmen om tot de meest effectieve aanpak van bijvoorbeeld ondermijnende criminaliteit te komen. Een dergelijke aanpak impliceert vaak dat partijen met elkaar gegevens uitwisselen en deze vervolgens samen verwerken om daaruit informatie af te leiden die sturing kan geven aan de inzet van hun taken en bevoegdheden.
Tegen deze achtergrond laat de praktijk zien dat samenwerkingsverbanden bij het gezamenlijk verwerken van gegevens soms op knelpunten stuiten. De verstrekking van gegevens aan een samenwerkingsverband berust veelal op grondslagen om aan afzonderlijke deelnemers aan dat verband gegevens te verstrekken. Hierdoor dient de noodzaak van verstrekking *per individuele deelnemer* te worden aangetoond. Een heldere basis om gegevens *voor het doel van het samenwerkingsverband als zodanig* te verstrekken ontbreekt dus veelal. Een tweede knelpunt betreft de verwerking van gegevens *binnen een samenwerkingsverband*. Iedere deelnemer aan een samenwerkingsverband is gehouden de door hem individueel ontvangen gegevens vertrouwelijk te behandelen. Deze eis staat in de weg aan een gezamenlijke gegevensverwerking binnen zo'n verband. Dat belemmert de mogelijkheden om in een gezamenlijk casusoverleg[2] gegevens over bepaalde personen en ondernemingen met elkaar in verband te brengen of een gezamenlijke data-analyse uit te voeren teneinde

[1] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119).
[2] Het kan daarbij gaan om analyses in een concrete casus, bijvoorbeeld inzake de aanpak van criminaliteit, waarbij partijen gezamenlijk bepalen welke interventies de meeste geschikte zijn om in de desbetreffende casus op te treden.

risico-indicatoren of risico-modellen vast te stellen, tenzij de deelnemers hun grondslag in sectorale wetgeving kunnen vinden. Weer een ander knelpunt is dat sectorale wetten veelal geen goede, op samenwerkingsverbanden toegesneden, grondslagen bevatten voor verstrekking aan en verdere verwerking van gegevens door samenwerkingsverbanden waaraan ook een of meer *private partijen* deelnemen, terwijl dat met het oog op de behartiging van een doel van zwaarwegend algemeen belang wel wenselijk kan zijn. Een laatste knelpunt dat hier wordt genoemd, is dat de verstrekking van de resultaten van de verwerking vanuit samenwerkingsverbanden thans vaak een suboptimale grondslag heeft als gevolg van het feit dat de grondslag voor de verstrekking van gegevens aan en de verwerking daarvan binnen een samenwerkingsverband ook al suboptimaal is of niet op samenwerkingsverband is toegesneden. Dit wetsvoorstel beoogt deze knelpunten weg te nemen bij de gegevensverwerking door samenwerkingsverbanden die bij of krachtens deze wet zijn aangewezen (zie nader § 3.3).
Om deze gegevensverwerking zorgvuldig te laten verlopen bevat dit wetsvoorstel ook een aantal generieke waarborgen ter aanvulling of precisering van de meer algemene waarborgen die de bestaande wetgeving met betrekking tot persoonsgegevens al kent. Deze hebben betrekking op onder meer de aanwijzing van de verwerkingsverantwoordelijken, de mogelijkheid om bij amvb voorwaarden en beperkingen aan de verwerkingen te stellen, de verlening van toegang tot de systemen waarin de samenwerkingsverbanden gegevens verwerken aan uitsluitend door de deelnemers geautoriseerde medewerkers, het loggen van gegevens die noodzakelijk zijn voor controle en toezicht, het instellen van een rechtmatigheidsadviescommissie die de rechtmatigheid van de verwerking van persoonsgegevens door het samenwerkingsverband beoordeelt, het treffen van technische en organisatorische maatregelen om de kwaliteit van de gezamenlijke gegevensverwerking te bevorderen, geheimhouding en het opstellen van een jaarverslag inzake de gegevensverwerking (zie nader § 3.4).

In dit algemeen deel van de memorie van toelichting zal hierna achtereenvolgens aandacht worden besteed aan de volgende onderwerpen:

§ 2	Aanleiding
§ 3	Hoofdlijnen wetsvoorstel
§ 3.1	Inleiding
§ 3.2	Reikwijdte wetsvoorstel
§ 3.2.1	Aanwijzing bij wet c.q. bij amvb
§ 3.2.2	Zwaarwegend doel van algemeen belang
§ 3.3	Oplossing knelpunten in de gegevensverwerking in het kader van samenwerkingsverbanden
§ 3.3.1	Verstrekking van gegevens aan een samenwerkingsverband
§ 3.3.2	Verwerking van gegevens binnen een samenwerkingsverband
§ 3.3.3	Verwerking van gegevens met private partijen
§ 3.3.4	Verstrekking van de resultaten van de verwerking uit een samenwerkingsverband
§ 3.4	Waarborgen
§ 3.5	Voorafgaande toetsende rol van de Autoriteit persoonsgegevens
§ 4	In de wet aangewezen samenwerkingsverbanden
§ 4.1	Het Financieel Expertisecentrum (FEC)
§ 4.2	De Infobox Crimineel en Onverklaarbaar vermogen (iCOV)
§ 4.3	De Regionale Informatie- en Expertisecentra (RIEC's)
§ 4.4	De Zorg- en Veiligheidshuizen (ZVH)
§ 5	Verhouding tot bestaande en nieuwe samenwerkingsverbanden
§ 6	Verhouding tot de AVG en andere wetgeving
§ 7	Grondrechtelijke aspecten
§ 8	Overige aspecten
§ 9	Advies Autoriteit persoonsgegevens
§ 10	Overige consultatiereacties

2. Aanleiding

Het voorstel vloeit voort uit een brief van het toenmalige kabinet van 14 december 2014 aan de Tweede Kamer over de aanpak van fraude (Kamerstukken II 2014/15, 32761, nr. 79). Het kabinet constateert in die brief dat de effecten van fraude met overheidsvoorzieningen verder reiken dan alleen de directe financiële schade voor de overheid zelf. Fraude ondermijnt ook de integriteit van het economisch stelsel en het vertrouwen in de financiële instellingen, tast de betaalbaarheid van voorzieningen aan en kan leiden tot een vermindering van het maatschappelijke draagvlak voor sociale voorzieningen en tot aantasting van het rechtsgevoel. Het kabinet stelt de aanpak van fraude dan ook te willen versterken. Dit vergt een brede en integrale benadering. Zo'n brede en integrale benadering vereist een efficiënte en doeltreffende samenwerking van alle betrokken partijen. Daarvoor is uitwisseling van informatie essentieel. Alleen dan kunnen partijen tot zo effectief mogelijke en op elkaar afgestemde interventies komen. Dit heeft tot gevolg dat overheidsorganisaties sinds een aantal jaren in toenemende mate in multidisciplinaire samenwerkingsverbanden opereren om aan die brede en integrale aanpak gestalte te geven. De ontwikkelingen op het terrein van ICT bieden partijen binnen de overheid immers steeds meer mogelijkheden om tot een snelle, accurate en volledige uitwisseling van informatie te komen en op grond van deze informatie analyses te maken die tot een integraal en effectief optreden leiden. De intensivering en verbreding van de samenwerking tussen diverse organisaties bij het voorkomen en bestrijden van fraude heeft intussen scherper zicht gegeven op grenzen en belemmeringen waar deze organisaties op stuiten als het gaat om het uitwisselen van de voor die samenwerking noodzakelijke gegevens. Tegelijkertijd, zo stelt het kabinet in zijn brief, is van belang om te benadrukken dat, als wordt bezien of dergelijke belemmeringen kunnen worden weggenomen, rekening moet worden gehouden met bepaalde belangen, zoals het recht op bescherming van persoonsgegevens, en met grenzen die op Europees niveau aan gegevensuitwisseling worden gesteld.

Tegen deze achtergrond heeft het toenmalige kabinet een verkenning laten uitvoeren naar een kaderwet voor de gegevensuitwisseling in samenwerkingsverbanden die als bijlage bij voornoemde brief van 14 december 2014 is gevoegd. Uit het rapport van de Werkgroep Verkenning kaderwet gegevensuitwisseling "Kennis delen geeft kracht" blijkt dat zich bij deze gegevensuitwisseling knelpunten voordoen in relatie tot onder meer de juridische status van samenwerkingsverbanden, de uitwisseling met private partijen, de verstrekking van gegevens aan en door de opsporingsdiensten en het openbaar ministerie, alsmede het uitvoeren van geavanceerde data-analyses op basis van bronnen die onder verschillende wettelijke regimes vallen (zie bijlage bij Kamerstukken II 2014/15, 32761, nr. 79). In zijn brief schrijft het kabinet zich te herkennen in deze knelpunten en trekt het de conclusie dat een aanvang dient te worden gemaakt met het voorbereiden van wetgeving ter oplossing daarvan. Het onderschrijft daarbij de conclusie dat deze wetgeving een bredere reikwijdte dient te krijgen dan fraudebestrijding (zie nader § 3.2.2). De brief en het rapport zijn vervolgens besproken in het Algemeen Overleg van 8 april 2015 over de rijksbrede aanpak van fraude (Kamerstukken II 2014/15, 17050, nr. 505). In dat overleg zijn verschillende aandachtspunten naar voren gebracht waarmee bij de voorbereiding van het wetsvoorstel rekening zou moeten worden gehouden. Het betreft onder meer een nadere onderbouwing van nut en noodzaak van een kaderwet en van het uitgangspunt "ja, tenzij" bij gegevensuitwisseling volgens de beoogde kaderwet, het belang van goede waarborgen en het uitvoeren van een Privacy Impact Assessment. Verderop in deze toelichting moge blijken dat met deze aandachtspunten rekening is gehouden.

3. Hoofdlijnen wetsvoorstel

3.1 Inleiding

Zoals in het rapport van de Werkgroep Verkenning kaderwet gegevensuitwisseling al naar voren komt, heeft gegevensverwerking altijd een centrale plaats gehad bij de interne werkprocessen van veel overheidsinstanties en in de verhouding overheid-burger. Gegevensverwerking is immers een belangrijk onderdeel van en dienstbaar aan de opgedragen taak van praktisch elke overheidsinstantie. Iedere overheidsinstantie heeft zijn eigen taak en oefent een eigen gegevenshuishouding uit bij de uitvoering van die taak. Zolang de gegevensverwerking plaatsvindt door de overheidsinstantie zelf binnen het kader van de eigen taak, ligt de bevoegdheid tot dergelijke gegevensverwerking in beginsel opgesloten in de taakomschrijving van de desbetreffende instantie. Een rechtsgrond voor verwerking van persoonsgegevens is daarmee gegeven. In deze situatie is het opnemen van bepalingen rond gegevensverwerking veelal beperkt tot het opnemen van verplichtingen tot informatieverstrekking aan burgers die met de betrokken overheidsinstantie te maken hebben. Ook is meestal voor de betrokken overheidsinstantie sprake van een geheimhoudingsplicht[3], zodat burgers en bedrijven erop kunnen vertrouwen dat hun gegevens in veilige handen zijn.

Als er sprake is van een gerechtvaardigde behoefte bij de ene overheidsinstantie aan gegevens waarover een andere overheidsinstantie beschikt en dus aan het uitwisselen van gegevens tussen overheidsinstanties, dient een dergelijke uitwisseling van gegevens van een adequate juridische grondslag te worden voorzien. Zo'n grondslag ontbreekt als de verstrekking van gegevens buiten de taken en bevoegdheden van de betrokken overheidsinstantie valt. De bevoegdheid gegevens te delen met een andere overheidsinstantie dient in dat geval expliciet in het leven te worden geroepen. Inmiddels is er dan ook een groot aantal bepalingen tot stand gekomen op grond waarvan de ene overheidsinstantie gegevens verstrekt aan de andere overheidsinstantie. Voor ieder rechtsgebied dan wel iedere overheidsinstantie is dit overigens op eigen wijze geregeld, passend binnen de regelgeving die geldt voor dat rechtsgebied of die instantie.

Voor zover sectorspecifieke regelingen bepalingen bevatten over verstrekking aan derden, hebben deze meestal betrekking op verstrekking aan één specifieke partij voor een specifiek doel en niet op verstrekking aan partijen die voor een gezamenlijk doel in een samenwerkingsverband opereren[4], laat staan op verstrekking aan samenwerkingsverbanden als zodanig. Bovendien bevatten deze sectorspecifieke regelingen meestal geen bepalingen over de wijze waarop en voorwaarden waaronder de verstrekte gegevens door zo'n samenwerkingsverband mogen worden verwerkt.[5] Een en ander leidt in de praktijk tot knelpunten die een optimale gegevensverwerking door bepaalde samenwerkingsverbanden, rekening houdend met het recht op bescherming van persoonsgegevens, bemoeilijken.

Nadat in § 3.2 is stilgestaan bij de reikwijdte van het wetsvoorstel, komen in § 3.3 de knelpunten aan bod die dit voorstel beoogt op te lossen.

3.2 Reikwijdte wetsvoorstel

3.2.1 Aanwijzing bij wet c.q. bij amvb

Het rapport van de Werkgroep Verkenning kaderwet gegevensuitwisseling schetste de contouren van een wet die de basis zou vormen voor bij convenant op te richten samenwerkingsverbanden. In zijn reactie op dit rapport ging ook het toenmalige kabinet ervan uit dat voor de oprichting van een samenwerkingsverband dat onder deze wet zou vallen, een convenant zou volstaan.

[3] Zie onder meer artikel 7 Wet politiegegevens (Wpg), artikel 52 Wet justitiële en strafvorderlijke gegevens (Wjsg), artikel 67 Algemene wet inzake rijksbelastingen (Awr) en artikel 74 Wet Suwi.
[4] Uitzonderingen hierop zijn te vinden in artikel 20 Wpg, artikel 28, tweede lid, onder d, Wet Bibob, artikel 64 Wet Suwi en artikel 43c, onder m, u en w, Uitvoeringsregeling Awr. Verder bevat ook de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) in artikel 33, eerste lid, onder b, een specifieke bepaling met betrekking tot verwerking van strafrechtelijke gegevens door en ten behoeve van samenwerkingsverbanden.
[5] Een uitzondering hierop vormen artikel 64 Wet Suwi en de daarop berustende bepalingen in het Besluit Suwi.

Het huidige kabinet was naderhand echter van oordeel dat aan de aanwijzing van samenwerkingsverbanden die onder de met dit wetsvoorstel beoogde Wet gegevensverwerking door samenwerkingsverbanden (WGS) vallen, een zwaardere eis moest worden gesteld. Deze eis, die opgenomen was in het wetsvoorstel, zoals dat ter consultatie is voorgelegd, hield in dat de aanwijzing daarvan bij amvb dient plaats te vinden. Het kabinet had hiervoor de volgende redenen. De eerste is dat het beter bij het legaliteitsbeginsel past als een samenwerkingsverband dat onder de WGS valt, is aangewezen bij amvb en als daarvoor bij amvb een doel van zwaarwegend algemeen belang wordt omschreven. Een tweede reden is dat de keuze voor een amvb een betere legitimatie geeft om, zo nodig, de ruimte te benutten die artikel 6, derde lid, van de AVG biedt om persoonsgegevens te laten verwerken. Een derde en laatste reden is dat met een keuze voor de amvb als aanwijzingseis, er een duidelijker verschil optreedt tussen samenwerkingsverbanden die op basis van de WGS zijn aangewezen, en andere samenwerkingsverbanden, die louter op een convenant berusten; op laatstbedoelde samenwerkingsverbanden is de WGS niet van toepassing.

Naar aanleiding van het advies van de Afdeling advisering van de Raad van State over het wetsvoorstel heeft het kabinet inmiddels de conclusie getrokken een verdergaande stap te moeten zetten. Die houdt in dat het wetsvoorstel zelf de gezamenlijke gegevensverwerking door een viertal samenwerkingsverbanden regelt: het FEC, iCOV, de RIEC's en de Zorg- en Veiligheidshuizen. Het gaat hier om verbanden die voor essentiële maatschappelijke vraagstukken samenwerken: de integrale aanpak van – samengevat – risico's van respectievelijk: inbreuken op de integriteit van de financiële sector, van witwas- of fraudeconstructies, van georganiseerde criminaliteit, en van complexe problemen rond personen op het vlak van zorg en veiligheid. Het betreft hier bovendien samenwerkingsverbanden die inmiddels ten minste vijf jaar bestaan en daarmee een bestendig karakter hebben.

Om voldoende flexibiliteit te houden voor het oprichten van nieuwe samenwerkingsverbanden nadat de WGS in werking is getreden, wordt met hoofdstuk 3 een delegatiegrondslag voorgesteld, op basis waarvan een nieuw samenwerkingsverband bij amvb kan worden aangewezen. Daarbij wordt een bijzondere nahangprocedure voorgesteld om het parlement ook bij de aanwijzing en regeling van dit nieuwe verband te betrekken. Deze procedure houdt in dat na publicatie van de amvb de Staten-Generaal een periode van vier weken krijgen waarin één van beide Kamers met een absolute meerderheid kan verzoeken om het in de amvb geregelde onderwerp bij wet te regelen. In dat geval wordt de amvb onverwijld ingetrokken en wordt een daartoe strekkend wetsvoorstel zo spoedig mogelijk ingediend. In vier bestaande wetten is deze procedure overigens geregeld in deze vorm.[6]

Aanwijzing van een samenwerkingsverband bij amvb is uitsluitend mogelijk als bij amvb doeleinden worden omschreven die passen binnen het raamwerk van hoofdstuk 3:

a. het voorkomen en bestrijden van ernstige vormen van criminaliteit;
b. het voorkomen van grootschalig of systematisch onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen; of
c. het voorkomen van grootschalige of systematische ontduiking van wettelijke verplichtingen tot betaling van belastingen, retributies en rechten bij in- en uitvoer.

Duidelijkheidshalve wordt benadrukt dat de aanwijzing in de zin van deze wet nadrukkelijk niet tot gevolg heeft dat er een nieuwe overheidsorgaan, instantie of zelfstandige entiteit van enige vorm ontstaat, waarmee er eventueel nieuwe juridische verhoudingen zouden ontstaan tussen de deelnemers of ter zake van het samenwerkingsverband als zodanig. Aan het wetsvoorstel ligt het uitgangspunt ten grondslag dat de gezamenlijke verwerking van persoonsgegevens en andere relevante

[6] Artikel 13, derde lid, Wet op het primair onderwijs, artikel 2.6.7, derde lid, Wet maatschappelijke ondersteuning 2015, artikelen 2, zesde lid, 13, zevende lid, en 22, zevende lid, Wet op de expertisecentra en artikel 65 Wet toelating zorginstellingen

gegevens ten dienste staat aan de uitoefening van de bestaande wettelijke taken en bevoegdheden van de deelnemers. Er worden met de aanwijzing of enige andere bepaling in dit wetsvoorstel derhalve geen nieuwe taken of bevoegdheden aan de deelnemers of aan de samenwerkingsverbanden als zodanig toegekend. Voor zover dit wetsvoorstel regels bevat over de juridische verhoudingen tussen de deelnemers, hebben die uitsluitend betrekking op de nadere uitwerking van de eisen die de Algemene verordening gegevensbescherming stelt ter zake van de gezamenlijke verwerking, zoals de gezamenlijke verwerkingsverantwoordelijkheid.
Evenmin regelt dit wetsvoorstel de organisatie, inrichting, positionering en het beheer van de samenwerkingsverbanden. De regeling daarvan is voorbehouden aan de deelnemers. Een samenwerkingsverband vraagt om ondersteuning in de vorm van huisvesting, ICT-voorzieningen, ondersteuning en personeel. De deelnemers maken onderling afspraken over de wijze waarop het samenwerkingsverband wordt ingericht, taken stellen, prioriteiten vaststellen en zorgdragen voor financiering en beheer. Ook kan sprake zijn van mandaatverlening in de zin van afdeling 10.1.1 van de Algemene wet bestuursrecht.

3.2.2 Doel van zwaarwegend algemeen belang

Het rapport van de Werkgroep Verkenning kaderwet gegevensuitwisseling heeft betrekking op gegevensverwerking op een breder terrein dan fraudebestrijding. Een eerste reden die daarvoor in het rapport wordt aangedragen, is dat de meeste samenwerkingsverbanden die zich met de aanpak van fraude bezighouden, ook andere doelen hebben. Een wet die zich beperkt tot gegevensverwerking ten behoeve van de fraudebestrijding zou tot gevolg hebben dat deze samenwerkingsverbanden ten dele wel en ten dele niet onder de werking van die wet vallen. Dat zou voor die samenwerkingsverbanden een onwerkbare situatie opleveren. Zo kunnen de RIEC's (Regionale Informatie- en Expertisecentra) bepaalde persoonsgegevens verwerken met het oog op tegelijkertijd georganiseerde hennepteelt èn fraude in de vastgoedsector. Het zou dan niet duidelijk zijn in hoeverre de verwerking van gegevens in dat geval onder het regime van de kaderwet zou plaatsvinden. Een andere reden is dat een kaderwet evenzeer van belang kan zijn met het oog op knelpunten bij de verwerking van gegevens door samenwerkingsverbanden op andere terreinen. Bij een relatief smalle kaderwet zou dus al gauw de behoefte ontstaan om voor aanpalende terreinen eveneens kaderwetgeving op te stellen.

Een en ander zou volgens het rapport pleiten voor een kaderwet die een breder terrein dan fraudebestrijding bestrijkt. Dit bredere terrein zou de volgende doeleinden kunnen omvatten:

a. de voorkoming van onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen en het bevorderen dat aan wettelijke verplichtingen wordt voldaan tot betaling van belastingen, retributies en rechten bij in- en uitvoer,
b. de uitoefening van toezicht op de naleving van wettelijke voorschriften,
c. de handhaving van de openbare orde en veiligheid,
d. de voorkoming en opsporing van strafbare feiten.

Blijkens een inventarisatie van samenwerkingsverbanden die bij het rapport is gevoegd, is het immers dit brede terrein, opgesomd onder a tot en met d, waarop zich samenwerkingsverbanden manifesteren die gegevens binnen en tussen het bestuursrechtelijke en strafrechtelijke domein willen verwerken. Hierbij valt te denken aan samenwerkingsverbanden op het terrein van de aanpak van de georganiseerde criminaliteit, de bestrijding van hennepteelt, de aanpak van verschillende vormen van fraude (uitkeringsfraude, vastgoedfraude, verzekeringsfraude, etc.) en de bestrijding van milieucriminaliteit, cybercrime en voertuigcriminaliteit.

In voornoemde brief van 14 december 2014 had het kabinet te kennen gegeven zich in deze brede reikwijdte goed te kunnen vinden. Het kabinet komt thans tot dezelfde afweging, aangevuld met het begrip "taak van zwaarwegend algemeen belang". Dit is een

beperkter begrip dan het begrip "taak van algemeen belang", dat in artikel 6 AVG wordt gehanteerd in de formulering van een van de rechtsgronden voor verwerking van persoonsgegevens.

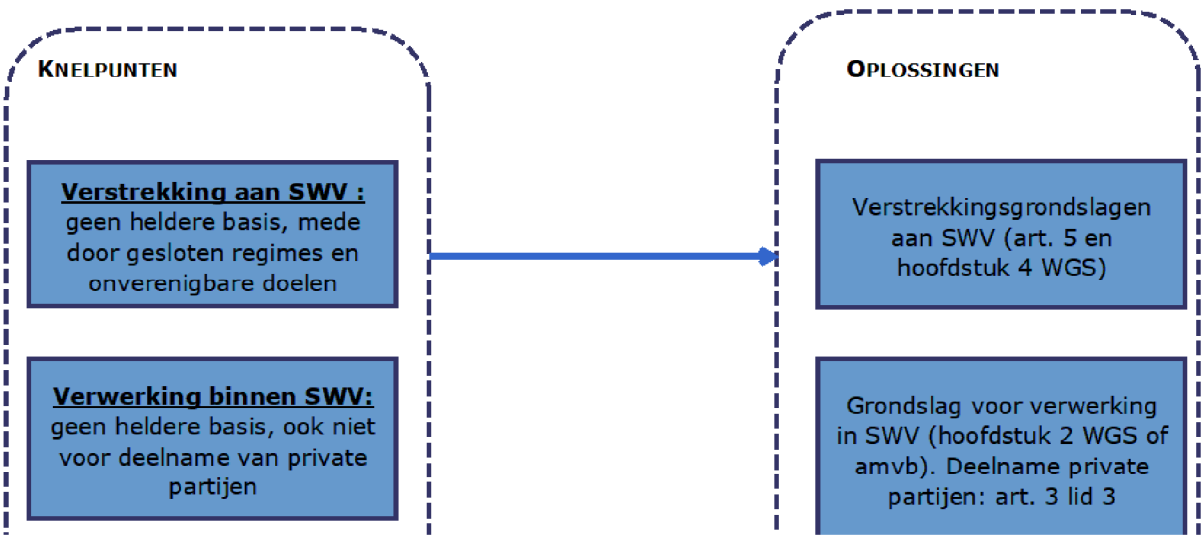
De term "zwaarwegend algemeen belang" is opgenomen omdat, gelet op de mogelijke impact van gezamenlijke verwerking van persoonsgegevens in een samenwerkingsverband voor de persoonlijke levenssfeer van de betrokkene, voorkomen moet worden dat deze gegevens al te gemakkelijk worden gedeeld. Door opname van de term "zwaarwegend algemeen belang" is de regering ertoe gehouden een concrete onderbouwing te geven van de aanwezigheid van een zwaarwegend algemeen belang, dat voor een specifiek samenwerkingsverband de verwerking van persoonsgegevens rechtvaardigt. Hierbij is een belangenafweging vereist tussen het belang dat gediend wordt met de gezamenlijke verwerking van persoonsgegevens en het belang van de persoonlijke levenssfeer van degenen op wie de persoonsgegevens betrekking hebben. Bij deze belangenafweging moeten ook de beginselen van proportionaliteit en subsidiariteit worden betrokken.

Het wetsvoorstel regelt dat een samenwerkingsverband *gezamenlijk* gegevens mag verwerken voor zover dat noodzakelijk is voor een bij of krachtens deze wet vastgesteld doel van zwaarwegend algemeen belang. Dit moet worden beschouwd als een taak van algemeen belang als bedoeld in 6, eerste lid, onder e, van de AVG. Zoals de tekst van het wetsvoorstel impliceert, bestaat de taak uit gegevensverwerking. Daarmee is niet beoogd dat het samenwerkingsverband een geheel op zichzelf staande taak wordt verleend of dat deelnemers er taken bij krijgen; de taak van het samenwerkingsverband is uiteindelijk bedoeld om de behartiging van algemene belangen van één of meer deelnemers te ondersteunen. Een samenwerkingsverband krijgt evenmin bestuursrechtelijke bevoegdheden.

De WGS laat onverlet dat voor een specifiek (type) samenwerkingsverband ook in de toekomst gekozen zou kunnen worden voor regeling daarvan in sectorale wetgeving. In het verleden is dat bijvoorbeeld al gebeurd voor samenwerkingsverbanden ten behoeve van de fraudeaanpak op het terrein van de sociale zekerheid, waarvoor artikel 64 Wet structuur uitvoeringsorganisatie werk en inkomen (hierna: Wet Suwi) een grondslag bevat. Zoals besproken in de vorige subparagraaf is er ook een mogelijkheid om bij amvb's samenwerkingsverbanden onder de reikwijdte van de WGS te brengen, via een bijzondere nahangprocedure. Dit heeft als voordeel dat het kader van de WGS daarvoor een "kapstok" vormt waaraan samenwerkingsverbanden kunnen worden opgehangen. Dat heeft een uniformerende werking en zorgt ervoor dat het niet nodig is voor ieder (type) samenwerkingsverband waarvoor een wettelijke grondslag nodig is, een nieuwe formeelwettelijke grondslag te creëren.

3.3 Oplossing knelpunten in de gegevensverwerking in het kader van samenwerkingsverbanden

In schemavorm kan deze paragraaf als volgt worden ingeleid (SWV = samenwerkingsverband):





Paragraaf 3.3.1 gaat in op het bovenste knelpunt uit het schema en de oplossing, paragrafen 3.3.2 en 3.3.3 behandelen het middelste knelpunt en de oplossing en tot slot gaat paragraaf 3.3.4 in op het laatste knelpunt en de oplossing.

Met de term knelpunten wordt gedoeld op het ontbreken van de voornoemde heldere, passende wettelijke grondslagen die zijn toegesneden op samenwerkingsverbanden. Dit zet een onnodige rem op het optimaal functioneren van samenwerkingsverbanden omdat bepaalde, noodzakelijke vormen van gezamenlijke, domeinoverstijgende gegevensverwerking nu niet mogen plaatsvinden of achterwege worden gelaten omdat er te veel onduidelijkheid bestaat over de grondslagen daarvoor. Dat laat onverlet dat er wettelijke beperkingen aan het verwerken van persoonsgegevens zijn die als waarborg ter bescherming van persoonsgegevens dienen. Dat dergelijke beperkingen soms als knelpunt worden ervaren, doet aan hun waarde niets af.

3.3.1 Verstrekking van gegevens aan een samenwerkingsverband

Een eerste knelpunt dat de WGS beoogt weg te nemen, ligt opgesloten in de bestaande geheimhoudingsbepalingen in combinatie met de vigerende mogelijkheden om gegevens aan derden te verstrekken, die verstrekking van gegevens aan samenwerkingsverbanden als zodanig veelal in de weg staan.

De mate waarin gegevens aan samenwerkingsverbanden kunnen worden verstrekt, wordt sterk bepaald door deze bestaande geheimhoudingsplichten en eventuele uitzonderingen daarop. Geheimhoudingsplichten kunnen zijn ingegeven met het oog op verschillende belangen. Het kan onder meer gaan om bescherming van private belangen (persoonlijke levenssfeer, bedrijfsgeheimen), bescherming van publieke belangen (veiligheid van de staat), bescherming van de bijzondere positie van bepaalde ambten (onschendbaarheid Koning) en de zorg voor de goede werking van het openbaar bestuur (mogelijkheid van intern beraad, geheimhouding van een bepaalde werkwijze, het belang van inspectie, toezicht en controle door bestuursorganen).[7]

Wetten waarin geheimhoudingsplichten zijn opgenomen, bevatten meestal ook bepalingen die de geheimhoudingsplicht doorbreken door mogelijkheden te creëren gegevens – al dan niet onder bepaalde voorwaarden – aan derden te verstrekken. Zoals hiervóór in § 3.1 al naar voren kwam, kennen de meeste sectorale wettelijke regelingen echter geen specifieke mogelijkheden tot verstrekking van gegevens aan samenwerkingsverbanden. Dat lijkt deels toe te schrijven aan het feit dat de gegevensverwerking door samenwerkingsverbanden nu meestal geen heldere juridische status heeft en evenmin een daarvoor in wetgeving omschreven doel van (zwaarwegend)

[7] 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.

algemeen belang. Dit heeft tot gevolg dat men nu veelal moet terugvallen op mogelijkheden tot verstrekking aan individuele partijen. Op basis van deze mogelijkheden moet de noodzaak van verstrekking van gegevens per individuele deelnemer van een samenwerkingsverband worden aangetoond, in plaats van dat dit alleen voor het doel van het verband als geheel behoeft, zoals de Afdeling advisering van de Raad van State verwoordde in haar advies bij het voorstel voor de Wijzigingswet financiële markten 2014 (vgl. Kamerstukken II 2012/13, 33632, nr. 4, blz. 18-19). Aldus houdt de bestaande wetgeving in onvoldoende mate rekening met de behoefte om gegevens aan een samenwerkingsverband als zodanig te kunnen verstrekken om deze gegevens voor het doel waarvoor dat verband in het leven is geroepen, gezamenlijk te verwerken in de vorm van bijvoorbeeld een gezamenlijke casus-analyse of een gezamenlijke data-analyse.

Aan deze behoefte wordt tegemoetgekomen door in dit wetsvoorstel de mogelijkheid te scheppen om aan de gegevensverwerking door samenwerkingsverbanden waarvoor deze behoefte geldt, een heldere wettelijke basis te geven. Dit geschiedt allereerst door bij of krachtens de WGS samenwerkingsverbanden aan te wijzen waarop de WGS van toepassing is. Het dient daarbij te gaan om samenwerkingsverbanden waarbinnen gegevens worden verwerkt voor de vervulling van een bij of krachtens de wet vastgesteld doel van zwaarwegend algemeen belang. Daarnaast schrijft het wetsvoorstel voor dat elke deelnemer aan een samenwerkingsverband dat onder de WGS valt, daaraan gegevens verstrekt die tot de bij of krachtens de WGS aangewezen categorieën behoren, voor zover dat noodzakelijk is voor de vervulling van het doel van het samenwerkingsverband, tenzij naar het oordeel van de deelnemer zwaarwegende redenen zich daartegen verzetten. Daardoor is het niet alleen niet langer nodig om de noodzaak van de verstrekking per individuele deelnemer aan te tonen, maar wordt ook de basis gelegd om de verstrekte gegevens gezamenlijk te kunnen verwerken (zie § 3.3.2).

Met dit voorschrift wijkt het wetsvoorstel af van het standpunt dat het kabinet eerder in zijn brief uit 2014 heeft ingenomen. In die brief ging het kabinet ervan uit dat de grondslagen voor verstrekking aan samenwerkingsverbanden als bedoeld in de kaderwet uitsluitend in de sectorale wetgeving zouden worden opgenomen. Daarbij speelde op de achtergrond de gedachte dat het aldus mogelijk zou zijn in iedere betrokken wet en daarop berustende bepalingen op het punt van uitzonderingen en voorwaarden maatwerk te leveren, waarbij rekening zou kunnen worden gehouden met de specifieke belangen die aan de geheimhoudingsplicht in de desbetreffende wet zijn verbonden. Nu er echter voor gekozen is de aanwijzing van een samenwerkingsverband dat onder de WGS valt niet bij convenant, maar bij wet of amvb te laten plaatsvinden, is er ook ruimte om daarin nadere voorwaarden en beperkingen aan de verstrekking te stellen. Overigens geeft de WGS voor verstrekking van gegevens slechts een grondslag, voor zover sectorale wetten daarvoor ruimte laten, bijvoorbeeld door te bepalen dat bij wettelijk voorschrift van een eventueel gesloten verstrekkingenregime in die wet kan worden afgeweken. Voor zover die ruimte er niet is, dient in de sectorale wet zelf een grondslag voor verstrekking te worden opgenomen. De algemene grondslag voor verstrekking van gegevens die in de WGS wordt opgenomen, staat er niet aan in de weg dat in specifieke sectorale wetten een zelfstandige grondslag voor verstrekking wordt opgenomen. Met het oog op het specifieke karakter van strafrechtelijke gegevens gebeurt dat bijvoorbeeld in de Wet politiegegevens (hierna: Wpg) en de Wet justitiële en strafvorderlijke gegevens (hierna: Wjsg). Een zelfstandige grondslag voor verstrekking wordt ingevolge dit wetsvoorstel verder gecreëerd in de Wet op het financieel toezicht, de Wet toezicht accountsorganisaties, de Wet toezicht trustkantoren 2018 en de Wet ter voorkoming van witwassen en financieren van terrorisme, de Sanctiewet 1977, de Wet toezicht financiële verslaggeving en de Wet handhaving consumentenbescherming.

Gekozen is voor een verstrekkingsplicht en niet voor een verstrekkingsbevoegdheid. Daarmee wil het kabinet benadrukken dat de samenwerking niet vrijblijvend kan zijn. Die verstrekkingsplicht is niet absoluut. Integendeel, de WGS bevat verschillende elementen waaruit blijkt dat de deelnemers een hoge mate van autonomie behouden:

- De deelnemers zijn gezamenlijk verwerkingsverantwoordelijke en in die zin ook gezamenlijk opdrachtgever. Dit impliceert dat een deelnemer mede bepaalt voor welke opdrachten gegevens moeten worden aangeleverd en uit dien hoofde ook opdrachten kan tegenhouden.
- De vraag welke gegevens een deelnemer als noodzakelijke gegevens in de zin van artikel 5 dient te verstrekken, is exclusief ter beantwoording van de deelnemer zelf.
- De deelnemer kan, ook al is hij van oordeel dat de verstrekking van gegevens op zich noodzakelijk is voor het doel van het samenwerkingsverband, besluiten om daar wegens zwaarwegende redenen van af te zien (artikel 5, eerste lid).
- Op de verplichting om gegevens te verstrekken kunnen op grond van artikel 8, eerste lid, bij amvb voorwaarden en beperkingen worden gesteld.

Het kabinet meent aldus een gebalanceerde uitvoering te hebben gegeven aan het eerder al voor de gegevensuitwisseling verwoorde uitgangspunt van "ja, tenzij".

Met betrekking tot de verstrekking van persoonsgegevens aan een samenwerkingsverband laat de praktijk nog een ander knelpunt zien. Dit knelpunt ligt opgesloten in het vereiste dat het doel van deze verstrekking in beginsel verenigbaar dient te zijn met het doel waarvoor de gegevens oorspronkelijk zijn verzameld.[8] De gedachte hierachter is dat, zoals de Afdeling advisering van de Raad van State aanhaalt in haar advies, dat een burger van wie persoonsgegevens voor een bepaald doel worden verzameld, er in beginsel niet op bedacht hoeft te zijn dat gegevens door een andere instantie dan waarmee hij contact heeft gehad, voor een heel ander doel worden gebruikt. Het principe van doelbinding is naar het oordeel van het kabinet één van de belangrijkste principes in het gegevensbeschermingsrecht en dient daarom ook voor samenwerkingsverbanden het uitgangspunt te blijven. Wel is het wenselijk om, indien daartoe een duidelijke noodzaak bestaat, ruimte te scheppen voor een samenwerkingsverband waaraan deelnemers persoonsgegevens verstrekken voor een ander doel dan waarvoor zij deze hebben verzameld, ook als dit onverenigbaar is met dat oorspronkelijke doel. Samenwerkingsverbanden stuiten namelijk soms op het probleem dat een verstrekking van gegevens aan dat verband door een van de deelnemers en de verwerking daarvan binnen het verband in onvoldoende mate beantwoordt aan dit principe van doelbinding. Dit principe kan op gespannen voet staan met het uitgangspunt van de integrale, multidisciplinaire benadering door een samenwerkingsverband.
Daarmee is niet gezegd dat het wenselijk is dit principe voor samenwerkingsverbanden in de zin van de WGS te allen tijde buiten toepassing te laten. De grondslagen voor verwerking van persoonsgegevens bij of krachtens de WGS zijn gericht op een doel van zwaarwegend algemeen belang dat niet op voorhand verenigbaar is met de doelen waarvoor de deelnemers de te verstrekken gegevens hebben verzameld.
Artikel 6, vierde lid, aanhef, AVG bepaalt dat de verwerking voor een ander, onverenigbaar, doel mag als dat een basis heeft in het lidstatelijk recht (dus de WGS). Het lidstatelijk recht moet dan wel één van de belangen van artikel 23, eerste lid, AVG beschermen. De bij de WGS toepasselijke onderdelen van artikel 23, eerste lid, AVG, zijn:
c) de openbare veiligheid;
d) de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
e) andere belangrijke doelstellingen van algemeen belang van de Unie of van een lidstaat, met name een belangrijk economisch of financieel belang van de Unie of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid.

De WGS bewerkstelligt dat verstrekking van persoonsgegevens door een deelnemer aan het samenwerkingsverband voor het doel van dat verband, niet verenigbaar hoeft te zijn met de oorspronkelijke doeleinden waarvoor de persoonsgegevens worden verwerkt.

3.3.2 Verwerking van gegevens binnen een samenwerkingsverband

[8] Zie artikel 5, eerste lid, onder b, AVG.

Omdat de gegevensverwerking binnen een samenwerkingsverband meestal geen heldere wettelijke grondslag heeft, betekent het feit dat een wettelijke regeling de mogelijkheid geeft om gegevens aan bepaalde partijen te verstrekken, nog niet dat die gegevens ook binnen een samenwerkingsverband van die partijen mogen worden uitgewisseld. De desbetreffende partijen mogen deze gegevens slechts verstrekken in een één-op-één relatie met de in de wet genoemde partijen. Ieder van deze partijen is vervolgens gehouden deze gegevens vertrouwelijk te behandelen. Deze eis staat in beginsel in de weg aan gegevensuitwisseling binnen een samenwerkingsverband, zoals de Raad van State eerder heeft opgemerkt in haar advies over een wetsvoorstel dat tot de Wijzigingswet financiële markten 2014 heeft geleid (vgl. Kamerstukken II 2012/13, 33632, nr. 4, blz. 18-19). Het gevolg daarvan is dat er thans slechts suboptimale mogelijkheden zijn om binnen een samenwerkingsverband gegevens in een gemeenschappelijk informatiesysteem te verwerken ten behoeve van een gezamenlijk casusoverleg of een gezamenlijke data-analyse en de uitkomsten daarvan in dat systeem vast te leggen. Het wetsvoorstel lost dit knelpunt op door een expliciete grondslag te geven voor de verwerking van gegevens binnen een samenwerkingsverband dat onder de WGS valt.

Voor zover het om data-analyses in samenwerkingsverbanden gaat, speelt er nog een ander knelpunt. Afhankelijk van het doel waarvoor zij zijn opgericht, mogen samenwerkingsverbanden thans op basis van gegevens van de deelnemers bepaalde patronen zichtbaar maken die op bijvoorbeeld fraude duiden, of groepsprofielen opstellen van bijvoorbeeld beroepsfraudeurs. Zij kunnen daartoe gebruikmaken van de mogelijkheid om ten behoeve van wetenschappelijk onderzoek en statistiek persoonsgegevens te verwerken. Deze mogelijkheid houdt in dat verwerking van gegevens voor wetenschappelijke en statistische doeleinden als niet onverenigbaar wordt beschouwd met het oorspronkelijke doel waarvoor de desbetreffende gegevens zijn verzameld.[9] Ook geldt bij verwerking van persoonsgegevens ten behoeve van wetenschappelijk onderzoek of statistiek niet het verbod om zgn. bijzondere categorieën van persoonsgegevens te verwerken.[10] Hetzelfde geldt met betrekking tot de verwerking van strafrechtelijke gegevens.[11]

Een en ander laat een individuele deelnemer aan een samenwerkingsverband voldoende ruimte om wanneer er in het samenwerkingsverband sprake is van geautomatiseerde gege-vensanalyse, de blootgelegde patronen en de groepsprofielen die hij van het samenwerkingsverband heeft ontvangen, te gebruiken om deze binnen de grenzen van zijn wettelijke taken en bevoegdheden te matchen met gegevens waarover hijzelf rechtmatig beschikt, om daaruit bijvoorbeeld lijsten te destilleren van personen die bepaalde risico's op het desbetreffende taakgebied vertonen. Dat is niet anders dan dat hij dergelijke lijsten opstelt aan de hand van patronen en profielen die op basis van meer "klassiek" wetenschappelijk onderzoek tot stand zijn gebracht. Wat op dit moment echter niet is toegestaan is dat samenwerkingsverbanden op basis van de door de deelnemers verstrekte persoonsgegevens gemeenschappelijke data-analyses verrichten die tot lijsten leiden van personen aan wie bepaalde risico's zijn verbonden, als het doel van deze analyse niet verenigbaar is met de doelen waarvoor de desbetreffende gegevens zijn verzameld. Omdat het dan om een verwerking voor operationele doeleinden zou gaan, kunnen de eerder bedoelde mogelijkheden van gegevensverwerking voor wetenschap en statistiek, met inbegrip van de mogelijkheid om voor onverenigbare doelen te verwerken, daarvoor geen basis bieden.[12] Als voor het onderzoek of de statistiek strafrechtelijke

[9] Verwezen zij naar artikel 5, eerste lid, onder b, AVG.
[10] Zie artikel 9, tweede lid, onder j, AVG en artikel 24 UAVG. Bijzondere persoonsgegevens betreffen persoonsgegevens met betrekking tot (onder meer) iemands ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, seksueel gedrag of seksuele gerichtheid.
[11] Zie daarover artikel 32, onder f, UAVG. Zie voorts artikel 33, eerste lid, onder a, UAVG, op grond waarvan het verbod van verwerking van strafrechtelijke persoonsgegevens niet geldt, indien de verwerkingsverantwoordelijke de gegevens heeft verkregen krachtens de Wpg of de Wjsg. Dat geldt ook voor verkrijging van gegevens die op grond van artikel 22 Wpg, artikel 15 Wjsg of artikel 39g Wjsg voor wetenschappelijk onderzoek en statistiek zijn verstrekt.
[12] De voormalige Artikel 29 werkgroep - inmiddels opgevolgd door het Europees Comité voor

gegevens worden verwerkt die op grond van de Wpg en Wjsg zijn verstrekt, geldt bovendien expliciet dat de resultaten van de verwerking geen persoonsgegevens mogen bevatten.[13] Een en ander brengt mee dat zo'n subjectgerichte data-analyse aan alle algemene voorwaarden voor gegevensverwerking moet voldoen, met inbegrip van de eisen rond doelbinding en met inachtneming van de verboden om bijzondere categorieën van persoonsgegevens of strafrechtelijke gegevens te verwerken.

Dit beperkt de mogelijkheden om in samenwerkingsverbanden met moderne analysetechnieken bepaalde risico's met betrekking tot individuele personen in beeld te brengen. Zo kan de Infobox Crimineel en Onverklaarbaar Vermogen (iCOV)[14] de door haar ontwikkelde profielen niet matchen met de haar ter beschikking staande gegevens om een lijst te genereren van personen met een groot risico dat zij fraude (gaan) plegen of geld witwassen. Eenzelfde knelpunt heeft zich destijds voorgedaan bij het project FinPro. In antwoord op Kamervragen over dat project heeft het kabinet dan ook de conclusie getrokken dat op dit moment een heldere basis ontbreekt voor het gebruik van de uitkomsten van moderne analysetechnieken door samenwerkingsverbanden ten behoeve van de uitvoering van de wettelijke taken van de deelnemers.[15] Immers, de basis die men daarvoor thans gebruikt, is het regime voor wetenschap en statistiek en op grond daarvan is verwerking van persoonsgegevens ten behoeve van operationele doeleinden niet mogelijk.

Bij of krachtens de WGS zal, afhankelijk van het doel van een bepaald (type) samenwerkingsverband, nader vastgesteld moeten worden welke wijzen van verwerking door dat verband worden toegestaan. Dat kan het uitvoeren van een gemeenschappelijke casusanalyse zijn. Het kan ook gaan om gemeenschappelijke data-analyses waarmee patronen worden blootgelegd of groepsprofielen worden opgesteld, teneinde aan de hand daarvan 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. Het is tegen deze achtergrond dat dit wetsvoorstel een duidelijke grondslag beoogt te geven voor het aldus verwerken van gegevens.

De behoefte aan voldoende mogelijkheden om in samenwerkingsverbanden gemeenschappelijke casusanalyses of data-analyses te kunnen verrichten, voor het doel van het samenwerkingsverband, is evident. Dergelijke analyses leveren immers doorgaans betere informatie op dan analyses die een individuele deelnemer aan het verband op grond van louter zijn eigen gegevens kan maken. Daarmee ontstaat een betere basis om deelnemers op een op elkaar afgestemde wijze binnen de bestaande eigen taken en bevoegdheden te laten optreden. Overigens wordt er hier nog op gewezen dat de uitkomst van een analyse binnen een samenwerkingsverband waaraan opsporingsdiensten en het OM deelnemen, onder de voorgestelde WGS weliswaar tot een lijst kan leiden met bijvoorbeeld personen die een verhoogd risico op het zijn van beroepsfraudeur laten zien, maar nog geen formele verdenking oplevert in de zin van artikel 27 van het Wetboek van Strafvordering. Zeker als zo'n lijst met behulp van Big Data technologie louter correlatieve en geen causale verbanden laat zien, kan van een formele verdenking (nog) geen sprake zijn. Daarvoor dienen concrete feiten en omstandigheden met betrekking tot de desbetreffende persoon op tafel te komen die op fraude wijzen.

3.3.3 Verwerking van gegevens met private partijen

---

gegevensbescherming – hanteert in dit verband het principe van functionele scheiding: "This means that data used for statistical purposes or other research purposes should not be available to 'support measures or decisions' that are taken with regard to the individual data subjects concerned (unless specifically authorized by the individuals concerned)." Zie hoofdstuk III.2.3 van Opinion 03/2013 on purpose limitation (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf).

[13] Zie artikel 22 Wpg en de artikelen 15 en 39g Wjsg.

[14] iCOV is een samenwerkingsverband van onder meer de Belastingdienst, de Douane, de FIOD, de politie, FIU Nederland en het OM.

[15] Aanhangsel Handelingen II 2015/16, nr. 3413.

Publiek-private samenwerking kan beide kanten voordelen opleveren. Er zit veel kennis over nieuwe ontwikkelingen, risico's en technologieën bij het bedrijfsleven en ook kunnen private partijen over informatie beschikken die voor een integrale aanpak van maatschappelijke vraagstukken van belang is. Zowel de private partij als de publieke partij kan op basis van uitgewisselde informatie actie ondernemen of een interventie plegen die bijdraagt aan het voorkomen en bestrijden van criminaliteit. In het rapport van de Werkgroep Verkenning kaderwet gegevensuitwisseling werden de volgende voorbeelden van publiek-private verbanden genoemd: energiebedrijven bij de aanpak van hennepkwekerijen, financiële dienstverleners bij het tegengaan van witwassen en transportondernemingen bij de handel in verboden goederen.

Een voorbeeld van een samenwerkingsverband waarin publiek-private samenwerking van eminent belang is, is het Financieel Expertise Centrum (FEC)[16]. Sommige FEC-partners werken dan ook al enige jaren samen met de bankensector. Zij doen dit vanuit de visie dat de integriteit van de financiële sector niet slechts een zaak is van de overheid. Zo hebben financiële instellingen een belangrijke poortwachtersfunctie in het kader van het voorkomen van witwassen en financieren van terrorisme. In een brief van 21 juli 2017 aan de Minister van Veiligheid en Justitie hebben de FEC-partners, de betrokken banken[17] en de Nederlandse Vereniging van Banken (NVB) aangegeven een nauwere samenwerking als een belangrijke stap te zien om financieel-economische criminaliteit efficiënter en effectiever te bestrijden en de integriteit van de financiële markten te versterken. Deze behoefte aan nauwere samenwerking stuit evenwel, zo blijkt uit de brief, op een aantal belemmeringen in de mogelijkheden om met elkaar gegevens uit te wisselen. Zo kunnen in het kader van het voorkomen van witwassen, terrorismefinanciering of bepaalde vormen van fraude, de bij de bank opgegeven gegevens niet worden getoetst bij publieke partijen. Als gevolg daarvan ontbreekt een integraal en volledig inzicht op zowel subjectniveau als op het gebied van het vaststellen van specifieke indicatoren in het algemeen voor het herkennen van financieel-economische criminaliteit. Hiermee vergelijkbare problemen zien we in de relatie tussen toezichthouders en private partijen die willen samenwerken en daartoe gegevens uitwisselen. De oorzaak van deze problemen ligt in het feit dat sectorale wetten veelal geen op samenwerkingsverbanden toegesneden grondslagen bevatten voor verstrekking van gegevens aan private partijen die aan samenwerkingsverbanden (willen) deelnemen, en voor een gezamenlijke verwerking binnen deze verbanden in de vorm van casus-analyses of data-analyses.

Het wetsvoorstel lost dit knelpunt op door in de WGS ruimte te bieden voor samenwerkingsverbanden waaraan ook private partijen deelnemen. Bij of krachtens de WGS kan dan voor een bepaald (type) samenwerkingsverband worden bepaald dat daaraan ook door een of meer met name genoemde private partijen wordt deelgenomen. Daarbij geldt dan uiteraard dat de deelname daarvan dient te worden getoetst aan de voorwaarde dat deelname noodzakelijk is voor de uitoefening van het doel van zwaarwegend algemeen belang waarvoor het samenwerkingsverband wordt aangewezen. Door het creëren van ruimte voor deelname van private partijen geldt vervolgens dat, indien aan een samenwerkingsverband krachtens de WGS ook een private partij deelneemt, dan ook de grondslagen gelden voor verstrekking van gegevens aan dat verband, de verwerking daarvan binnen het verband en de grondslagen voor verstrekking uit dat verband van resultaten van de verwerking. Op deze wijze kunnen zowel overheidsinstanties als private partijen die aan dergelijke samenwerkingsverbanden deelnemen, daaraan gegevens verstrekken en kan het verband deze verwerken tot voor een deelnemer noodzakelijke informatie. Tegen deze achtergrond wijst het kabinet er graag op dat de FEC-partners, de betrokken banken en de NVB in hun brief van 21 juli 2017 het belang benadrukken dat zij hechten aan de totstandkoming van een WGS.

[16] Het FEC is een samenwerkingsverband tussen autoriteiten met een toezicht-, controle-, vervolgings- of opsporingstaak in de financiële sector en is opgericht om de integriteit van deze sector te versterken. Deelnemers aan het FEC zijn: Autoriteit Financiële Markten (AFM), Belastingdienst, De Nederlandsche Bank (DNB), Financial Intelligence Unit - Nederland (FIU), Fiscale Opsporingsdienst (FIOD), Openbaar Ministerie (OM) en Politie.
[17] ABN AMRO Bank, Rabobank, Volksbank en ING Bank.

Overigens biedt de WGS een basis om bij of krachtens de wet nadere voorwaarden en beperkingen te stellen aan de verstrekking aan en verdere verwerking van persoonsgegevens ten behoeve van dit verband. Aldus kan rekening worden gehouden met de specifieke belangen van overheidsinstanties die aan het verband deelnemen, om bepaalde gegevens niet of slechts onder voorwaarden aan dit verband te verstrekken en te laten verwerken. Dat kan vooral van belang zijn voor samenwerkingsverbanden waaraan ook private partijen deelnemen.

3.3.4 Verstrekking van de resultaten van de verwerking uit een samenwerkingsverband

De gezamenlijke verwerking van gegevens binnen een samenwerkingsverband zal informatie – die nodig is voor diens doel van zwaarwegend algemeen belang – opleveren die elke deelnemer afzonderlijk nooit zou kunnen genereren. De hoeveelheid van relevante gegevens en de variëteit aan invalshoeken die deze kennen, zal bij een samenwerkingsverband immers aanmerkelijk groter zijn dan die van de deelnemers afzonderlijk. Daardoor kunnen bijvoorbeeld risico-taxaties worden uitgevoerd met betrekking tot personen of fenomenen die een veel completer beeld daarvan opleveren dan in het geval dat zo'n risico-taxatie uitsluitend op basis van eigen gegevens zou worden verricht.

Omdat de gegevensverwerking door een samenwerkingsverband meestal geen heldere wettelijke grondslag heeft, is echter de basis om het verband de informatieproducten die het genereert, aan deelnemers of aan derden te laten verstrekken, eveneens niet helder of onduidelijk. Nu aan de gegevensverwerking door samenwerkingsverbanden die op grond van de WGS zijn aangewezen, een heldere wettelijke grondslag wordt toegekend, kan de WGS ook een duidelijke basis bieden voor de verstrekking van dergelijke producten aan deelnemers of aan derden. De WGS voorziet daarin door te bepalen dat het samenwerkingsverband de hier be-doelde informatieproducten aan de deelnemers van het verband verstrekt, voor zover verstrekking van deze resultaten noodzakelijk is voor de vervulling van een publiek-rechtelijke taak die aan de deelnemer is opgedragen, wanneer deze verenigbaar is met het doel van het samenwerkingsverband, of indien het een private deelnemer zonder publiekrechtelijke taak betreft, ten behoeve van de behartiging van de ge-rechtvaardigde belangen of wettelijke verplichtingen van deze private deelnemer, wanneer deze verenigbaar zijn met het doel van het samenwerkingsverband.

Verstrekking van het resultaat aan een derde is niet mogelijk, tenzij dat specifiek bij of krachtens de WGS is bepaald en is voldaan aan de voorwaarden van artikel 7, tweede lid.

Met betrekking tot de verstrekking van de resultaten van de verwerking uit een samenwerkingsverband verdient de verstrekking daarvan aan opsporingsdiensten en OM nog bijzondere aandacht. Voor het bestuursrechtelijke en het strafrechtelijke domein gelden immers 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 soms hand in hand kunnen gaan met opsporing en vervolging. In dat verband is van belang dat opsporingsdiensten en OM een groeiende behoefte hebben om in samenwerkingsverbanden aan informatie te komen die hen in een fase waarin nog geen sprake van een (vermoeden van een) strafbaar feit en van een mogelijke verdachte is, kan helpen bij het signaleren van trends en het maken van analyses om de criminaliteit beter te kunnen bestrijden. Het kan daarbij onder meer gaan om analyses in een concrete casus, waarbij partijen gezamenlijk bepalen welke interventies de meest geschikte zijn om in de desbetreffende casus uit te voeren. Voor opsporingsdiensten en OM kan dat betekenen dat men op basis van de verkregen informatie een opsporingsonderzoek start. Het kan ook gaan om een situatie die een meer proactief of

preventief karakter heeft. Te denken valt aan het uitvoeren van een gemeenschappelijke data-analyse op grond waarvan de deelnemers het risico taxeren dat bepaalde personen fraude plegen. Overigens wordt hier, zoals dat ook in § 3.3.2 al is gedaan, er nadrukkelijk op gewezen dat de uitkomst van een analyse binnen een samenwerkingsverband waaraan opsporingsdiensten of OM deelnemen, onder de voorgestelde WGS weliswaar tot een lijst kan leiden met bijvoorbeeld personen die een verhoogd risico op bijvoorbeeld witwassen laten zien, maar nog geen verdenking oplevert. Aldus geeft het wetsvoorstel een betere basis voor het verstrekken van informatieproducten aan OM en opsporingsdiensten uit een samenwerkingsverband waaraan zij deelnemen, in een fase waarin (nog) geen verdenking bestaat. Die blijkt nodig te zijn, omdat soms onvoldoende helder leek te zijn of en, zo ja, in welke omstandigheden opsporingsdiensten en OM op rechtmatige wijze dergelijke informatieproducten kunnen krijgen.[18]

3.4 Waarborgen

Met het oog op een rechtmatige en behoorlijke verwerking van persoonsgegevens door samenwerkingsverbanden als bedoeld in de WGS is het van essentieel belang dat deze verwerking met de nodige waarborgen is omringd.

Deze waarborgen zijn voor een belangrijk deel al verankerd in bestaande wetgeving, zoals die ook geldt voor gegevensverwerking door samenwerkingsverbanden die niet onder de WGS vallen. Het gaat in de eerste plaats om de beginselen die in artikel 5 AVG zijn vastgelegd: rechtmatigheid, behoorlijkheid, transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid, alsmede de verantwoordingsplicht van de verwerkingsverantwoordelijke. Verder kan worden gewezen op de rechten die betrokkenen hebben: het recht op inzage, rectificatie, wissing van gegevens, beperking van de verwerking en bezwaar.[19] Tot slot valt te wijzen op de verplichtingen die voor de verwerkingsverantwoordelijken gelden, zoals de informatieverplichtingen, de verplichting tot gegevensbescherming door ontwerp en door standaardinstellingen, de verplichting tot het bijhouden van een register van de verwerkingsactiviteiten en de verplichting tot beveiliging van de verwerking.[20]

Met betrekking tot de verplichting om betrokkenen te informeren over hen betreffende verwerkingen van persoonsgegevens wordt erop gewezen dat deze niet van toepassing is indien de uitzonderingen op grond van artikel 13 of 14 AVG opgaan of op grond van de algemene uitzonderingsbepaling van artikel 23 AVG, dat is uitgewerkt in artikel 41 Uitvoeringswet AVG. In beide situaties zoals geregeld in artikel 13 en 14 AVG geldt dat de informatie niet hoeft te worden verstrekt als de betrokkene al over de informatie beschikt. Als de persoonsgegevens niet van de betrokkene zelf worden verkregen, zijn er meer uitzonderingsmogelijkheden: op grond van artikel 14, vijfde lid, AVG kan informatieverstrekking door de verwerkingsverantwoordelijke achterwege blijven:

- als het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen of indien het verstrekken van de informatie de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen (artikel 14, vijfde lid, onderdeel b). In het geval van de WGS is onder meer deze laatste uitzondering van belang;
- als het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven bij een wet die op de verwerkingsverantwoordelijke van toepassing is en die voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen (artikel 14, vijfde lid, onderdeel c). In het geval van de door de WGS verplichte verstrekking van gegevens door deelnemers aan het

[18] Dit blijkt onder meer uit een brief van 4 juni 2012 van de toenmalige [redacted] van het College van Procureurs-Generaal aan de toenmalige Minister van Veiligheid van Justitie waarin hij verzocht de wetgeving zo aan te passen dat een verstrekking van gegevens binnen een samenwerkingsverband mogelijk is zonder dat daaraan een vordering op grond van het stelsel van strafvorderlijke bevoegdheden ten grondslag ligt.
[19] Zie de artikelen 15 tot en met 18 en 21 AVG.
[20] Zie de artikelen 12 tot en met 14, 25, 30 en 32 tot en met 34 AVG.

samenwerkingsverband is deze uitzondering van toepassing in de gevallen waarin anderszins passende maatregelen worden getroffen;
- als de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van Unierecht of lidstatelijk recht, waaronder een wettelijke geheimhoudingsplicht (artikel 14, vijfde lid, onder d, AVG).

In aanvulling op de hier genoemde waarborgen bevat de WGS verspreid over een aantal artikelen verschillende waarborgen voor de verwerking van persoonsgegevens door samenwerkingsverbanden als bedoeld in de WGS. Hierbij is in aanmerking genomen dat in een samenwerkingsverband gegevens worden verwerkt die afkomstig zijn van verschillende deelnemers. Iedere deelnemer die bij of krachtens de WGS gedefinieerde gegevens verstrekt, heeft die eerder verzameld, geanalyseerd en gebruikt voor eigen doeleinden. De aard en inhoud van die te verstrekken gegevens, de context waarbinnen die worden gebruikt en de beoordeling daarvan verschilt per deelnemer. De mogelijkheden voor een samenwerkingsverband tot verwerking van die uit onderscheidenlijke bronnen verkregen gegevens met ieder een eigen achtergrond en doel, zijn ook om die reden voorzien van waarborgen.

Verwerking is uitsluitend toegestaan voor zover dat noodzakelijk is voor de vervulling van het doel van het desbetreffende samenwerkingsverband. Dat doel moet bij of krachtens de WGS worden omschreven. De toetsing aan het vereiste van noodzakelijkheid van verwerking voor die taak houdt in dat aan de eisen die artikel 8, tweede lid, van het EVRM aan verwerking stelt, moet zijn voldaan (zie hierna nader onder § 7). Bij of krachtens de WGS worden regels gesteld omtrent de wijze waarop het samenwerkingsverband gegevens kan verwerken. De wijze van verwerking omvat niet enkel het aggregeren van gegevens, maar ook het analyseren en beoordelen daarvan. Het bepalen van de wijze van verwerking omvat daarmee verschillende fases van verwerking. Het betreft criteria waaraan bij verwerking moet worden voldaan of welke methode voor verwerking moet worden toegepast. Bij die vaststelling is een belangrijk uitgangspunt dat toepassing van criteria of een methode niet tot discriminatie of andere ongewenste uitkomsten zal leiden. Ook dient inzicht te bestaan in herkomst, doel, actualiteit, betrouwbaarheid en totstandkoming van uit verschillende bronnen verkregen gegevens die een gemeenschappelijke verwerking ondergaan. Door de wijze van verwerking te regelen, biedt dit waarborgen voor het op verantwoorde en behoorlijke wijze verwerken van gegevens binnen een samenwerkingsverband. Er kan bij de vaststelling van de wijze van verwerking voorts rekening worden gehouden met inherente verschillen tussen de verwerking van persoonsgegevens en andere dan persoonsgegevens, zoals bedrijfsgegevens die niet tot een natuurlijke persoon zijn te herleiden. Ook de mogelijkheid om bijvoorbeeld risicoprofielen te kunnen vastleggen, is uitsluitend mogelijk bij of krachtens de WGS.

Daarnaast bevat de WGS ook een artikel dat specifiek betrekking op waarborgen heeft (artikel 8). Ingevolge dat artikel kunnen bij amvb nadere voorwaarden en beperkingen te worden gesteld aan alle verwerkingen van gegevens op grond van deze wet, met inbegrip van de verstrekking van gegevens aan het samenwerkingsverband, en aan verstrekkingen van gegevens op grond van een andere wet aan een samenwerkingsverband.

In het voorgestelde artikel 8 is voorts voorzien in een aantal specifieke waarborgen:
- een systeem van autorisaties, dat wil zeggen de verlening van toegang tot de systemen waarin de samenwerkingsverbanden gegevens verwerken aan uitsluitend door de deelnemers geautoriseerde medewerkers;
- een verplichting tot screening van medewerkers;
- het verplichting tot het loggen van gegevens die noodzakelijk zijn voor controle en toezicht;
- een verplichting tot het instellen van een rechtmatigheidsadviescommissie die de rechtmatigheid van de verwerking van persoonsgegevens door het samenwerkingsverband beoordeelt;
- een vernietigingstermijn;

- een adequaat beveiligingsniveau, ten minste overeenkomstig richtlijnen van de minister van BZK. Bij dat laatste kan worden gedacht aan de Baseline Informatiebeveiliging Overheid (BIO), die de ministerraad op 14 december 2018 heeft vastgesteld voor het Rijk en in het interbestuurlijk verkeer met het Rijk. De BIO is een gemeenschappelijk normenkader, gebaseerd op de internationale norm ISO 27001/2 voor de beveiliging van de informatie(systemen) van de overheid en bevat een concretisering van een aantal normen tot verplichte overheidsmaatregelen.

Bij geautomatiseerde gegevensanalyse regelt artikel 8a tevens de volgende waarborgen:

- de verplichting zorg te dragen voor adequate en uniforme technische en organisatorische maatregelen voor de bevordering van de kwaliteit van de gezamenlijke geautomatiseerde gegevensanalyse en de bevordering van de juistheid en de volledigheid van de gegevens die daarbij worden verwerkt; afhankelijk van het samenwerkingsverband en het type data-analyse kan het daarbij bijvoorbeeld gaan om het testen van te gebruiken algoritmes op basis van test cases of scenario's en het hanteren van standaardmethodieken van werken, zoals CRISP DM (Cross Industry Standard Process for Data Mining).
- de plicht tot inhoudelijke tussenkomst van de rechtmatigheidsadviescommissie bij de verstrekking van een resultaat van geautomatiseerde gegevensanalyse, die zich vergewist van de zorgvuldige totstandkoming van het resultaat;
- de verplichting om op een voor het publiek toegankelijke wijze uitleg te geven over de gehanteerde patronen en indicatoren of andere onderliggende logica, tenzij volgens een deelnemer zwaarwegende redenen zich daartegen verzetten;
- de verplichting tot terugmelding van onjuistheden in bronbestanden.

Daarnaast verdienen de volgende waarborgen hier vermelding:

- de verplichting tot een periodiek privacy audit (artikel 8b);
- de verplichting om een jaarverslag uit te brengen (artikel 9a);
- de verplichting voor ontvangers van resultaten van de gegevensverwerking van het samenwerkingsverband om terug te koppelen wat de effectiviteit en bruikbaarheid van de resultaten was (artikel 7). De deelnemers van het samenwerkingsverband evalueren hiermee de gehanteerde werkwijze. Om bij te dragen aan de kwaliteit van de gegevens is het van belang dat er een terugkoppeling moet zijn: wat wordt gedaan met de meldingen die zijn gedaan met gebruikmaking van bijvoorbeeld data-analysetechnieken? Hebben die daadwerkelijk witwasconstructies aan het licht gebracht of waren het onterechte meldingen? Deze feedback is nodig om te toetsen of de gegevensverwerking noodzakelijk en effectief is. Feitelijk is dit een kwaliteitscirkel. Een constante aanscherping van de werkwijze, en, indien van toepassing de gehanteerde patronen en indicatoren, is wezenlijk;
- de verplichting om voldoende en gekwalificeerd personeel aan te wijzen voor het samenwerkingsverband;
- de verplichting om bij amvb een contactpunt voor betrokkenen aan te wijzen en om bij amvb regels te stellen over de werkwijze en de respectieve verantwoordelijkheden van de deelnemers (artikel 4);
- de verplichting om categorieën van persoonsgegevens die deelnemers aan het samenwerkingsverband moeten verstrekken, bij of krachtens de WGS aan te wijzen. Dit draagt bij aan de transparantie van de gegevensverwerking (artikel 5).
- de geheimhoudingsplicht (artikel 9): ook schrijft de WGS voor dat de verwerkingsverantwoordelijken jegens derden verplicht zijn tot geheimhouding van de informatie die uit uitgevoerde analyses voortkomt behoudens voor zover de verstrekking van resultaten is toegestaan (artikel 7), enig ander wettelijk voorschrift voorziet in de bevoegdheid of verplichting om de gegevens te verstrekken of voor zover de gegevensverstrekking noodzakelijk is voor het afleggen van verantwoording door een medewerker aan de deelnemer die hem heeft aangewezen voor de inzet in het samenwerkingsverband.

Over bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard gaan overigens in principe andere wetten, zoals de Uitvoeringswet AVG, die een aantal uitzonderingen bevat op het verbod dergelijke gegevens te verwerken. Voor enkele specifieke categorieën van dergelijke gegevens regelt dit wetsvoorstel een uitzondering op dit verbod, die overigens niet alleen de bevoegdheid maar ook een plicht regelt tot verstrekking. Het gaat dan om politiegegevens, strafrechtelijke en justitiële gegevens, waarvoor de voorgestelde artikelen 20, derde lid, van de Wpg en 8b en 39fa van de Wjsg een verstrekkingsplicht gaan bevatten. De verwerking door het samenwerkingsverband van dergelijke ontvangen gegevens is op grond van de rechtstreekse werking van de AVG uitsluitend mogelijk voor doeleinden die binnen het toepassingsbereik van de AVG vallen. De verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming en de opsporing van strafbare feiten, met inbegrip van de bescherming tegen en de voorkoming van bedreigingen voor de openbare veiligheid valt onder de richtlijn gegevensbescherming opsporing en vervolging.[21] Overigens zijn samenwerkingsverbanden geen bevoegde autoriteiten in de zin van deze richtlijn en vallen samenwerkingsverbanden in de zin van de WGS onder de AVG.

3.5 Voorafgaande toetsende rol van de Autoriteit persoonsgegevens

Zoals blijkt uit de vorige paragraaf, is het kabinet ervan doordrongen dat het creëren van meer mogelijkheden tot informatiedeling ook deugdelijke waarborgen vergt ter bescherming van de privacy. In aanvulling op deze waarborgen, zal de Autoriteit persoonsgegevens (hierna: AP) – naast haar adviserende rol ten aanzien van de desbetreffende regelgeving op grond van artikel 36, vierde lid, AVG – een toetsende rol vooraf hebben met betrekking tot concrete gegevensverwerkingen in samenwerkingsverbanden. Het gaat daarbij om voorafgaande raadpleging (artikel 36, eerste lid, AVG).
Een samenwerkingsverband moet de AP voorafgaand aan een voorgenomen verwerking van persoonsgegevens raadplegen wanneer de uitkomst van de gegevensbeschermingseffectbeoordeling (PIA) is dat er sprake is van een hoog risico wanneer het samenwerkingsverband geen maatregelen neemt om het risico te beperken. Dit vloeit voort uit artikel 36, eerste lid, AVG. Als de toezichthouder van oordeel is dat de voorgenomen verwerking niet aan de verordening zal voldoen, geeft zij een schriftelijk advies binnen acht weken na het verzoek om raadpleging. Overweging 94 van de verordening stelt hierover: *«Het uitblijven van een reactie van de toezichthoudende autoriteit binnen die termijn dient evenwel een optreden van de toezichthoudende autoriteit overeenkomstig haar in deze verordening neergelegde taken en bevoegdheden onverlet te laten, onder meer de bevoegdheid om verwerkingen te verbieden.»*

4. In de wet aangewezen samenwerkingsverbanden

4.1 Het Financieel Expertisecentrum (FEC)

Het Financieel Expertisecentrum (FEC) is een samenwerkingsverband van diverse overheidsorganisaties dat als doel heeft de integriteit van de financiële sector te versterken. Aan sommige activiteiten van het FEC nemen ook private partijen uit deze sector deel. Bedreigingen en risico's van en inbreuken op de integriteit van de financiële sector moeten worden voorkomen en bestreden. De deelnemers in het FEC treden gezamenlijk op tegen bedreigingen en risico's ten aanzien van de integriteit van de financiële sector, houden toezicht op de naleving van de hiervoor relevante regelgeving of handhaven deze waar nodig.
Om deze doelstelling van het samenwerkingsverband te bereiken is het noodzakelijk dat de deelnemers relevante gegevens uitwisselen en gezamenlijk verder verwerken. Zij doen

[21] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PbEU 2016, L 119)

dit in de vorm van signalenoverleggen en gegevensanalyses om daaruit informatie te verkrijgen die zij kunnen benutten bij de uitoefening van hun taken en bevoegdheden. De deelnemers aan het FEC zijn toezichthouders of andere handhavende instanties ten opzichte van de partijen die onderdeel uitmaken van de financiële sector, of ze zijn informatieleverancier van voornoemde instanties. Daarnaast wordt door het samenwerkingsverband FEC ingezet op het gezamenlijk voorkomen en bestrijden van het gebruik van de financiële sector voor financieel-economische criminaliteit, zoals witwassen, en andere vormen van ernstige, met name ondermijnende criminaliteit alsmede terrorismefinanciering. Met het oog op dit laatste doel werken de deelnemers aan het FEC, met uitzondering van de Belastingdienst, ook al enige jaren samen met financiële instellingen, te weten: de Nederlandse Vereniging van Banken, ING Bank, ABN Amro Bank, Rabobank, Volksbank en Aegon.

Terrorismebestrijding en Veiligheid (NCTV), die tot taak heeft het risico op terroristische aanslagen in Nederland zoveel mogelijk te verkleinen, benadrukt het belang van publiek-private samenwerking om bestrijding van terrorismefinanciering tegen te gaan, waarbij met name de samenwerking met banken en verzekeraars van groot belang is. Daartoe is enkele jaren geleden als publiek-private samenwerking de Taskforce Terrorismefinanciering in de vorm van een pilot begonnen en vervolgens is deze werkwijze, vanwege de goede resultaten, in een structurele aanpak omgezet. Daarbij is in de pilot, gelet op het belang dat de NCTV aan nauwe publiek-private samenwerking op dit terrein hecht, naast de banken ook een bank-verzekeraar meegenomen, mede gelet op de taak van de verzekeraars op grond van de Wet ter voorkoming van witwassen en het financieren van terrorisme (Wwft). Op het moment dat uit de resultaten van de Taskforce blijkt dat het effectief en efficiënt, noodzakelijk en proportioneel is om meer verzekeraars aan de Taskforce deel te laten nemen, kunnen bij amvb meer verzekeraars als deelnemer aan de Taskforce worden aangewezen. Dergelijke publiek-private samenwerking gebeurt vanuit de visie dat de integriteit van het financiële stelsel niet slechts een zaak is van de overheid. Deze visie klinkt ook door in de Wwft, die op dit vlak verplichtingen aan onder meer banken en andere financiële ondernemingen oplegt.

De kerntaken van het FEC die voortkomen uit voornoemde doelstelling, hebben behalve op gegevensverwerking ten behoeve van de zgn. reguliere taken van het FEC ook betrekking op structurele informatie-uitwisseling in onder meer de Terrorismefinanciering Taskforce en de pilot Serious Crime Taskforce, het fungeren als een kenniscentrum en het gezamenlijk uitvoeren van (PPS-)projecten en programma's, onder meer in het programma FEC Terrorismefinanciering, inclusief de daaronder vallende pilot ongewenste buitenlandse financiering.

De volgende organisaties werken in het FEC samen:

- Openbaar ministerie (OM);
- Politie;
- Financial Intelligence Unit-Nederland (FIU);
- Rijksbelastingdienst;
- Fiscale inlichtingen- en opsporingsdienst;
- Autoriteit Financiële Markten;
- De Nederlandsche Bank.

Aan het programma FEC Terrorismefinanciering nemen naast voornoemde partijen ook de Immigratie- en Naturalisatiedienst, de Koninklijke marechaussee, het Bureau Financieel Toezicht en de Algemene Inlichtingen- en Veiligheidsdienst deel. Hun deelname beperkt zich tot het verstrekken van gegevens en het verkrijgen van informatieproducten uit het programma.
Aan uitsluitend de signalenoverleggen in het kader van de beide taskforces nemen ook de eerdergenoemde banken en verzekeraar deel.

De deelnemers aan het FEC hebben alle een taak bij het versterken van de integriteit van de financiële sector. Door gegevens, kennis, inzicht en vaardigheden met elkaar te delen, kunnen bedreigingen en risico's ten aanzien van de integriteit van de financiële sector effectiever en efficiënter worden onderkend. Dit is van belang met het oog op de

beoordeling of aanleiding kan bestaan om publiekrechtelijke, toezichthoudende of andere handhavende bevoegdheden toe te passen door de publieke deelnemers. Voor de private partijen biedt het de mogelijkheid om verbeterde (nieuwe) maatregelen te treffen ter voorkoming van het gebruik van de financiële sector voor financieel-economische criminaliteit.

Het FEC voert binnen de kaders van de huidige wetgeving de volgende verwerkingsactiviteiten uit:

- Signalenoverleg en kennisdeling ten behoeve van de reguliere activiteiten voor het doel van het FEC;
- Signalenoverleg en gegevensanalyse ten behoeve van het Programma Terrorismefinanciering;
- Signalenoverleg ten behoeve van de Taskforce Terrorismefinanciering;
- Signalenoverleg ten behoeve van Taskforce Serious Crime.

Deze activiteiten worden uitgevoerd met inachtneming van het Informatieprotocol FEC 2019 (Stcrt. 2019, nr. 43749), het Convenant Terrorismefinanciering Taskforce (Stcrt 2019, nr. 43628) en Convenant Pilot Serious Crime Taskforce (Stcrt 2019, nr. 43629).

De WGS brengt geen verandering in de deelname door de verschillende (categorieën van) partijen aan de onderscheidene verwerkingsactiviteiten van het FEC. Zij bevat met het oog op die activiteiten wel de volgende nieuwe onderdelen:

- de mogelijkheid om in aanvulling op de bestaande mogelijkheden van gegevensverwerking waarbij de noodzaak van de verstrekking van gegevens per deelnemer moet worden aangetoond, gegevens voortaan ten behoeve van het doel van het FEC als geheel aan meerdere of alle deelnemers tegelijk te verstrekken en in een signalenoverleg of gegevensanalyse verder te verwerken;
- verstrekking van de resultaten van de verwerking binnen het FEC aan derden, met inbegrip van andere samenwerkingsverbanden, voor zover dat noodzakelijk is voor doeleinden die verenigbaar zijn met de doeleinden van het FEC;
- verplichte verstrekking van gegevens aan het FEC, voor zover dat noodzakelijk is voor het doel van het samenwerkingsverband, met de mogelijkheid daarop uitzonderingen te maken of daaraan voorwaarden te stellen;
- de mogelijkheid om voortaan ook ten behoeve van de reguliere activiteiten van het FEC gegevensanalyses uit te voeren zoals dat nu in het kader van terrorismefinanciering gebeurt.

Het FEC hanteert verschillende waarborgen die bijdragen aan de zorgvuldigheid van de gegevensverwerking. Deze zijn deels terug te vinden in artikel 8 van het wetsvoorstel en zullen voor een ander deel worden opgenomen in de amvb waarin bepaalde aspecten van de gegevensverwerking nader worden uitgewerkt. Daarbij valt te denken aan de aanwijzing van [redacted] die tot taak heeft te waarborgen dat de gezamenlijke verwerkingsverantwoordelijken op een zorgvuldige wijze uitvoering geven aan de verplichtingen die voortvloeien uit de AVG. Op dit moment vervult [redacted] van de FEC-eenheid, dat als bureau het FEC ondersteunt, die rol. Een andere waarborg zou kunnen zijn gelegen in de vastlegging in de amvb van het "GAZO-principe" (geen actie onder overleg). Dit principe houdt in dat er door de FEC-eenheid, het FEC TF (terrorismefinanciering) analyseteam en door de bij het FEC betrokken partijen gedurende de FEC-samenwerking geen gebruik mag worden gemaakt van de ingebrachte persoonsgegevens zonder overleg met en instemming van de FEC-partner(s) waarvan de persoonsgegevens oorspronkelijk afkomstig zijn. Iedere FEC-partner heeft dan een inspanningsverplichting ervoor zorg te dragen dat binnen zijn organisatie zodanige waarborgen worden getroffen dat aan het GAZO-principe kan worden voldaan. Zowel de rol van regisseur als het GAZO-principe zijn nu in het Informatieprotocol FEC 2019 opgenomen.

De juridische begrenzing van de gegevensverwerking is thans nog in het FEC-convenant en het daarbij behorende informatieprotocol en in de convenanten voor beide Taskforces

geregeld, maar wordt met dit wetsvoorstel op het niveau van wet vastgelegd. Daarnaast worden nadere regels voor het FEC bij algemene maatregel van bestuur gesteld.

4.2 De Infobox Crimineel en Onverklaarbaar vermogen (iCOV)

Criminelen die ongehinderd in de auto blijven rondrijden die is aangeschaft met oneerlijk verdiend geld. Omzet die moedwillig te hoog in de boeken terecht komt om zo te profiteren van onterechte btw-teruggave. Frauderen voor eigen gewin, waarbij de staat en dus de samenleving de rekening betaalt. Het zijn onverteerbare feiten voor eerlijke burgers en dienstbare bestuurders. Anders gesteld: misdaad mag niet lonen, maar doet het helaas soms wel.

Een van de manieren om dergelijke misstanden het hoofd te bieden, is via de infobox Crimineel en Onverklaarbaar Vermogen (iCOV). Door samen te werken en informatie te delen, wordt het voor kwaadwillenden minder eenvoudig om crimineel geld in de eigen zak te houden. Op voorspraak van de minister van Veiligheid en Justitie is in 2013 daarom het samenwerkingsverband iCOV opgericht.

De infobox Crimineel en Onverklaarbaar Vermogen (hierna: "iCOV") is een samenwerkingsverband van diverse overheidsorganisaties. Het gaat hierbij onder meer om opsporingsdiensten, organisaties met een fiscale taak of taak op het gebied van invordering, en toezichthouders. Het samenwerkingsverband stelt rapportages samen. Deze rapportages dragen bij aan de bestrijding van onder meer witwassen, belastingontduiking, fraudebestrijding, inning van overheidsvorderingen en de bevordering en bewaking van correcte marktwerking.

Het gaat hier voor het overgrote deel om verschijnselen die een ondermijnend karakter hebben en hun tentakels uitsteken tot diep in verschillende sectoren van de samenleving. Deze verschijnselen vragen dan ook om een antwoord van verschillende overheidsorganisaties. Niet alleen om frauduleuze of ondermijnende activiteiten op het eigen terrein te kunnen aanpakken, maar juist om de problemen integraal te benaderen om zo tot een algehele interventie of aanpak te komen. Op deze wijze kan de overheid haar burgers efficiënter beschermen tegen kwalijke praktijken in den brede en vergroot dit het vertrouwen in de samenleving en de overheid als geheel. Voor deze integrale benadering is het noodzakelijk dat data van meerdere partijen geïntegreerd worden om een volledig beeld te krijgen. Dit beeld kan niet verkregen worden als elke partij afzonderlijk naar de eigen data kijkt. Daarvoor is de problematiek te veel verborgen. De kracht zit juist in de samenhang van de data waardoor patronen, dwarsverbanden en fenomenen zichtbaar kunnen worden. Deze dwarsverbanden kunnen van belang zijn voor de taakuitoefening van alle in iCOV samenwerkende organisaties, zowel in een afzonderlijke als gezamenlijke interventiestrategie. De kracht van het samenwerkingsverband zit er verder in dat de aanvrager nu niet bij iedere organisatie afzonderlijk de informatie hoeft op te vragen, maar dit in één keer kan doen bij het samenwerkingsverband. Dit levert een efficiëntieslag op. Een andere kracht van het samenwerkingsverband is dat zij alle informatie overzichtelijk in één document weer kan geven waardoor er relaties worden gelegd die niet of heel moeilijk boven water zouden komen als de informatie afzonderlijk opgevraagd wordt per overheidsorganisatie.

De volgende organisaties werken samen in iCOV:

- Openbaar Ministerie (OM);
- Politie;
- Rijksrecherche;
- Financial Intelligence Unit-Nederland (FIU);
- Centraal Justitieel Incassobureau (CJIB);
- Belastingdienst (in het bijzonder Belastingen/Toeslagen/Douane);
- Belastingdienst/Fiscale Inlichtingen- en Opsporingsdienst (FIOD);
- Inspectie Leefomgeving en Transport-Inlichtingen- en Opsporingsdienst (ILT-IOD);
- Inspectie Sociale Zaken en Werkgelegenheid-Directie Opsporing (ISZW-DO);

- Nederlandse Voedsel- en Warenautoriteit- Inlichtingen- en Opsporingsdienst (NVWA-IOD);
- Autoriteit Consument & Markt (ACM);
- De Nederlandsche Bank (DNB).

De rapportages van iCOV maken inzichtelijk waar het criminele of fiscaal ontdoken vermogen wordt verborgen. Ze tonen tevens welke sleutelfiguren zich hiermee bezighouden. Het geldspoor volgen is daarbij van onschatbare waarde om de daadwerkelijk belanghebbenden te traceren en de modus operandi bloot te leggen. Dit is allereerst van belang bij het oplossen van strafrechtelijke, fiscale of bestuurlijke casussen. Maar de rapportages dragen ook bij aan een meer strategisch inzicht over waar bepaalde problemen zich voordoen en wat de kenmerken hiervan zijn. Dit maakt een effectievere inzet van mensen en middelen mogelijk en zorgt dat barrières kunnen worden opgeworpen tegen (de facilitering van) criminele geldstromen. Er speelt nog een ander belang. Door crimineel of fiscaal ontdoken vermogen af te pakken, wordt de stimulans om met ondermijnende activiteiten door te gaan onaantrekkelijker gemaakt. Immers: wie gevangenisstraf krijgt, vastgoed en bolides moet inleveren én een naheffing van de Belastingdienst krijgt, verliest aan status. Dat zal zeker indruk maken op de crimineel en zijn omgeving.

iCOV vervaardigt onder de noemer "productie" drie typen standaardrapportages die zgn. sturingsinformatie voor operationele doeleinden opleveren:

iCOV Rapportage Vermogen en Inkomen (iRVI)
De iRVI is een overzicht van het vermogen en de inkomsten van een of meer, op basis van vooraf vastgelegde criteria bevraagde natuurlijke personen (subjecten) of rechtspersonen. De iRVI wordt samengesteld op basis van actuele en historische gegevens. De historische gegevens gaan in beginsel vijf jaar terug in de tijd, maar de leverende partij mag al naar gelang de bewaartermijn die zij hanteert, hiervan afwijken. De gegevens bevatten enkele relatietypen zoals het adres van een of meer subjecten of rechtspersonen, maar ook familierelaties (zoals kinderen en ouders) en de relaties met rechtspersonen. De iRVI kent twee varianten, te weten:

- Subject: overzicht van de vermogens- en inkomstenpositie van een subject, inclusief banktegoeden, hypotheekgegevens, RDW-gegevens, informatie over erfenissen en schenkingen, alimentatie, verdachte transacties en winst- en omzetgegevens.
- Rechtspersoon: een overzicht van de vermogens- en inkomstenpositie van een rechtspersoon, inclusief vastgoed, banktegoeden, aandeelhoudersconstructies, winst- en omzetgegevens, RDW-gegevens over eigendom van voertuigen en banktegoeden.

De iRVI wordt volledig geautomatiseerd gegenereerd op basis van gegevens van het Kadaster, de Kamer van Koophandel, de Belastingdienst, de Rijksdienst voor het wegverkeer en de politie. De fiscale data behelzen niet alleen de data van de Belastingdienst, maar ook de data van derden waarvan de Belastingdienst voor haar taken gebruik mag maken en die meegeleverd worden via de Belastingdienst. Een voorbeeld hiervan zijn de data van het Kadaster. Inmiddels zijn iRVI's gebruikt in zittingen bij de strafrechter, om aan te tonen dat een subject over vermogen beschikte dat via legale weg niet verklaarbaar was, en dit gebruik van iRVI's is door de strafrechter reeds meerdere malen geaccepteerd.

iCOV Rapportage Relaties (iRR)
Dit is een rapportage over de financieel-zakelijke relaties rondom een persoon of bedrijf, ook wel relatiescan genoemd. Een van de kenmerken van fraude of witwassen is immers het verhullen van (financieel) vermogen in het eigen relatienetwerk. Daarom is het noodzakelijk om in de directe omgeving van een bevraagd persoon te kijken naar indicaties voor het bezit van onverklaarbare of zelfs onrechtmatige vermogensbestanddelen. In de iRR komen financieel-zakelijke relaties in beeld, maar ook familieleden en (ex-)partners. Als er sprake is van een BV of VOF komt ook de eigenaar

van het bedrijf in beeld. Dit geldt ook voor eventuele bestuursfuncties van stichtingen en verenigingen. De relatiescan geeft een weergave tot drie lagen vanaf het bevraagde subject. Dit houdt in dat er tot drie stappen vanaf het bevraagde subject de relaties zichtbaar worden weergegeven indien deze relevant zijn. Daarnaast kunnen afhankelijk van de aanvrager bepaalde politiegegevens worden getoond, waaronder vermoedelijke criminele relaties. Vermogen wordt vaak verhuld verderop in het netwerk van de betrokkene, niet zo zeer bij de directe relaties, daardoor zijn drie lagen noodzakelijk om in kaart brengen.

De iRR wordt in eerste instantie automatisch gegenereerd op basis van de voor iCOV beschikbare bronnen. Aansluitend vindt er een selectie van de gegevens plaats door menselijke tussenkomst. Hierbij wordt irrelevante en disproportionele informatie eruit gefilterd. Bijvoorbeeld de relatie met onroerendgoedbezit met een woningcorporatie of gemeente kan weinig zeggend zijn. In een gemeente als Amsterdam heeft praktisch elke huiseigenaar een relatie met de gemeente vanwege de erfpacht. Het opnemen van alle overige (natuurlijke en rechts-) personen met eenzelfde relatie, levert dan geen betekenisvolle toevoeging voor de aanvrager op.
Een ander voorbeeld is een 'verdachte transactie' (gemeld bij de FIU) naar het CJIB, die voortkomt uit het feit dat iemand een contante storting heeft gedaan aan het CJIB om zijn boete te betalen. De iRR zou in dit geval alle andere personen die ook een verdachte transactie naar het CJIB hebben gedaan, tonen. Dit wordt echter door een iCOV-medewerker eruit gefilterd.
Aansluitend wordt de rapportage besproken met de aanvrager om zo de relevante relaties toe te lichten. De iRR biedt als zodanig sturingsinformatie voor het onderzoek waarmee de aanvrager is belast.

iCOV-rapportage Thema (iRT)
Om een meer strategisch inzicht te verkrijgen in een veelzijdige problematiek is het noodzakelijk om thematische analyses te kunnen doen. Een iRT biedt inzichten over ontwikkelingen en trends in een bepaald geografisch gebied. Deze inzichten zien nu op witwassen via vastgoed. De iRT geeft de mogelijkheid om inzicht te kunnen verkrijgen in de mogelijke omvang van het fenomeen aan de hand van gevalideerde indicatoren. Dit levert sturingsinformatie op voor een aanvragende partij.
De resultaten uit dit onderzoek zijn nu nog anoniem en worden opgeleverd onder de naam "iRT NN" (NN staat voor "nomen nescio").

Nieuw onder de WGS
Op dit moment voert iCOV deze standaardrapportages nog uit op basis van de bestaande wettelijke bevoegdheden van de desbetreffende individuele deelnemer en alleen als die deelnemer daar specifiek om heeft gevraagd.
Daarbij vormen bestaande geheimhoudingsplichten een knelpunt om voor die rapportages data van verschillende deelnemers te combineren. Onder de WGS is dat wel mogelijk, waardoor er een vollediger beeld en dus ook meer sturingsinformatie ontstaat. Onder de WGS geldt dat er gekeken zal worden naar de doelstellingen van het samenwerkingsverband. Indien de aanvraag hierbinnen past worden de benodigde data verwerkt in de rapportage. Op grond van artikel 7, eerste lid, onder a, van het wetsvoorstel kan de deelnemer de rapportage ontvangen indien dat noodzakelijk is voor de vervulling van een publiekrechtelijke taak die aan de deelnemer is opgedragen, wanneer deze taak verenigbaar is met het doel van het samenwerkingsverband.

Daarnaast maakt de WGS de uitvoering van een deels nieuwe methode mogelijk: de iRT compact. Deze methode houdt in dat, indien bepaalde tot dan toe gepseudonimiseerde subjecten of objecten op basis van vooraf vastgestelde indicatoren hiertoe aanleiding geven, op grond van de uitkomsten van een iRT NN wordt overgestapt naar deze iRT compact. Bij een iRT compact worden de desbetreffende subjecten en objecten (bedrijven) weer genonimiseerd, d.w.z. weer van een naam en andere identificerende gegevens voorzien. Op die subjecten en objecten wordt dan een iRVI en iRR uitgevoerd en worden de resultaten daarvan geanalyseerd en weergegeven in een iRT compact. Een iRT compact kan aldus sturingsinformatie bieden die de afzonderlijke deelnemer kan

helpen bij een efficiëntere en effectievere invulling van de eigen taak. Voor een iRT compact dient overigens wel een nieuwe aanvraag te worden ingediend. Zij kan, anders gezegd, niet automatisch volgen op een uitgevoerde iRT NN. De onderzoeksvraag voor een iRT compact wordt dan toegespitst op gegevens die herleidbaar zijn naar de subjecten of objecten die op basis van eerder bedoelde criteria zijn geselecteerd.

Wetenschap en innovatie
Naast verwerkingen ten behoeve van deze standaardrapportages vinden bij iCOV ook geautomatiseerde verwerkingen plaats voor wetenschappelijke onderzoeken en innovatieve vernieuwingen. Als er innovatieve handelingen en onderzoeken worden gedaan voor de kwaliteitsverbetering van de producten van iCOV, worden deze werkzaamheden uitgevoerd in een afgescheiden zone binnen dezelfde omgeving als waarbinnen het beheer van gegevens voor productiedoeleinden plaatsvindt. Dit geldt ook voor handelingen ter verbetering van de technische performance en verdere bescherming van de privacy door privacy by design en privacy enhancing technology of voor het toevoegen c.q. minimaliseren van data. Deze werkzaamheden worden net als de werkzaamheden voor wetenschap uitgevoerd op een lokale IT-omgeving. Deze omgeving is zowel fysiek als IT-technisch extra beveiligd. De toegang tot deze ruimte is beperkt tot slechts enkele personen op basis van noodzakelijkheid. Verder zijn er aanvullende inbraakdetectiemaatregelen en hangen er camera's. De belangrijkste IT-technische beveiliging is wel dat er een gescheiden netwerk is dat geen connectie heeft met enig bedrijfsnetwerk of het internet (behalve indien systeemupdates noodzakelijk zijn). Verder is deze omgeving geëncrypted en worden alle handelingen gelogd. De verwerkingen in het kader van wetenschap en innovatie vinden plaats onder het regime van de artikelen 89 AVG, 22 Wpg en 39g juncto 15 Wjsg. In die artikelen is bepaald dat de resultaten van de activiteiten in het kader van wetenschappelijk onderzoek en statistiek geen persoonsgegevens mogen bevatten.
Binnen innovatie en wetenschap worden er wetenschappelijke onderzoeken verricht ten behoeve van innovatieve vernieuwingen voor de ontwikkeling van rapportage,- en analyse mogelijkheden binnen iCOV. Een greep uit de verwerkingen die binnen wetenschap en innovatie plaatsvinden:

1. Methodes ontwikkelen om nieuwe data(bestanden) te beoordelen
2. Ontwikkelen van productaanpassingen
   a. Aanvullingen m.b.v. nieuwe data
   b. Verbeterde lay-out / performance etc. van bestaande producten
3. Testen nieuwe (versies van) software
4. Onderzoek naar nieuwe indicatoren voor themarapportage .

Waarborgen
iCOV hanteert verscheidene waarborgen in verschillende verwerkingsstadia die bijdragen aan de zorgvuldigheid bij de gegevensverwerking. Deze zijn deels terug te vinden in artikel 8 van het wetsvoorstel en zullen voor het andere deel worden opgenomen in de amvb waarin bepaalde aspecten van de gegevensverwerking nader worden uitgewerkt. Een van de waarborgen wordt er hier uitgelicht, omdat die ook zal gelden voor de andere samenwerkingsverbanden die onder de WGS vallen. Het betreft de instelling van een zgn. rechtmatigheidsadviescommissie. Deze commissie heeft tot taak de rechtmatigheid van de verwerking van persoonsgegevens in het samenwerkingsverband structureel te beoordelen en om voorstellen aan het samenwerkingsverband te doen om onrechtmatigheden op te lossen. Zo adviseert de rechtmatigheidsadviescommissie van iCOV onder meer over de vraag of een iRT NN qua scope past binnen de wettelijke doelstellingen van het samenwerkingsverband en beoordeelt zij de behoefte aan eventuele nieuwe indicatoren en producten binnen iCOV. Andere waarborgen die genoemd kunnen worden, zijn het uitvoeren van een periodieke review van de noodzaak om bepaalde datasets aan te leveren (draagt bij aan data-minimalisatie), de toepassing van strikte autorisatie- en screeningsvereisten om het risico van oneigenlijke datatoegang te minimaliseren, menselijke validatie van de aan te leveren datasets (géén geautomatiseerde levering) en de eis dat op basis van de geleverde sturingsinformatie altijd vervolgonderzoek plaatsvindt (sturingsinformatie levert geen vermoeden van een

strafbaar feit of een andersoortige overtreding van een wettelijk voorschrift op). De informatie bij iCOV wordt vanaf 2018 verwerkt in de hoger gerubriceerde omgeving van het Rijk; dit betekent dat deze dezelfde status heeft als de gevoelige informatie van de Rijksrecherche of van documentatie rondom het MH17-onderzoek. De gevolgen van deze hogere rubricering zijn verstrekkend als het gaat om opslag, beheer, toegang en beveiliging.

De juridische begrenzing van de gegevensverwerking is thans nog in het iCOV-convenant (Stcrt. 2019, 11302) en de daarbij behorende protocollen gegevensverwerking geregeld. Het convenant benadrukt dat een verstrekking alleen kan plaatsvinden als dat wettelijk is toegestaan; het creëert geen nieuwe bevoegdheden tot verstrekking of verwerking.
Met dit wetsvoorstel wordt de juridische begrenzing op het niveau van wet vastgelegd. Daarnaast worden nadere regels gesteld voor iCOV bij algemene maatregel van bestuur.

4.3 De Regionale Informatie- en Expertisecentra (RIEC's)

In artikel 30, eerste lid, worden de regionale informatie- en expertisecentra (RIEC's) aangewezen als samenwerkingsverbanden in de zin van deze wet.

Met het ondertekenen van het Bestuurlijk akkoord geïntegreerde decentrale aanpak georganiseerde misdaad in september 2008[22] hebben de ministers van Binnenlandse Zaken en Koninkrijksrelaties, van Justitie, van Defensie, van Sociale Zaken, de staatssecretaris van Financiën en de voorzitters van het college van procureurs-generaal en van de Vereniging van Nederlandse Gemeenten de basis gelegd voor de bestuurlijke aanpak van georganiseerde misdaad. Dit bestuurlijk akkoord bevatte een modelconvenant op basis waarvan gemeenten, het openbaar ministerie, de politie, de Koninklijke marechaussee, de toenmalige SIOD, de Belastingdienst en de FIOD/ECD in regionaal verband met elkaar een samenwerkingsverband zijn aangegaan om met een geïntegreerde aanpak de georganiseerde misdaad te bestrijden.

In vervolg daarop zijn met het afsluiten van destijds elf convenanten even zoveel regionale informatie- en expertisecentra opgericht om deze vorm van samenwerking te ondersteunen. Daarmee is toen een basis gelegd voor de geïntegreerde aanpak van georganiseerde misdaad en het in dat verband bijeenbrengen van bij de deelnemende partijen aanwezige bestuurlijke en strafrechtelijke informatie.

Een herzien convenant is in 2014 afgesloten. Daarmee zijn de RIEC's onder één convenant gebracht en vanaf dat moment georganiseerd op de schaal van de 10 politie-eenheden. Sindsdien zijn verschillende (landelijk georganiseerde) partijen toegetreden die een bijdrage kunnen leveren aan het realiseren van de doelstellingen van de RIEC's. De RIEC's bestaan thans uit alle gemeenten (vertegenwoordigd door de burgemeester resp. het college van burgemeester en wethouders), alle provincies (vertegenwoordigd door de commissaris van de Koning resp. gedeputeerde staten, het openbaar ministerie, de nationale politie, de Koninklijke marechaussee, de Douane, het openbaar ministerie, de belastingdienst / belastingen, de belastingdienst / Fiscale Inlichtingen en Opsporingsdienst, de belastingdienst / toeslagen, de Inspectie Sociale Zaken en Werkgelegenheid, de Immigratie en Naturalisatie Dienst, de Nederlandse voedsel en warenautoriteit en het Uitvoeringsinstituut Werknemersverzekeringen.

Daarnaast is inmiddels het Landelijk informatie- en expertisecentrum (LIEC) ingesteld (ondergebracht bij het ministerie van Justitie en Veiligheid), dat de RIEC's ondersteunt, onder meer door het in samenwerking met de RIEC's zorgdragen voor landelijke standaarden ten behoeve van uniformiteit van de hoofdwerkprocessen en informatiedeling, het bieden van specialistische ondersteuning en functioneren als landelijk kenniscentrum voor de bestuurlijke en georganiseerde criminaliteit, het systeembeheer en het technisch beheer van het IT-systeem voor de deelnemers van de RIEC's uitvoert en de minister van Justitie en Veiligheid adviseert. Het LIEC verwerkt niet eigenstandig persoonsgegevens en is geen verwerkingsverantwoordelijke.

[22] Kamerstukken II, 2009, 29 911, nr. 27.

In het convenant dat aan de samenwerking ten grondslag ligt zijn de organisatorische aspecten van de samenwerking geregeld. Dat betreft onder meer het instellen van –per regio- een stuurgroep en de wijze van verantwoording van het RIEC.
De juridische begrenzing van de gegevensverwerking en de verantwoording daarover is thans nog in het RIEC-convenant, het daarbijbehorende privacy-protocol en de bijbehorende werkprocesbeschrijvingen geregeld, maar wordt met dit wetsvoorstel op het niveau van wet vastgelegd. Daarnaast worden bij of krachtens algemene maatregel van bestuur nadere regels gesteld over de gezamenlijke gegevensverwerking door de RIEC's.

4.4 De Zorg- en Veiligheidshuizen (ZVH)

Veel criminaliteits- en veiligheidsvraagstukken zijn geworteld in sociale en/of zorgproblematiek. Ook maken criminelen relatief vaak misbruik van kwetsbaren in de samenleving. Een effectieve aanpak van deze vraagstukken vraagt daarom vaak om samenwerking tussen deelnemers uit het zorg-, sociaal en veiligheidsdomein, ook in het belang van de betrokkene. Dat vraagt om een samenwerkingsruimte waarin verschillende deelnemers uit verschillende domeinen met inachtneming van elkaars taken, verantwoordelijkheden en bevoegdheden hun inzet richting een betrokkene met elkaar kunnen afstemmen om zo tot een persoonsgerichte aanpak te komen.

Zorg- en Veiligheidshuizen focussen zich op complexe casuïstiek. In de context van de zorg- en veiligheidshuizen betekent dit casuïstiek waarbij een burger (potentieel) crimineel en overlastgevend gedrag vertoont, vaak met risico's voor de veiligheid van hemzelf en zijn omgeving, en waar dit gedrag mede veroorzaakt wordt door problemen die de persoon ervaart op het gebied van het sociaal en of zorgdomein. In dergelijke situaties zijn de verbinding tussen de straf- en zorgketen, en interventies vanuit de gemeente en haar partners een voorwaarde voor een succesvolle en duurzame aanpak van het (potentieel) crimineel en overlastgevend gedrag. Onderdeel daarvan kan ook zijn dat drang en dwangmaatregelen nodig zijn om de noodzakelijke begeleiding, zorg- en hulpverlening te realiseren. Verbindend uitgangspunt tussen de bij de aanpak betrokken partijen is daarbij dat als het beter gaat met de persoon, het (potentieel) crimineel en overlastgevend gedrag zal afnemen, of veiligheidsrisico's voor de persoon en zijn omgeving zullen afnemen.

Zorg- en Veiligheidshuizen richten zich op complexe casuïstiek die niet door één deelnemer of keten alleen kan worden opgelost. Daarbij kan worden gedacht aan individuen met complexe problematiek zoals psychiatrische of verslavingsproblematiek hetgeen leidt tot overlast of dreigend gevaarlijk gedrag voor anderen. Ook kunnen personen door hun psychische/psychosociale problematiek of verstandelijke beperking kwetsbaar zijn om in criminele activiteiten verzeild te raken. Door te komen tot een gezamenlijk beeld van de situatie kunnen de deelnemers beter de gewenste aard en intensiteit van hun interventie bepalen mede gelet op het geheel aan gewenste interventies. Het kan ook gaan om een overlastgevend gezin waarbij moeder verslaafd is, vader agressief, het ene kind laag verstandelijk beperkt is, het andere kind de buurt onveilig maakt. Dat vraagt van de deelnemers om één gezamenlijk beeld van de situatie te krijgen en vanuit één plan onder andere zorg (bijvoorbeeld behandeling voor de verslaving van de moeder), straf (na een gepleegde inbraak door een zoon) en bestuurlijke interventies (tijdelijk huisverbod dat is opgelegd aan de vader) in te zetten. De gezamenlijke inspanning leidt ertoe dat het gezin minder overlast veroorzaakt, benodigde hulp wordt ingezet en niet meer of duidelijk minder in aanraking komt met justitie. Bij het komen tot een persoonsgerichte aanpak staan de volgende vragen centraal. Heeft de persoon of betrokkenen binnen het gezin problemen op meerdere gebieden? Is er sprake van crimineel of overlastgevend gedrag of dreigt dit in de toekomst te gebeuren? Zijn voor de aanpak van de problematiek partijen uit meerdere ketens nodig?

Bij de aanpak van dergelijke complexe casuïstiek zijn de betrokken deelnemers afhankelijk van elkaars inspanningen om succesvolle en duurzame resultaten te bereiken.

1912034 02691

De samenwerking binnen het Zorg- en Veiligheidshuis heeft tot doel om ervoor te zorgen dat – gelet op de aard van de problematiek - samenwerking tot stand kan komen tussen de juiste deelnemers. Met het oog daarop verwerken zij gezamenlijk gegevens binnen het Zorg- en Veiligheidshuis, om een zo compleet mogelijk persoonsbeeld te kunnen creëren teneinde tot een multidisciplinaire aanpak (zorg, hulpverlening, straf) van complexe problematiek te komen. Daarbij is het streven om steeds zoveel mogelijk te komen tot een maatwerkaanpak, zowel met betrekking tot de te betrekken deelnemers in een concreet geval, als de te verwerken persoonsgegevens.

Deelnemers aan de Zorg- en Veiligheidshuizen kunnen individuele casussen voorleggen welke na acceptatie kunnen leiden tot een persoonsgerichte aanpak met coördinatie en monitoring door de deelnemers. Daarnaast kunnen Zorg- en Veiligheidshuizen lijsten vaststellen met personen binnen een doelgroep van een geprioriteerd veiligheidsprobleem, ten behoeve van het bepalen en uitvoeren van een gezamenlijke strategie door de deelnemers.

De huidige regelgeving over gegevensverwerking biedt geen goed juridisch kader voor de gegevensverwerking die nodig is om tot samenwerking en afstemming tussen deelnemers te kunnen komen. Onder de huidige juridische kaders dient steeds vooraf vastgesteld te worden voor iedere deelnemer of er een grondslag en noodzaak is om gegevens te verstrekken. Dat knelt in situaties waarin het beeld van de complexe persoonsgerichte casuïstiek pas kan worden vastgesteld als de informatie van verschillende deelnemers is samengebracht. Pas aan de hand van het dan ontstane beeld kan worden vastgesteld welke deelnemers in een specifiek geval nodig zijn voor de persoonsgerichte aanpak. Een tweede probleem is dat de huidige regelgeving over gegevensverwerking geen kader biedt voor de gezamenlijke verwerking van gegevens die plaatsvindt tijdens een casusoverleg. In principe zal nu iedere deelnemer aan een casusoverleg per casus steeds vooraf moeten nagaan of elke andere deelnemer aan het casusoverleg wel een voldoende grondslag heeft om kennis te mogen nemen van de gegevens die zij inbrengt. Dit stelt de praktijk voor een vrijwel onmogelijke opgave. Het risico ontstaat daardoor dat deelnemers die individueel allemaal noodzakelijk zijn om tot een goede aanpak te komen, toch niet tot een goede afstemming kunnen komen.
Dit wetsvoorstel creëert een juridisch kader voor de gezamenlijke gegevensverwerking die nodig is voor partijen om ook in dergelijke situaties tot een goed beeld en een goede aanpak te komen, en daartoe gezamenlijk casusoverleg te kunnen voeren. Tegelijkertijd stelt het regels aan de verdere verwerking van dergelijke gegevens om de persoonlijke levenssfeer van de betrokkene te beschermen.

Opname van de Zorg- en Veiligheidshuizen creëert een duidelijk juridisch kader voor de gegevensverwerking in het Zorg- en Veiligheidshuis ten behoeve van de samenwerking rond complexe casuïstiek, de mogelijkheden voor partijen om gezamenlijk gegevens te verwerken ten behoeve van die samenwerking, en om criteria te stellen ter bescherming van de persoonlijke levenssfeer van de burger.
Meer specifiek kan onder de dit wetsvoorstel sneller en grondiger worden gewerkt doordat:

- er duidelijkheid is over de grondslag voor het verstrekken van gegevens aan een Zorg- en Veiligheidshuis door de deelnemers, inclusief bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard. De noodzakelijke informatie kan daardoor sneller bij elkaar komen en er kan sneller duidelijk worden welke deelnemers noodzakelijk zijn om te betrekken bij een casus;
- er een juridisch kader wordt gecreëerd voor het verwerken van gegevens ten behoeve van het verkennen van de casus en het voeren van casusoverleg. Hierdoor wordt het mogelijk om gezamenlijk gegevens te verwerken binnen het samenwerkingsverband ten behoeve van de verkenning van de problematiek en de persoonsgerichte aanpak, ook als de afzonderlijke juridische kaders van de betrokken deelnemers een bilaterale uitwisseling tussen alle betrokken partijen niet mogelijk maken. Hierdoor kan er een grondiger analyse plaatsvinden van de

casus, en kunnen meer invalshoeken meegenomen worden, waardoor de kans op een succesvolle persoonsgerichte aanpak wordt verhoogd;
- er een juridisch kader ontstaat voor de verstrekking van persoonsgegevens tussen Zorg- en Veiligheidshuizen. De Zorg- en Veiligheidshuizen zijn regionaal georganiseerd en vanwege verplaatsing van betrokkenen, moet het mogelijk zijn dat Zorg- en Veiligheidshuizen in verschillende regio's gegevens aan elkaar verstrekken. Hierdoor wordt samenwerking tussen Zorg- en Veiligheidshuizen mogelijk indien de casus dat noodzakelijk maakt. Opname in dit wetsvoorstel leidt tevens tot regulering van een praktijk. Door de regulering in dit wetsvoorstel ontstaat duidelijkheid over de voorwaarden waaronder gegevensverwerking in het kader van de Zorg- en Veiligheidshuizen plaats kan vinden, en creëert het wetsvoorstel transparantie voor de burger, onder meer over de vraag op welke manier hij zijn rechten op grond van de AVG kan uitoefenen. Tevens maakt het wetsvoorstel het mogelijk om bij algemene maatregel van bestuur nadere regels te stellen om een zorgvuldige en rechtmatige gegevensverwerking te waarborgen. De persoonlijke levenssfeer van de burger kan daardoor beter worden beschermd.

Zorg- en Veiligheidshuizen beschikken op dit moment al over een privacy protocol met betrekking tot de verwerking en uitwisseling van gegevens tijdens de uitvoering van de werkzaamheden, de beperkingen en randvoorwaarden die daarbij in acht genomen moeten worden, de afspraken die nodig zijn om een zorgvuldige omgang met gegevens te waarborgen, en de wijze waarop invulling gegeven wordt aan bijvoorbeeld de rechten van betrokkene en de informatieplicht richting de betrokkene uit de AVG. Bij de voorbereiding van de algemene maatregel van bestuur, bedoeld in artikel 8, negende lid, zal worden bezien welke waarborgen uit dat protocol in aanvulling op de waarborgen van artikel 8 en 8a in die algemene maatregel van bestuur voor de Zorg- en Veiligheidshuizen zullen worden vastgelegd.

5. Verhouding tot bestaande en nieuwe samenwerkingsverbanden

De WGS heeft niet tot doel een exclusief regime voor gegevensverwerking door samenwerkingsverbanden te creëren. Zij heeft dan ook geen implicaties voor de talloze bestaande samenwerkingsverbanden die binnen de grenzen van het huidige recht voldoende ruimte hebben om op de door hen gewenste wijze persoonsgegevens te verwerken.

Voor zover er samenwerkingsverbanden zijn die gemeenschappelijke casusanalyses of data-analyses willen verrichten waarvoor thans geen of hooguit een suboptimale grondslag bestaat, kan worden overwogen deze tot een samenwerkingsverband om te vormen dat bij of krachtens de WGS wordt aangewezen. Zo'n samenwerkingsverband zal uiteraard op het moment van inwerkingtreding, ten volle aan de voorschriften uit de WGS en de amvb moeten voldoen.

De vraag welke bestaande samenwerkingsverbanden op enig moment onder de werking van de WGS worden gebracht, is een vraag die thans nog bewust is opengelaten. Dat heeft verschillende redenen. De belangrijkste is dat partijen die aan zo'n samenwerkingsverband deelnemen, eerst zullen willen afwachten hoe de WGS er precies uit gaat zien om goed te kunnen beoordelen welke meerwaarde deze voor het desbetreffende samenwerkingsverband zal hebben. Bestaande samenwerkingsverbanden zullen zich ook een beeld van de nieuwe wetgeving willen vormen, voordat zij kunnen beoordelen of zij onder de werking van de WGS willen gaan vallen.

Zoals nader toegelicht in paragraaf 3.2.1, worden in het wetsvoorstel zelf de gezamenlijke gegevensverwerking door een viertal *bestaande* samenwerkingsverbanden geregeld: het FEC, iCOV, de RIEC's en de Zorg- en Veiligheidshuizen. Het gaat hier om verbanden die voor essentiële maatschappelijke vraagstukken samenwerken en het betreft bovendien samenwerkingsverbanden die inmiddels ten minste vijf jaar bestaan en daarmee een bestendig karakter hebben.

Tot slot is de WGS uiteraard ook bestemd voor samenwerkingsverbanden die thans nog niet bestaan, maar in de toekomst mogelijk worden opgericht. Het moet dan gaan om samenwerkingsverbanden waarvan de deelnemers voor een gemeenschappelijk doel gezamenlijk persoonsgegevens willen verwerken in de vorm van casusanalyses en data-analyses. De verwachting bestaat dat de behoefte daaraan zal toenemen, nu blijkens de toename van het aantal samenwerkingsverbanden steeds meer wordt onderkend dat vraagstukken een integrale aanpak vergen waarvan het combineren en analyseren van gegevens een essentieel onderdeel uitmaakt.

6. Verhouding tot de AVG en andere wetgeving

Op de verwerking van persoonsgegevens binnen samenwerkingsverbanden is alleen de AVG van toepassing. Het gaat in dit wetsvoorstel om het in kaart brengen van benodigde interventies, niet om het verrichten van daadwerkelijke interventies. In de fase van het in kaart brengen staat nog niet vast of een eventuele interventie noodzakelijk is. Evenmin is tevoren duidelijk of deze mogelijke interventie een strafrechtelijke, bestuursrechtelijke of andere aard zou hebben. Het samenwerkingsverband doet niet aan opsporing of vervolging. Het samenwerkingsverband is ook geen bevoegde autoriteit[23] in de zin van de richtlijn, wat ook een voorwaarde is voor toepasselijkheid van de richtlijn gegevensbescherming opsporing en vervolging. Bepalend voor de toepasselijkheid van de richtlijn zijn immers (1) het zijn van bevoegde autoriteit in de zin van de richtlijn, en (2) de doeleinden waarop de verwerking van persoonsgegevens door een bevoegde instantie betrekking hebben. Deze twee voorwaarden zijn cumulatief.
De verstrekking van politiegegevens en van justitiële en strafvorderlijke gegevens door opsporingsambtenaren en officieren van justitie aan een samenwerkingsverband valt wel onder de reikwijdte van de richtlijn gegevensbescherming opsporing en vervolging. Dit betekent dat die verstrekking moet voldoen aan de vereisten zoals die zijn neergelegd in de (voorgestelde wijzigingen van) Wpg en de Wjsg.
De WGS past binnen de voorwaarden die de AVG stelt. De AVG biedt een rechtsgrond voor verwerking van persoonsgegevens, als deze voortvloeit uit een wettelijke verplichting of noodzakelijk is voor de vervulling van een taak van algemeen belang en deze taak is vastgesteld bij lidstatelijk recht.[24] De WGS biedt deze lidstatelijke basis in combinatie met krachtens de WGS vastgestelde amvb's.

De AVG biedt onder voorwaarden ook ruimte voor verstrekking van persoonsgegevens voor een ander doel dan waarvoor deze zijn verzameld. Zoals uit § 3.3.1 blijkt wordt met dit wetsvoorstel mede beoogd de mogelijkheid te scheppen om, indien daartoe in geval van een specifiek samenwerkingsverband aanleiding bestaat, daaraan voor een bepaald doel door een deelnemer persoonsgegevens te laten verstrekken, ook als dit onverenigbaar is met het doel waarvoor de gegevens oorspronkelijk zijn verzameld.

Verder gelden voor de verstrekking van persoonsgegevens aan een samenwerkingsverband als bedoeld in de WGS en de verwerking daarvan door het verband uiteraard ook de overige voorschriften uit de AVG. Dat betreft onder meer de voorschriften over de rechten van de betrokkenen en over de verplichtingen van de verwerkingsverantwoordelijken (zie hiervóór § 3.4).

De bepalingen over gegevensverwerking in sectorale wetten blijven met betrekking tot samenwerkingsverbanden als bedoeld in de WGS in beginsel hun gelding behouden. Dit geldt voor bijvoorbeeld voor de geheimhoudingsplicht uit artikel 28 Wet Bibob, waarvan geen afwijking bij wettelijk voorschrift is toegestaan. Wel geeft de WGS voor verstrekking van persoonsgegevens aan een samenwerkingsverband als bedoeld in deze wet een

[23] Bevoegde autoriteit is (a) iedere overheidsinstantie die bevoegd is voor de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, of (b) ieder ander orgaan dat of iedere andere entiteit die krachtens het recht van de lidstaten is gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen met het oog op de onder punt a genoemde doelen (artikel 3, zevende lid, RI).
[24] Artikel 6, eerste lid, onder c en e, en derde lid, aanhef en onder b, AVG.

grondslag, voor zover sectorale wetten, zoals de Algemene wet inzake rijksbelastingen en de Wet Suwi, daarvoor ruimte laten, bijvoorbeeld door te bepalen dat bij wettelijk voorschrift van een eventueel gesloten verstrekkingenregime in die wet kan worden afgeweken. Overigens staat, zoals in § 3.3.1 al naar voren is gebracht, het bestaan van deze grondslag er niet aan de in de weg dat in sectorale wetten een zelfstandige grondslag voor verstrekking wordt opgenomen. Met het oog op het specifieke karakter van strafrechtelijke gegevens gebeurt dat in de Wpg en de Wjsg. Andere wetten die een specifieke verstrekkingsgrondslag krijgen, zijn onder meer de Wet op het financieel toezicht, de Wet toezicht accountsorganisaties, de Wet toezicht trustkantoren 2018 en de Wet ter voorkoming van witwassen en financieren van terrorisme.

7. Grondrechtelijke aspecten

Het EVRM beschermt in artikel 8 het recht op respect voor het privéleven. Ingevolge het tweede lid van dit artikel is een inmenging in de uitoefening van dit recht 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.

Uit de eis dat de inmenging bij wet moet zijn voorzien, vloeit voort dat die inmenging moet berusten op een naar behoren bekend gemaakt wettelijk voorschrift waaruit de burger met voldoende precisie kan opmaken welke op zijn privéleven betrekking hebbende gegevens met het oog op de vervulling van een bepaalde overheidstaak kunnen worden verzameld en vastgelegd, en onder welke voorwaarden die gegevens met dat doel kunnen worden bewerkt, bewaard en gebruikt.[25] Het gaat hierbij om een wettelijk voorschrift in materiële zin. Dit betekent dat aan de hier bedoelde eisen van toegankelijkheid en voorzienbaarheid kan worden voldaan door een wet of amvb. De wet of amvb waarmee een specifiek (type) samenwerkingsverband wordt aangewezen zal aan eerder bedoelde eisen moeten voldoen. De WGS of amvb schrijft met het oog daarop onder meer voor, voor welk specifiek doel van zwaarwegend algemeen belang dit verband persoonsgegevens verwerkt, welke categorieën van persoonsgegevens moeten worden verstrekt, welke wijze van verwerking daarbij wordt gehanteerd en welke voorschriften gelden met betrekking tot het bewaren en vernietigen daarvan.

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 is een maatregel slechts noodzakelijk indien deze relevant is om het beoogde doel te bereiken en verder moet voldaan zijn aan het proportionaliteits- en het subsidiariteitsvereiste. In algemene zin kan worden gesteld dat samenwerkingsverbanden die op grond van de WGS zijn aangewezen, persoonsgegevens mogen verwerken ten behoeve van een gemeenschappelijke casusanalyse of data-analyse, die deelnemers met de uitkomsten van deze analyses in staat stelt op een effectievere wijze op te treden. Domeinoverstijgende, gezamenlijke gegevensverwerking is in de praktijk noodzakelijk voor zwaarwegende algemene belangen. Bij de gezamenlijke gegevensverwerking door het viertal samenwerkingsverbanden dat dit wetsvoorstel regelt (het FEC, iCOV, de RIEC's en de Zorg- en Veiligheidshuizen) gaat het om verbanden die voor essentiële maatschappelijke vraagstukken samenwerken: de integrale aanpak van – samengevat – risico's van respectievelijk: inbreuken op de integriteit van de financiële sector, van witwas- of fraudeconstructies, van georganiseerde criminaliteit, en van complexe problemen rond personen op het vlak van zorg en veiligheid. Gezamenlijke gegevensverwerking is in het bijzonder in het kader van de bestrijding van ondermijning een belangrijk instrument. Daar is het bij uitstek noodzakelijk dat meerdere partijen samenwerken en met het oog daarop (persoons)gegevens kunnen uitwisselen. Hier is in de praktijk grote behoefte aan, zo

[25] ABRvS 26 juli 2017, ECLI:NL:RVS:2017:2008.

blijkt uit signalen van medeoverheden, private partijen, en partners in het Strategisch Beraad Ondermijning (SBO). Er zijn nu geen goede, op samenwerkingsverbanden toegesneden, grondslagen voor domeinoverstijgende, gezamenlijke gegevensverwerking. Dat blijkt ook uit een advies dat de Raad van State destijds over een wijziging van de Wet op het financieel toezicht heeft uitgebracht (Kamerstukken II 2012/13, 33632, nr. 4, blz. 18-19). De WGS is hiervoor nodig. Unilaterale verstrekking is weliswaar vaak al mogelijk, maar daar gaat de WGS niet over. De WGS voorziet daarom in de noodzakelijke grondslagen voor domeinoverstijgende, gezamenlijke gegevensverwerking en voorkomt bovendien dat regels over de samenwerkingsverbanden onnodig uiteenlopen.

Wat betreft de proportionaliteit is van belang dat de gegevensverwerking dient te worden beperkt tot gegevens van de deelnemers *die noodzakelijk zijn voor de taak van het samenwerkingsverband*. Op grond van artikel 7 kunnen de deelnemers slechts het resultaat van die verwerking terugontvangen van het samenwerkingsverband, indien de verstrekking van deze resultaten noodzakelijk is voor de vervulling van een publiekrechtelijke taak die aan de deelnemer is opgedragen, wanneer deze verenigbaar is met het doel van het samenwerkingsverband, of indien het een private deelnemer zonder publiekrechtelijke taak betreft, ten behoeve van de behartiging van de gerechtvaardigde belangen of wettelijke verplichtingen van deze private deelnemer, wanneer deze verenigbaar zijn met het doel van het samenwerkingsverband.

Wat betreft de subsidiariteit geldt dat niet kan worden volstaan met lichtere, minder ingrijpende instrumenten. Hiervoor wordt verwezen naar de uitvoerige knelpuntenanalyse die reeds heeft plaatsgevonden, waarvan paragraaf 3.3 van deze memorie van toelichting een samenvatting vormt. Samenwerkingsverbanden moeten derhalve voor gezamenlijke, domeinoverstijgende gegevensverwerking worden voorzien van een wettelijke grondslag voor die gegevensverwerking.

Of de gegevensverwerking in een samenwerkingsverband ook in een concreet geval aan de hier genoemde vereisten voldoet, zal moeten worden getoetst voorafgaand aan de aanwijzing van het samenwerkingsverband en derhalve bij de voorbereiding van de wet of amvb waarmee het verband wordt aangewezen.

Dat de inmenging noodzakelijk moet zijn met het oog op een van de in artikel 8 EVRM genoemde belangen, brengt mee dat het doel van zwaarwegend algemeen belang waarvoor binnen een samenwerkingsverband als bedoeld in de WGS persoonsgegevens worden verwerkt, een doel dient te zijn dat ten minste ook een of meer van de in het EVRM genoemde belangen vertegenwoordigt. Daarmee zal rekening moeten worden gehouden in de wet of amvb waarin het desbetreffende doel van zwaarwegend algemeen belang uitdrukkelijk wordt omschreven. Paragraaf 4 van deze memorie van toelichting beschrijft dit voor de vier (clusters van) samenwerkingsverbanden die in dit wetsvoorstel worden aangewezen als samenwerkingsverband in de zin van de WGS. Bij het FEC, iCOV, de RIEC's en de Zorg- en Veiligheidshuizen gaat het om verbanden die voor essentiële maatschappelijke vraagstukken samenwerken: de integrale aanpak van – samengevat – risico's van respectievelijk: inbreuken op de integriteit van de financiële sector, van witwas- of fraudeconstructies, van georganiseerde criminaliteit, en van complexe problemen rond personen op het vlak van zorg en veiligheid. De gegevensverstrekking dient aldus belangen die in het tweede lid van artikel 8 van het EVRM worden genoemd: onder meer het voorkomen van wanordelijkheden en strafbare feiten en de bescherming van de rechten en vrijheden van anderen.

Het Handvest van de grondrechten van de Europese Unie legt in artikel 8 het recht vast op bescherming van persoonsgegevens. Op basis van dit artikel moeten gegevens eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van betrokkenen of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Verder bepaalt dit artikel dat eenieder recht heeft op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan en dat een onafhankelijke autoriteit toeziet op de naleving. De WGS en de krachtens deze wet vast te stellen amvb's zullen voorzien in een gerechtvaardigde grondslag voor de gegevensverwerking door onder de WGS vallende

samenwerkingsverbanden en in voorschriften voor een eerlijke verwerking voor specifieke doeleinden. De overige hier genoemde vereisten uit artikel 8 van het handvest worden ingevuld door de AVG en de Uitvoeringswet AVG. Zo zijn in de AVG geregeld de beginselen inzake verwerking van persoonsgegevens (artikel 5), de rechten van betrokkene (artikelen 12-23), privacy by design (artikel 25), de verplichting tot een register van de verwerkingsactiviteiten (artikel 30), de verplichting tot beveiliging (artikel 32), de verplichting om een gegevensbeschermingseffectbeoordeling uit te voeren (artikel 35) en voorafgaande raadpleging (artikel 36).

De Grondwet geeft in artikel 10, eerste lid, eenieder, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer. Ook dit recht is niet absoluut: bij of krachtens de wet kunnen daaraan beperkingen worden gesteld. De argumenten die hierboven zijn gegeven ter rechtvaardiging van de inbreuk op het recht op respect voor het privéleven in artikel 8 van het EVRM, gelden evenzeer ter onderbouwing van de wettelijke beperkingen op grond van artikel 10 van de Grondwet.

8. Overige aspecten

8.1 Uitkomsten gegevensbeschermingseffectbeoordeling

De AVG schrijft in artikel 35 voor in welke gevallen van gegevensverwerking een zgn. gegevensbeschermingseffectbeoordeling (PIA) dient te worden uitgevoerd. Voor de vier (clusters van) samenwerkingsverbanden die in dit wetsvoorstel worden aangewezen als samenwerkingsverband in de zin van de WGS, zijn PIA's uitgevoerd. De uitkomsten van de PIA zijn meegenomen bij de vormgeving van het wetsvoorstel. Dit heeft tot de volgende aanpassingen geleid.

De zeggenschap van een individuele deelnemer over de verstrekking van de resultaten van de verwerking aan een derde is vergroot door niet meer te eisen dat hij daartegen zwaarwegende redenen moet aanvoeren. Voldoende is dat hij daartegen bezwaar heeft. Dit verkleint de mate waarin die uitkomsten met inbegrip van eventuele persoonsgegevens aan derden worden verstrekt.

Buiten de mogelijkheden die artikel 8, eerste lid, biedt om de deelname van banken en andere financiële ondernemingen aan verwerkingen door het FEC te beperken, is deze deelname als gevolg van de PIA voor het FEC in artikel 12, onder h, verdergaand geclausuleerd door te bepalen dat zij zich beperkt tot bij amvb te beschrijven specifieke verwerkingen of onderdelen daarvan. Op basis daarvan zal deze deelname bij amvb worden beperkt tot de verwerkingen in de Terrorismefinanciering Taskforces en de Serious Crime Taskforces. Verder is het aantal overheidsinstanties dat in artikel 12 als reguliere deelnemer wordt aangewezen, beperkt door die instanties die uitsluitend aan een aantal specifiek verwerkingen of onderdelen daarvan deelnemen, met die restrictie bij amvb aan te wijzen. Het betreft hier de Immigratie- en Naturalisatiedienst, de Koninklijke marechaussee, het Bureau Financieel Toezicht en de Algemene Inlichtingen – en Veiligheidsdienst, die alle in beperkte zin alleen aan het programma FEC Terrorismefinanciering deelnemen (zie ook par. 4.1).
Uit een oogpunt van voorzienbaarheid is aan artikel 15 een bepaling toegevoegd die voorschrijft dat bij amvb nadere regels worden gesteld over de criteria om een bepaalde casus voor te dragen voor het casusoverleg van het FEC, waaronder de aard, de eisen van kwaliteit en betrouwbaarheid waaraan de casus moet voldoen.

Als gevolg van de PIA voor iCOV zijn de verwerkingsmethoden van iCOV die de drie standaardrapportages iRVI, iRR en iRT NN opleveren, en de beoogde nieuwe methode, iRT compact (zie par. 4.2) specifiek in de WGS omschreven. Verder worden in par. 4.2. verschillende waarborgen genoemd die iCOV toepast, waaronder privacy enhancing technologies.

De DPIA voor de RIEC's heeft ertoe geleid dat in artikel 36 nauwkeuriger voor elke fase van verwerking is aangegeven welke persoonsgegevens mogen worden gebruikt. In de toelichting op artikel 31a is benadrukt dat de analyses van handhavingsknelpunten en de

gebieds- of wijkscans en nulmetingen in statistische beelden uitmonden die geen persoonsbeelden bevatten.

Tot slot heeft de DPIA voor de Zorg- en Veiligheidshuizen tot gevolg gehad dat in artikel 47 uit een oogpunt van een betere voorzienbaarheid van de verwerkingen die daar plaatsvinden, een expliciete verwijzing naar de behandeling van complexe casuïstiek is opgenomen. Verder is in par. 4.4. vastgelegd dat bij de voorbereiding van de amvb, bedoeld in artikel 8, negende lid, zal worden bezien welke waarborgen uit het privacyprotocol van de Zorg- en Veiligheidshuizen in aanvulling op de waarborgen van artikel 8 en 8a in die amvb voor de Zorg- en Veiligheidshuizen zullen worden vastgelegd.

8.2 Financiële aspecten

Voor zover dit wetsvoorstel bestaande verwerkingsactiviteiten van de vier samenwerkingsverbanden codificeert, heeft het voorstel geen financiële gevolgen, administratieve lasten of bestuurslasten.
Voor iCOV geldt dat de WGS op haar verzoek een nieuwe verwerkingsmethode introduceert: de themascan. Het gebruik van die methode is niet verplicht. Het is aan de deelnemers van iCOV om te beslissen deze methode daadwerkelijk verder te ontwikkelen en in beheer te gaan nemen. Als dat het geval is, zullen zij ook voor dekking van de kosten moeten zorgen.
Het wetsvoorstel noemt in de artikelen 8, 8a en 8b een aantal waarborgen die bij of krachtens amvb zullen worden uitgewerkt. Daarbij gaat het bijvoorbeeld om het registreren van bepaalde onderdelen van de verwerkingen met het oog op controle en toezicht op de naleving van de verplichtingen die op de samenwerkingsverbanden rusten bij het verwerken van persoonsgegevens. Een andere waarborg is de instelling van een zgn. rechtmatigheidscommissie die de rechtmatigheid van de gegevensverwerking door het desbetreffende samenwerkingsverband beoordeelt. Deze waarborgen zullen mogelijk uitvoeringslasten meebrengen, al kan een deel van deze waarborgen worden aangemerkt als waarborgen ter nadere invulling van voorschriften die ook al uit de AVG voortvloeien. Zo kan voornoemde registratie worden gezien als een in artikel 32, eerste lid, onder b, AVG bedoelde passende technische en organisatorische maatregel om "het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingsdiensten en systemen te garanderen". De uitvoeringslasten van de instelling van een rechtmatigheidscommissie kunnen ook zeer beperkt blijven als bij amvb wordt bepaald dat deze zoveel mogelijk worden samengesteld uit privacy-officers van de deelnemende organisaties. De vormgeving van de waarborgen zal bij of krachtens amvb worden geregeld. Pas dan is het mogelijk een uitvoeringstoets te doen. De mogelijke financiële consequenties die uit de amvb's voortvloeien, worden specifiek gedekt binnen de begroting van de betrokken organisaties betreffende het samenwerkingsverband.
In artikel 9a wordt voorgeschreven dat het samenwerkingsverband jaarlijks een jaarverslag opstelt waarin een verantwoording wordt gegeven van de effectiviteit en bruikbaarheid van de resultaten van de gegevensverwerking door het verband. Hiermee wordt invulling gegeven aan het vereiste van de noodzakelijkheid van de gegevensverwerking, zoals dat in artikel 5, eerste lid, onder c, AVG, is vastgelegd. In zoverre valt deze waarborg als een normaal onderdeel van de control-cyclus worden aangemerkt.

9. Advies Autoriteit persoonsgegevens

9.1 Eerste advies

De AP bracht op 4 januari 2019 advies uit. Naar aanleiding van het advies is het wetsvoorstel aangepast op diverse punten.

Er is een aantal andere aanpassingen gepleegd, geheel of gedeeltelijk, naar aanleiding van het advies:

- De mogelijkheid om regels te stellen over de onderlinge verantwoordelijkheidsverdeling in een samenwerkingsverband is vervangen door een verplichting (artikel 4, vierde lid).

- Geregeld is dat de deelnemers één functionaris gegevensbescherming aanwijzen voor het samenwerkingsverband (artikel 4, tweede lid). Dit voorkomt onduidelijkheden.
- De grondslagen voor subdelegatie naar het niveau van ministeriële regeling zijn grotendeels geschrapt naar aanleiding van de opmerking van de AP dat het bij de aanwijzing van de deelnemers, de wijze van verwerking en de invulling van de waarborgen gaat om aspecten die zodanig belangrijk zijn voor de bescherming van persoonsgegevens dat naar verwachting maar in beperkte mate sprake zal kunnen zijn van voorschriften die volgens staand wetgevingsbeleid in een ministeriële regeling kunnen worden neergelegd.

Niet overgenomen punten
Gelet op het advies van de Afdeling advisering van de Raad van State is het advies niet overgenomen om expliciet te regelen dat een kandidaat-deelnemer kan worden aangewezen na zijn instemming.

De AP noemt drie alternatieven. Het eerste alternatief houdt in dat in principe wordt volstaan met de bestaande wetgeving, dat betere naleving daarvan wordt bevorderd en dat slechts incidenteel de wetgeving wordt aangepast indien een inventarisatie van de knelpunten daartoe aanleiding geeft. Dit advies gaat voorbij aan de uitvoerige knelpuntenanalyse die reeds heeft plaatsgevonden, waarvan paragraaf 3.3 van deze memorie van toelichting een samenvatting vormt. Het advies gaat hier niet op in, maar weerspreekt niet dat samenwerkingsverbanden voor gezamenlijke, domeinoverstijgende gegevensverwerking moeten worden voorzien van een wettelijke grondslag voor die gegevensverwerking. De Afdeling advisering van de Raad van State overweegt overigens in haar advies dat de overheid ernstige en ondermijnende criminaliteit moet kunnen voorkomen, opsporen en bestrijden en dat bestuursorganen die gegevens hebben over zulke criminaliteit die gegevens daartoe moeten kunnen uitwisselen met elkaar en ook met private partijen, zodat zij effectief kunnen optreden. De Afdeling advisering onderschrijft nut en noodzaak van een wettelijke regeling.

Het tweede alternatief is het invoeren van een mechanisme dat vergelijkbaar is met de melding ongebruikelijke transacties, namelijk een melding "ongebruikelijke en mogelijk ondermijnende transactie". Het is lastig om inspiratie te ontlenen aan het mechanisme van de melding ongebruikelijke transacties, omdat bij de WGS (onder meer) risicomeldingen – anders dan bij de melding ongebruikelijke transacties – niet het startpunt maar het product van de gegevensverwerking moeten zijn. Daardoor gaat de vergelijking mank. Ook gaat deze variant voorbij aan de behoefte aan een bredere scope, maar ook aan de knelpunten, zoals die in bestaande samenwerkingsverbanden worden ervaren.
Het derde alternatief, "Versterken bestaande mogelijkheid AVG", houdt in dat de mogelijkheid uit artikel 36, vijfde lid, AVG wordt gebruikt, om bij nationale wet gevallen aan te wijzen waarin de AP om voorafgaande toestemming dient te worden verzocht. Dit alternatief is bij nadere afweging niet overgenomen omdat voorafgaande toestemming van de AP zou betekenen dat de uitvoering van het wetsvoorstel, nadat dit door het parlement is aangenomen, de facto afhankelijk wordt gesteld van de toestemming van een zelfstandig bestuursorgaan. De Afdeling advisering van de Raad van State schreef in haar advies op het onderhavige wetsvoorstel over voorafgaande toestemming: "Deze bepaling is weliswaar gebaseerd op de AVG maar is in de praktijk niet zonder problemen: het houdt in dat de AP intensief wordt betrokken bij een bestuurlijke afweging, die niet gemaakt zou moeten worden door de toezichthouder maar door het bevoegde en aanspreekbare bestuursorgaan. Dat orgaan is bovendien beter op de hoogte van de elementen die op zijn eigen specifieke werkterrein afgewogen moeten worden dan de algemene toezichthouder. Daar komt bij dat het verlenen van toestemming gelet op de complexiteit van de materie en de verschillende belangen die in het geding zijn, een omvangrijk onderzoek noodzakelijk zal maken."
Om wel te voorzien in aanvullende waarborgen, zijn diverse andere waarborgen toegevoegd aan het wetsvoorstel. Tot slot biedt het instrument van voorafgaande raadpleging uit de AVG een belangrijke waarborg (zie paragraaf 3.5).

Bezwaren van de AP tegen het wetsvoorstel
De AP heeft ernstige bezwaren vanuit rechtsstatelijk perspectief. Kern van de kritiek is dat de delegatiegrondslagen in de WGS –in theorie– schier oneindige mogelijkheden bieden. Daardoor zou het risico bestaan op omzeiling van fijnzinnige structuren en waarborgen uit de specifieke wetten die op de deelnemers aan het samenwerkingsverband normaal gesproken van toepassing zijn. Grote bezwaren zijn de (on)evenredigheid en de te ruime reikwijdte van de WGS. Doelbinding is in de WGS niet meer de natuurlijke begrenzing. Bovendien maakt een dergelijk ruime delegatiebepaling volgens de AP inbreuk op het primaat van de (formele) wetgever.

Aan de voornaamste bedenkingen van de AP is voldaan door vier (clusters van) samenwerkingsverbanden in het wetsvoorstel zelf te regelen in plaats van bij amvb. Weliswaar kunnen volgens het wetsvoorstel vanwege de flexibiliteit daarnaast samenwerkingsverbanden bij amvb worden aangewezen, maar dit is slechts mogelijk binnen de beperkte reikwijdte van hoofdstuk 3 en na toepassing van een bijzondere nahangprocedure bij het parlement.

De stelling van de AP dat de WGS tot een ernstige verwatering van de rechtstatelijke uitgangspunten zal leiden die voor de verschillende rechtsgebieden gelden, wordt niet onderschreven. In het licht van voetnoot 5 waarin deze uitgangspunten zijn beschreven, lijkt het vooral te gaan om de onschuldpresumptie in het strafrecht die meebrengt dat eerst bij een verdenking van een strafbaar feit bijzondere bevoegdheden tot het verzamelen van persoonsgegevens beschikbaar komen waarvan de uitoefening aan relatief zware voorwaarden dient te voldoen. De WGS laat een rechtsstatelijk uitgangspunt als dit evenwel volledig in stand: zij doet in geen enkel opzicht afbreuk aan de wettelijke waarborgen die gelden vanaf het moment waarop een verdenking ontstaat. De stelling van de AP dat in het strafrecht het verbod van zelfincriminatie en de presumptie van onschuld ernstig dreigen te worden gerelativeerd, mist dan ook grond. De AP lijkt er ook aan voorbij te gaan dat de scheiding tussen de verschillende rechtsgebieden nu al niet absoluut is. Er zijn immers nu al talrijke bepalingen die het mogelijk maken om persoonsgegevens uit het ene rechtsgebied te benutten binnen een ander rechtsgebied (bijvoorbeeld het Besluit politiegegevens en de Uitvoeringsregeling Awr). Anders dan de AP stelt, valt niet in te zien waarom de WGS veel beschermende normen in belangrijke mate zou uithollen. De WGS bevat aanvullende waarborgen, onder meer in artikel 8 en volgende. De door de AP veronderstelde relativering van bestuursrechtelijke beginselen doet zich onder de WGS evenmin voor.

Dat verantwoordelijkheden door de WGS worden veralgemeniseerd, valt evenmin in te zien. Aan de bestaande verantwoordelijkheden van overheidsinstanties voor de uitoefening van hun taken en bevoegdheden wordt immers niet getornd. Ook de veronderstelling dat private partijen verantwoordelijk worden voor publieke taken/verwerkingen is in haar algemeenheid onjuist. In de toedeling van publieke taken brengt de WGS geen verandering, zoals wordt geëxpliciteerd in het voorgestelde artikel 3, vierde lid. Helder blijft wat overheidstaken zijn en wat niet. Dat laat onverlet dat er overheidstaken kunnen zijn waarmee min of meer dezelfde doelen worden nagestreefd als die welke door private partijen kunnen worden nagestreefd, zoals het tegengaan van fraude. Het is mede voor dit type gemeenschappelijke doelen waarvoor samenwerkingsverbanden in het leven worden geroepen.

Dat een instantie die zelf niet bevoegd is bepaalde gegevens te verzamelen, die gegevens op grond van de WGS kan verkrijgen van een andere deelnemer die wel bevoegd is die gegevens te verzamelen, is als constructie niet uitzonderlijk. Zij is niet wezenlijk anders dan andere, al bestaande legitieme constructies waarin instanties bepaalde gegevens mogen doorverstrekken aan andere instanties. Het principe van doelbinding is geen absoluut beginsel. Artikel 6, vierde lid, AVG staat ook verdere verwerking voor een niet-verenigbaar doel toe, mits wettelijk geregeld en in het kader van een zwaarwegend algemeen belang. Het wetsvoorstel beoogt zo'n grondslag te bieden.

Anders dan het advies impliceert, betekent dit niet dat alle persoonsgegevens van de deelnemers in één groot bestand worden samengevoegd, dat alle deelnemers vrijelijk kunnen raadplegen. Het samenwerkingsverband verwerkt de ontvangen gegevens; het gaat hierbij volgens artikel 5 slechts om de gegevens die noodzakelijk zijn voor de taak van het samenwerkingsverband. Op grond van artikel 7 van het wetsvoorstel kan het samenwerkingsverband vervolgens het *resultaat* van die verwerking verstrekken aan de deelnemende bestuursorganen. De deelnemers mogen dus niet vrijelijk elkaars databestanden raadplegen.

Dat een afwijking van een wettelijke geheimhoudingsbepaling bij amvb zou geschieden is, is anders dan de AP stelt, niet aan de orde. Hoofdstuk 4 van het wetsvoorstel bevat afwijkingen van wettelijke geheimhoudingsplichten en artikel 5 vormt een uitzondering op wettelijke geheimhoudingsplichten die de ruimte scheppen om bij wettelijk voorschrift of wettelijke plicht een uitzondering te maken.

9.2 Aanvullend advies

Naar aanleiding van het eerste advies van de AP is het wetsvoorstel aangepast en eind februari 2019 voorgelegd aan de AP. Op 19 april 2019 heeft de AP haar aanvullende advies uitgebracht.

1. De AP merkt op dat het karakter van een brede kaderwet van onbepaalde duur die een nog onbekende maar potentieel forse inbreuk op de bescherming van persoonsgegevens maakt, op gespannen voet staat met de eisen die het EU-recht op dit punt aan de wetgeving stelt. Pas bij de latere amvb's kan volgens de AP worden beoordeeld of de wezenlijke inhoud van het grondrecht op bescherming van persoonsgegevens zal worden geëerbiedigd en of de verwerkingen noodzakelijk zijn. Als gevolg van het karakter van een inhoudelijk neutrale kaderwet hangt de vraag of de in het eerdere advies geschetste risico's inzake uitholling van rechtstatelijke waarborgen zich ook daadwerkelijk zullen verwezenlijken, vrijwel volledig af van de inhoud van de amvb's. De AP stelt dat de materiële en temporele reikwijdte vrijwel onbegrensd is. Ook wijst de AP erop dat het brede, facultatieve karakter van het wetsvoorstel niet leidt tot regulering en harmonisatie van de gegroeide praktijk aan samenwerkingsverbanden.

Aan de voornaamste bedenkingen van de AP is voldaan door vier (clusters van) samenwerkingsverbanden in het wetsvoorstel zelf te regelen in plaats van bij amvb. Weliswaar kunnen volgens het wetsvoorstel vanwege de flexibiliteit daarnaast samenwerkingsverbanden bij amvb worden aangewezen, maar dit is slechts mogelijk binnen de beperkte reikwijdte van hoofdstuk 3 en na toepassing van een bijzondere nahangprocedure bij het parlement. De stelling van de AP dat het wetsvoorstel een nog onbekende maar potentieel forse inbreuk op de bescherming van persoonsgegevens maakt, kunnen wij dan ook niet delen. Evenmin delen wij de daaraan gekoppelde conclusie van de AP dat het karakter van de wet op gespannen voet staat met de eisen die het EU-recht op dit punt aan de wetgeving stelt.
Voor zover binnen de beperkte reikwijdte van hoofdstuk 3 van het wetsvoorstel samenwerkingsverbanden bij amvb kunnen worden aangewezen, is bovendien allerminst sprake van een blanco delegatie. Integendeel, die gedelegeerde regelgevende bevoegdheid wordt door de formele wetgever begrensd door allerhande voorwaarden en waarborgen. Bovendien moet de regering straks bij het opstellen van de amvb's uiteraard binnen de grenzen van de AVG opereren. Wij zien daarom ook niet in waarom het karakter van dit wetsvoorstel in strijd zou zijn met de eisen die het EU-recht stelt. De reikwijdte van de delegatiegrondslagen mag overigens ruim zijn: zowel het EVRM als de AVG kennen een materieel wetsbegrip.
De AP stelt dat een brede kaderwet een rechtvaardiging zou kunnen vinden als deze de gegroeide praktijk aan samenwerkingsverbanden zou reguleren voor alle samenwerkingsverbanden. Gelet op de verscheidenheid aan samenwerkingsverbanden achten wij dat geen begaanbare weg. Voor een deel van de samenwerkingsverbanden bestaat geen noodzaak tot gezamenlijke verwerking van persoonsgegevens, bijvoorbeeld omdat zij geen persoonsgegevens verwerken, omdat zij louter bilateraal persoonsgegevens verwerken, en/of omdat zij behoorlijk kunnen functioneren met

bestaande grondslagen voor gegevensverwerking, zoals grondslagen uit sectorale wetgeving, de grondslag om ten behoeve van wetenschappelijk onderzoek en statistiek persoonsgegevens te verwerken, of de grondslag om persoonsgegevens verder te verwerken voor verenigbare doelen. Voor wat betreft de samenwerkingsverbanden die onder de WGS worden aangewezen, heeft de WGS natuurlijk wel een harmoniserende werking.

2. De AP adviseert om de inzet op een brede facultatieve kaderwet te heroverwegen en daarbij te bezien of een op concrete, bestaande samenwerkingsverbanden toegespitst wetsvoorstel, zo mogelijk met een tijdelijk karakter, de komende tijd mogelijk al voldoende voorziet in een oplossing voor de geconstateerde knelpunten.

De heroverweging heeft ertoe geleid dat vier (clusters van) samenwerkingsverbanden in het wetsvoorstel zelf zijn opgenomen.

3. Indien de opzet ongewijzigd blijft, adviseert de AP te bepalen dat de wet vijf jaar na inwerkingtreding wordt geëvalueerd waarbij in het bijzonder de reikwijdte voorwerp van aandacht zal moeten zijn. Ook adviseert de AP om te bepalen dat elke amvb uiterlijk 5 jaar na inwerkingtreding vervalt, behoudens verlenging bij amvb na evaluatie (horizonbepaling). Zodoende is periodieke heroverweging van de noodzaak van het desbetreffende samenwerkingsverband gegarandeerd.

Met de AP zijn wij van mening dat het zinvol is om na vijf jaren de afweging te maken of een samenwerkingsverband nog steeds noodzakelijk is en of de wet op de juiste manier functioneert. Het wetsvoorstel is dan ook aangepast met een verplichting om zowel de wet als de amvb's na vijf jaar te evalueren. Een horizonbepaling daarentegen achten wij hier niet op zijn plaats. Het gaat immers naar zijn aard niet om een tijdelijk probleem of een tijdelijk fenomeen. Het is duidelijk dat er altijd behoefte zal zijn aan het delen van informatie en dus ook persoonsgegevens. Natuurlijk kan het door gewijzigde omstandigheden zo zijn dat een samenwerkingsverband overbodig wordt of dat er geen behoefte meer is aan de deelname van bepaalde partijen of het gebruik van bepaalde persoonsgegevens. Maar in dat geval wordt de samenwerking beëindigd of wordt de reikwijdte ervan beperkt.

4. De AP adviseert primair om de meest vergaande inbreuken op grondrechten niet te onttrekken aan de volle betrokkenheid van de formele wetgever en adviseert subsidiair om voor de amvb's een zogenoemde voorhangprocedure bij het parlement voor te schrijven.

Ook aan deze bedenkingen van de AP is voldaan door vier (clusters van) samenwerkingsverbanden in het wetsvoorstel zelf te regelen in plaats van bij amvb. Voor zover daarnaast samenwerkingsverbanden bij amvb kunnen worden aangewezen, is dat slechts mogelijk na toepassing van een bijzondere nahangprocedure bij het parlement.

5. De AP adviseert om de memorie van toelichting aan te vullen met een concrete casusbeschrijving van een bij amvb aangewezen samenwerkingsverband waaruit in het bijzonder duidelijk blijkt welke voorschriften in een amvb als beoogd zullen worden opgenomen.

In hoofdstuk 2 van het aangepaste wetsvoorstel is een viertal (clusters van) samenwerkingsverbanden geregeld.

6. De AP adviseert in de toelichting een uiteenzetting op te nemen over de gevolgen van toepasselijkheid in voorkomend geval van het richtlijnregime in relatie tot samenwerkingsverbanden en de bepalingen van het wetsvoorstel en zo nodig ook bij de casusbeschrijving hier aandacht aan te schenken.

Aan het begin van paragraaf 6 van deze memorie is de uiteenzetting toegevoegd.

7. De AP adviseert in het wetsvoorstel voor te schrijven dat de amvb nauwkeurig bepaalt wat de resultaten van de verwerking zijn en in welke vorm deze worden verstrekt.

Gelet op het uitgangspunt van dataminimalisatie delen wij de opvatting van de AP dat het wetsvoorstel of de amvb nauwkeurig moet bepalen wat de resultaten van de verwerking zijn. Dit wordt dan ook geregeld in het wetsvoorstel dan wel de amvb, afhankelijk van de vraag op welk niveau het samenwerkingsverband wordt aangewezen.

8. De AP adviseert de geheimhoudingsbepaling zo te formuleren dat deze niet alleen geldt voor organisaties ten opzichte van derden, maar ook voor natuurlijke personen ten opzichte van de eigen organisatie en derden, voor zover het gaat om andere gegevens dan de resultaten van de verwerking.

De AP wijst terecht op het onderscheid tussen een geheimhoudingsplicht die slechts rust op de organisatie en een geheimhoudingsplicht die rust op een natuurlijke persoon. Hoewel een dergelijke beperkte reikwijdte van de geheimhoudingsplicht ook niet is beoogd, vinden wij het bij nader inzien toch zinvol om dit in het wetsvoorstel buiten twijfel te stellen. Met het oog daarop bevat het nieuwe artikel 9, eerste lid, een geheimhoudingsplicht voor degenen die betrokken zijn bij de werkzaamheden van het samenwerkingsverband en daarbij de beschikking krijgen over persoonsgegevens en voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift ter zake van die gegevens een geheimhoudingsplicht geldt.
Artikel 9, tweede lid, bevat een (afgeleide) geheimhoudingsplicht voor de ontvangers van de resultaten, voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift ter zake van die gegevens een geheimhoudingsplicht geldt.

9. De AP adviseert de bevoegdheid tot het aanwijzen van deelnemers neer te leggen bij de minister die het aangaat en per deelnemer een regulier besluit op aanvraag te laten nemen.

Voor zover mogelijk hebben wij bij de vier (clusters van) samenwerkingsverbanden de deelnemers in het wetsvoorstel opgenomen, omdat het bij de aanwijzing van de deelnemers gaat om de kern en de aard van het samenwerkingsverband. Niettemin delen wij de opvatting van de AP uit het aanvullend advies in zoverre dat het bij amvb aanwijzen van concrete - ook private - partijen zich soms minder goed verhoudt met de vereiste snelle aanpassing van de samenstelling van het samenwerkingsverband. Daarom achten wij het passend om het in bepaalde gevallen mogelijk te maken om bij of krachtens amvb deelnemers aan te wijzen. Die mogelijkheid blijft dan wel beperkt tot het aanwijzen van deelnemers die onderdeel uitmaken van een reeds in het wetsvoorstel aangewezen categorie, zoals overheidsinstanties of banken.

10. De AP adviseert het wetsvoorstel zo in te richten dat het besluit tot aanwijzing het recht geeft om deel te nemen aan het samenwerkingsverband, maar niet de verplichting daartoe.

Indien de wettelijke aanwijzing als deelnemer niet de verplichting geeft om deel te nemen, zou dat betekenen dat een deelnemer van de ene op de andere dag uit het samenwerkingsverband zou kunnen treden. Dat zou zeer ongewenst zijn met het oog op het doel waarvoor een samenwerkingsverband is opgericht en de continuïteit ervan. Met de Afdeling advisering van de Raad van State[26] zijn wij van mening dat de wetgever zijn verantwoordelijkheid moet nemen gelet op de zwaarwegende publieke belangen waar het hier om gaat.

11. De AP adviseert zodanige wettelijke voorzieningen te treffen dat bij uittreding van een deelnemer is gegarandeerd dat onverminderd recht wordt gedaan aan de beginselen.

[26] Zie paragraaf 2, onder c, van het advies van de Afdeling advisering van de Raad van State.

We zijn het uiteraard eens met de AP dat recht gedaan moet worden aan de beginselen die gelden voor het verwerken en beschermen van persoonsgegevens. Die verplichting vloeit ook voort uit artikel 5 AVG. Bij uittreding vloeit daarnaast uit het wetsvoorstel voort dat de gegevenstoevoer door de uittredende deelnemer per direct moet worden beëindigd en dat de uittredende deelnemer per direct moet stoppen met de verwerking van gegevens binnen het samenwerkingsverband. De verwerkingsgrondslagen zijn immers alleen van toepassing op deelnemers.
Een uitgetreden deelnemer ontvangt niet langer op grond van artikel 7, eerste lid, de resultaten. Voor wat betreft reeds ontvangen resultaten geldt dat de ontvanger deze mag verwerken zolang dat noodzakelijk is voor de (afronding van) de vervulling van de doeleinden waarvoor deze gegevens op grond van artikel 7 zijn verkregen. Daarna mogen de gegevens in beginsel niet meer worden bewaard, afhankelijk van het gegevensbeschermingsregime dat op de ontvangende verwerkingsverantwoordelijke van toepassing is.

12. De AP adviseert de toelichting aan te vullen met een duiding van de geschatte omvang van de voor de AP nieuwe taak inzake "voorafgaande toestemming" en, eventueel meerjarig, de bekostiging daarvan.

In paragraaf 9.1 is toegelicht waarom "voorafgaande toestemming" niet is opgenomen in het wetsvoorstel.

10. Overige consultatiereacties

Dit wetsvoorstel stond open voor (internet)consultatie van 6 juli tot 20 september 2018. Er zijn 72 burgerreacties ontvangen en 21 reacties van organisaties: de AP, Amnesty, College voor de rechten van de mens, FEC (Financieel Expertise Centrum), FIU, iCOV, Koninklijke Notariële Beroepsorganisatie, NJCM, Nederlandse Vereniging van Banken, NOvA, NVvR, OM, Piratenpartij, Platform Bescherming Burgerrechten, Politie, Privacy barometer, Privacy first, Reclassering, Regioburgemeesters, Verbond van verzekeraars en VNG.
Het advies van de AP is in de vorige paragraaf apart behandeld.

Steunbetuigingen zijn ontvangen van:
- *FEC:* "stap in de goede richting bij de totstandkoming van een sterkere en effectievere publiek-private samenwerking in de bestrijding van financieel-economische criminaliteit";
- *iCOV:* "een solide basis … aan samenwerkingsverbanden om hun werkzaamheden efficiënt, effectief en juridisch verankerd uit te voeren";
- *OM:* "instemming en waardering van het wetsvoorstel";
- *Politie:* "een oplossing … voor het juridisch complexe vraagstuk van de uitwisseling van persoonsgegevens door partijen in samenwerkingsverbanden";
- *VNG en Bureau Regioburgemeesters:* "goede ontwikkeling dat er een wettelijk raamwerk met meer mogelijkheden wordt gemaakt voor informatie-uitwisseling in samenwerkingsverbanden";
- *NOvA:* "onderkent de wenselijkheid gegevensverwerking en -uitwisseling in samenwerkingsverbanden van een betere wettelijke grondslag te voorzien";
- *Koninklijke Notariële Beroepsorganisatie:* "juicht het wetsvoorstel, dat met de nodige privacywaarborgen een wettelijke basis voor gegevensdeling binnen samenwerkingsverbanden doet ontstaan, …toe";
- *Reclassering Nederland:* "Een wettelijke regeling voor gegevensuitwisseling in samenwerkingsverbanden acht RN wenselijk".

Enigszins positieve reacties zijn ontvangen van:
- *NJCM:* "verwelkomt … dat het kabinet de tot nu toe informele samenwerkingsverbanden voor het uitwisselen van data tussen verschillende overheidsinstanties onderling… formeel wil vormgeven… [maar] is tegelijkertijd

uitermate bezorgd over de huidige opzet van de WGS… Volgens het NJCM dient de instelling van een samenwerkingsverband plaats te vinden per formele wet";
- *Nederlandse Vereniging van Banken:* "De NVB en banken ondersteunen deze ambitie… Tegelijk bestaat er in de voorgestelde opzet nog te veel onduidelijkheid over onder meer de feitelijke reikwijdte van de wet, de privacy van burgers en klanten, de mate waarin medewerking en samenwerking al dan niet op basis van vrijwilligheid geschiedt en de voorgestelde wijzigingen in de geheimhoudingsplicht van toezichthouders die mogelijk deelnemer zijn in een bij amvb aangewezen samenwerkingsverband".

Gedurende de consultatie zijn evenwel ook veel kritische reacties ontvangen. Deze kritiek richt zich vooral op de volgende hoofdpunten:

1. De *inbreuk op de privacy is niet gerechtvaardigd*, onder meer omdat de wettelijke basis niet voldoende duidelijk en precies is, niet is voldaan aan het voorzienbaarheidsvereiste en sprake is van een "big data carte blanche" (o.a. AP, College voor de Rechten van de Mens, Amnesty, Platform bescherming burgerrechten, Privacy First, burgerreacties). NVvR vindt het juridisch kader gelet op EVRM en EU-recht echter voldoende onderbouwd, maar zij benadrukt dat de uitkomst van een data-analyse pas na beoordeling door de verantwoordelijke autoriteiten (m.n. het OM) een verdenking oplevert.

Wat betreft de precisie van de wettelijke basis is van belang dat het wetsvoorstel zo precies mogelijk de doelstellingen van de gegevensverwerking door samenwerkingsverbanden regelt. Deze doelstellingen zijn zo concreet mogelijk geregeld voor de vier (clusters van) samenwerkingsverbanden die in het wetsvoorstel zijn opgenomen. Dat is in lijn met artikel 5, eerste lid, onder b, AVG, dat verplicht tot "welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden". Voor zover samenwerkingsverbanden bij amvb kunnen worden aangewezen, moet de doelstelling voldoen aan de beperkte reikwijdte van hoofdstuk 3. De precisie van de wettelijke basis, zal dan ook grotendeels afhangen van de betreffende amvb. Er is geen sprake van een big data carte blanche.
De wettelijke basis is wel voorzienbaar: het wetsvoorstel of de amvb maakt de gegevensverwerking voorzienbaar. Zie ook punt 4: het EVRM kent een materieel wetsbegrip. Vanuit dat perspectief is het niveau van regelgeving niet te laag.
De stelling van de NVvR wordt onderschreven, dat de uitkomst van een data-analyse pas na beoordeling door de verantwoordelijke autoriteiten (m.n. het OM) een verdenking oplevert. Hierop wordt ingegaan bij punt 11.

2. *Noodzaak onvoldoende onderbouwd* (AP, Platform bescherming burgerrechten, Privacy barometer, Privacy first, burgerreacties). In de reacties van individuele burgers worden als alternatieven genoemd het 1) het samenwerken via verwerkingsovereenkomsten en 2) het intensiever handhaven van de bestaande wet.

Het wetsvoorstel is nodig omdat gezamenlijke, domeinoverstijgende gegevensverwerking door samenwerkingsverbanden nu veelal goede grondslagen mist in sectorale wetgeving. Louter unilaterale verstrekking is weliswaar vaak al mogelijk, maar bij de WGS gaat het niet om unilaterale verstrekking maar om gezamenlijke gegevensverwerking, wat nu nog niet altijd kan. Uiteraard moeten hierbij de waarborgen van de AVG in acht worden genomen, maar de AVG staat als zodanig niet in de weg aan sectoroverstijgende vormen van informatie-uitwisseling. Een deugdelijke wettelijke grondslag is wel vereist. Het wetsvoorstel voorziet daarin.
Gezamenlijke, domeinoverstijgende gegevensverwerking door samenwerkingsverbanden is onder meer in het kader van de bestrijding van ondermijning een belangrijk instrument. Daar is het bij uitstek noodzakelijk dat meerdere partijen samenwerken en met het oog daarop (persoons)gegevens kunnen uitwisselen. Integrale informatie-uitwisseling is een goede mogelijkheid om ondermijning aan te pakken. Handhavingsorganisaties zijn het erover eens dat een integrale aanpak, waarbij een combinatie van instrumenten wordt ingezet, aanzienlijk effectiever is dan een

enkelvoudige benadering, waarbij alleen één domein (bijvoorbeeld het strafrecht) wordt ingezet. Informatiegestuurd opsporen is belangrijk. Koppelen van gegevens van opsporingsdiensten en van informatie in bijvoorbeeld iCOV kan van grote dienst zijn voor de bestrijding van ondermijnende criminaliteit. Informatiegestuurde opsporing kan eraan bijdragen om grote witwasconstructies op te sporen.
Verschillende overheidsinstanties op zowel lokaal als landelijk niveau en ook sommige private partijen hebben gevraagd om met spoed domeinoverstijgende informatiedeling mogelijk te maken in de aanpak van ondermijning. Zo stelde MKB in zijn publicatie "Speerpunten MKB-Nederland voor Justitie en Veiligheid"[27]: "Het beter uitwisselen van informatie kan criminaliteitsbestrijding én criminaliteit voorkomen veel effectiever maken. Verbeteringen zijn nodig in de informatie-uitwisseling publiek-publiek, publiek-privaat en privaat-privaat. Er moet nu eindelijk echt vaart gemaakt worden met de Wet gegevensverwerking door samenwerkingsverbanden."
Wat betreft de alternatieven: alternatief 1 geeft geen soelaas en alternatief 2 scheert langs de problemen heen. Het waar nodig intensiever handhaven van bestaande wetgeving en de extra mogelijkheden die dit wetsvoorstel biedt, zijn bovendien complementair aan elkaar.

3. *Taken en doelen van samenwerkingsverbanden zijn veel te ruim* (AP, NOvA, Amnesty, NJCM, Piratenpartij, Platform bescherming burgerrechten, Privacy barometer). De NOvA bepleit schrappen van de doelen "toezicht op de naleving van wettelijke voorschriften" en "handhaven van de openbare orde of veiligheid". De Nederlandse Vereniging van Banken wil enerzijds "toezicht op de naleving van wettelijke voorschriften" beperken tot "toezicht op de naleving van *gewichtige* wettelijke voorschriften" en wil anderzijds de reikwijdte uitbreiden met "bestrijding van witwassen en terrorismefinanciering en het bevorderen van de integriteit van het financiële stelsel". Bureau Regioburgemeesters wil de zorg, intragemeentelijke samenwerkingsverbanden en niet-zwaarwegende algemene belangen aan de reikwijdte toevoegen. Verbond van Verzekeraars wil private belangen toevoegen.

Aan deze bedenking is voldaan doordat het wetsvoorstel zo precies mogelijk de doelstellingen van de gegevensverwerking regelt voor de vier (clusters van) samenwerkingsverbanden die in het wetsvoorstel zijn opgenomen. Voor zover samenwerkingsverbanden bij amvb kunnen worden aangewezen, moet de doelstelling voldoen aan de beperkte reikwijdte van hoofdstuk 3. De taken en doelen zullen niet veel te ruim zijn doordat een amvb onder het wetsvoorstel niet alle doelen uit hoofdstuk 3 kan omvatten; wel kunnen hieruit één of enkele nader gespecificeerde subdoelen worden geselecteerd. Bij het opstellen van een amvb voor een samenwerkingsverband dient dus het doel van het desbetreffende samenwerkingsverband te worden geconcretiseerd binnen de kaders van hoofdstuk 3.
Het voorstel om de doelen "toezicht op de naleving van wettelijke voorschriften" en "handhaven van de openbare orde of veiligheid" te schrappen, is gevolgd door de doeleinden te clausuleren.
Het voorstel om "bestrijding van witwassen en terrorismefinanciering en het bevorderen van de integriteit van het financiële stelsel" toe te voegen is overgenomen in de doelstelling van het FEC.
Het voorstel om niet-zwaarwegende belangen toe te voegen, zou de drempel te laag maken gelet op de proportionaliteit.

4. *Amvb's zijn een te laag niveau van regelgeving* (College voor de Rechten van de Mens, FEC, NJCM, Platform bescherming burgerrechten, Privacy barometer). Zij bepleiten instelling van een samenwerkingsverband per formele wet: één wet per doel. Bureau Regioburgemeesters, VNG en het Verbond van Verzekeraars vinden amvb's juist een te hoog niveau van regelgeving: zij zien dit als onwerkbaar, inflexibel en traag. De Koninklijke Notariële Beroepsorganisatie vindt het acceptabel maar bepleit een voorhangprocedure.

[27] https://www.mkb.nl/sites/default/files/speerpunten_justitie_en_veiligheid.pdf

Aan deze bedenking is voldaan door vier (clusters van) samenwerkingsverbanden in het wetsvoorstel zelf te regelen in plaats van bij amvb. Weliswaar kunnen volgens het wetsvoorstel vanwege de flexibiliteit daarnaast samenwerkingsverbanden bij amvb worden aangewezen, maar dit is slechts mogelijk binnen de beperkte reikwijdte van hoofdstuk 3 en na toepassing van een bijzondere nahangprocedure bij het parlement.

5. *Onvoldoende waarborgen om de privacy te beschermen* (AP, College voor de Rechten van de Mens, Amnesty, Platform bescherming burgerrechten, Privacy First, burgerreacties), zoals analoge toepassing van de minimumvereisten voor heimelijke surveillance, toezicht zoals in de WIV, het vooraf uitsluiten van gegevenscategorieën, een onafhankelijke kwaliteitstoets van de gehanteerde analysemethodes, regels omtrent algoritmes, doelbinding, minimale gegevensverwerking, juistheid, controle en bewaartermijn, et cetera. NOvA bepleit om in de amvb naarmate er grotere hoeveelheden gegevens worden gedeeld, een grotere mate van bescherming te regelen. Het OM vindt dat ook de categorieën betrokkenen bij of krachtens amvb dienen te worden bepaald.

Voor een overzicht van en toelichting op de waarborgen verwijzen wij naar paragraaf 3.4 van deze memorie van toelichting. Naar aanleiding van de consultatie en het advies van de Afdeling advisering van de Raad van State zijn aanvullende waarborgen opgenomen in het wetsvoorstel. In artikel 8 van het wetsvoorstel zijn onder meer de volgende waarborgen toegevoegd, in aanvulling op de waarborgen die de AVG biedt, zoals de verplichting tot privacy by design op grond van de AVG:

- *een systeem van autorisaties, dat wil zeggen de verlening van toegang tot de systemen waarin de samenwerkingsverbanden gegevens verwerken aan uitsluitend door de deelnemers geautoriseerde medewerkers;*
- *een verplichting tot screening van medewerkers;*
- *het verplichting tot het loggen van gegevens die noodzakelijk zijn voor controle en toezicht;*
- *een verplichting tot het instellen van een rechtmatigheidsadviescommissie die de rechtmatigheid van de verwerking van persoonsgegevens door het samenwerkingsverband beoordeelt;*
- *een vernietigingstermijn;*
- *een adequaat beveiligingsniveau, ten minste overeenkomstig richtlijnen van de minister van BZK.*

Bij geautomatiseerde gegevensanalyse regelt artikel 8a tevens de volgende waarborgen:

- *de verplichting zorg te dragen voor adequate en uniforme technische en organisatorische maatregelen in verband met de bevordering van de kwaliteit van de gezamenlijke geautomatiseerde gegevensanalyse alsmede ter bevordering van de juistheid en de volledigheid van de gegevens die daarbij worden verwerkt;*
- *de plicht tot inhoudelijke tussenkomst van de rechtmatigheidsadviescommissie bij de verstrekking van een resultaat van geautomatiseerde gegevensanalyse, die zich vergewist van de zorgvuldige totstandkoming van het resultaat;*
- *de verplichting om op een voor het publiek toegankelijke wijze uitleg te geven over de gehanteerde patronen en indicatoren of andere onderliggende logica, tenzij volgens een deelnemer zwaarwegende redenen zich daartegen verzetten;*
- *de verplichting tot terugmelding van onjuistheden in bronbestanden.*

De WGS gaat niet over initiële gegevensverzameling, maar over verdere verwerking. Analoge toepassing van de minimumvereisten voor heimelijke surveillance en toezicht zoals in de Wet op de inlichtingen- en veiligheidsdiensten 2017 is daarom niet aan de orde.
Op het vooraf uitsluiten van gegevenscategorieën wordt hierna ingegaan bij punt 14.
Wat betreft de kwaliteitstoets van de gehanteerde analysemethodes en regels omtrent algoritmes, wijzen wij op de kwaliteitswaarborgen bij geautomatiseerde gegevensanalyse (artikel 8a), de rechtmatigheidsadviescommissie (artikel 8), de verplichte terugkoppeling van de resultaten en evaluatie daarvan (artikel 7) en de verplichting tot periodieke privacy audits (artikel 8b). De functionaris voor gegevensbescherming heeft ook een rol bij de onafhankelijke kwaliteitstoets.

Wat betreft het voorstel voor regels omtrent doelbinding, minimale gegevensverwerking, juistheid, controle en het niet langer opslaan van gegevens dan noodzakelijk, wordt opgemerkt dat artikel 5 AVG hiertoe reeds verplicht.
Wat betreft het voorstel voor een grotere mate van bescherming naarmate er grotere hoeveelheden gegevens worden gedeeld: artikel 32 AVG voorziet hierin, doordat het ook "omvang" als factor noemt.
Wat betreft het bij of krachtens amvb bepalen van categorieën betrokkenen: in de artikelen uit het wetsvoorstel die de te verstrekken categorieën gegevens opsommen is waar mogelijk ook omschreven welke categorieën betrokkenen het betreft.

6. *Onverenigbare verwerkingen mogelijk maken moet niet bij amvb* maar bij formele wet geschieden of moet überhaupt worden beperkt tot zeer beperkte uitzonderingsgevallen (NOvA, Amnesty, NJCM, Platform bescherming burgerrechten, Verbond van Verzekeraars).

Aan deze bedenking is voldaan door vier (clusters van) samenwerkingsverbanden in het wetsvoorstel zelf te regelen in plaats van bij amvb. Weliswaar kunnen volgens het wetsvoorstel vanwege de flexibiliteit daarnaast samenwerkingsverbanden bij amvb worden aangewezen, maar dit is slechts mogelijk binnen de beperkte reikwijdte van hoofdstuk 3 en na toepassing van een bijzondere nahangprocedure bij het parlement.

7. *De verplichting tot verstrekking van gegevens door de deelnemers aan het samenwerkingsverband moet worden vervangen door een mogelijkheid* tot gegevensverstrekking op grond van de taak van algemeen belang (aldus AP). Als het een verplichting tot gegevensverstrekking blijft, moet die worden beperkt (namelijk tot gegevens die van groot belang zijn, aldus Nederlandse Vereniging van Banken) of deze moet worden uitgebreid (door schrapping van de uitzonderingsclausule i.v.m. zwaarwegende redenen, aldus Bureau Regioburgemeesters).

Een nadeel van het schrappen van de leveringsplicht van deelnemers aan het samenwerkingsverband is het volgende: in de evaluatie van de Wet controle op rechtspersonen (Kamerstukken II 2013/14, 33857, nr. 1, bijlage) is gebleken dat het ontbreken van een leveringsverplichting voor informatieleveranciers (uitzonderingen zijn de Belastingdienst en het UWV) geregeld leidde tot de vraag vanuit de informatieleverancier of deze voor het toezicht op rechtspersonen wel verplicht is tot levering en hoe deze plicht zich verhoudt tot de op de informatieleverancier rustende geheimhoudingsplicht. Daarbij kwam het voor dat om die reden niet werd geleverd, wat de volledigheid en bruikbaarheid van de risicomeldingen negatief kon beïnvloeden (Evaluatie Wcr, blz. 20). Om een dergelijke situatie te voorkomen is in de WGS gekozen voor een verplichting tot verstrekking van gegevens voor de deelnemers.
De voor artikel 5 gedane tekstsuggestie "gegevens die van groot belang zijn" zou een onvoldoende objectieve maatstaf zijn en daarmee onwerkbaar.
De uitzonderingsclausule inzake zwaarwegende redenen is van belang voor maatwerk.

8. *Gebrek aan transparantie*: de informatieplicht is de uitzondering op de regel geworden, terwijl artikel 14, vijfde lid, onder c, AVG uitsluitend een uitzondering toestaat mits passende maatregelen worden getroffen om de gerechtvaardigde belangen van de betrokkene te beschermen. Die passende maatregelen ontbreken. Als iemand niet weet op welke lijstjes hij voorkomt, kan hij daartegen geen verweer voeren (NOvA, Amnesty, Piratenpartij, Platform bescherming burgerrechten, Privacy barometer, burgerreacties).

In paragraaf 3.4 van deze memorie van toelichting is ingegaan op de informatieplichten jegens betrokkenen op grond van de AVG, en op de uitzonderingsgronden. Zo geldt onder meer een uitzondering indien het verstrekken van de informatie de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen (artikel 14, vijfde lid, onderdeel b, AVG). In aanvulling op paragraaf 3.4 merken wij op dat voorkomen moet worden dat potentiële criminelen een kijkje in de keuken hebben kunnen nemen en hun kennis over de informatiepositie en werkwijze van de handhavingsorganisaties kunnen uitbreiden. Als (volledig) bekend wordt wat de

werkwijze is, is er het risico dat degenen op wie het toezicht is gericht hun gedrag daarop aanpassen, waardoor de bruikbaarheid van bijvoorbeeld een profiel en de effectiviteit van het toezicht worden verminderd.
Het wetsvoorstel bevat specifieke transparantieverplichtingen binnen de grenzen van het mogelijke: indien een samenwerkingsverband gezamenlijke geautomatiseerde gegevensverwerking verricht, verschaft het, tenzij naar het oordeel van een deelnemer zwaarwegende redenen zich daartegen verzetten, op een voor het publiek toegankelijke wijze uitleg over de gehanteerde patronen en indicatoren of andere onderliggende logica als bedoeld in artikel 14, tweede lid, onder g, van de Algemene verordening gegevensbescherming.
Het wetsvoorstel schrijft bovendien voor dat het samenwerkingsverband jaarlijks een jaarverslag opstelt waarin een verantwoording wordt gegeven van de effectiviteit en bruikbaarheid van de resultaten van de gegevensverwerking door het verband.

Er zijn ook mogelijkheden om verweer te voeren: de betrokkene kan een weigering om te voldoen aan een inzageverzoek in de zin van artikel 15 AVG voorleggen aan de rechter: indien een verwerkingsverantwoordelijke een bestuursorgaan is, dan worden beslissingen die genomen zijn inzake de rechten van betrokkene gelijkgesteld aan besluiten in de zin van de Awb op grond van artikel 34 van de Uitvoeringswet AVG, zodat bestuursrechtelijke rechtsbescherming openstaat. Indien een verwerkingsverantwoordelijke geen bestuursorgaan is, dan gelden dergelijke beslissingen niet als besluiten, waardoor civielrechtelijke rechtsbescherming openstaat (artikel 35 Uitvoeringswet AVG).

9. *Rechtsbescherming ontbreekt*, bijvoorbeeld tegen onterechte verdachtmaking van mensen als gevolg van fouten en vooroordelen in algoritmen (Amnesty, Platform bescherming burgerrechten, Privacy barometer, burgerreacties).

Tegen de achterliggende besluiten bestaat rechtsbescherming. Betrokkenen kunnen in beginsel hun recht van bezwaar uitoefenen op grond van artikel 21 AVG, wanneer de persoonsgegevens worden verwerkt op grond van artikel 6, eerste lid, onderdeel e (taak van algemeen belang of f (gerechtvaardigde belangen).
Wat betreft de risico's van fouten en vooroordelen in algoritmen geldt dat deze geadresseerd zullen moeten worden, wil de gegevensverwerking in het samenwerkingsverband juridisch aanvaardbaar zijn. De deelnemers zullen zorgvuldig te werk moeten gaan, onder meer door te zorgen dat de gegevens van voldoende kwaliteit zijn en dat zij beschikken over de nodige expertise om goede analyses uit te voeren en de uitkomsten op een passende en controleerbare wijze te duiden.
Voor zover het gebruik van big data uitmondt in een besluit als bedoeld in de Awb, kan de betrokkene de big-data-analyse in ieder geval in dat verband aan de orde stellen. Dat kan in beginsel al in de fase van voorbereiding van het besluit. Een belanghebbende moet immers in de gelegenheid worden gesteld om een zienswijze te geven, indien de beschikking mede zou steunen op gegevens over feiten en belangen die de belanghebbende betreffen en die gegevens niet door hemzelf zijn verstrekt (art. 4:7 en 4:8 Awb).
Van belang is dat reeds bij het ontwerpen van informatiesystemen en de daarin toe te passen analyses erin wordt voorzien dat betekenis toekomt aan rechtsbeginselen als het gelijkheidsbeginsel, het willekeursverbod, het formele en materiële gelijkheidsbeginsel. Zo is er rechtsbescherming vooraf.
In geen geval zal er sprake zijn van geautomatiseerde besluitvorming door het samenwerkingsverband als bedoeld in artikel 22 AVG.

10. *Gebrek aan databeveiliging* (Piratenpartij en veel burgerreacties): geen controle of data worden gebruikt voor andere doelen; risico op datamisbruik; het samenbrengen van informatie maakt de risico's van hacken veel groter; de overheid heeft geen goed track record op het gebied van databeveiliging en niet voldoende deskundigheid op ICT-vlak; medewerkers van samenwerkingsverbanden die betrokken zijn bij ondermijnende activiteiten kunnen de gegevensuitwisseling saboteren of data lekken.

Uiteraard moet een aantal infrastructurele maatregelen worden getroffen en voorzieningen beschikbaar zijn om kwetsbaarheden zoals datalekken, misbruik en oneigenlijk gebruik te voorkomen. Artikel 32 AVG verplicht tot databeveiliging. Artikel 8 van het wetsvoorstel bepaalt bovendien dat binnen het samenwerkingsverband persoonsgegevens uitsluitend worden verwerkt in systemen waarvoor een adequaat beveiligingsniveau geldt. Daarbij dienen persoonsgegevens te worden beveiligd, ten minste volgens de minister van Binnenlandse Zaken en Koninkrijksrelaties vastgestelde richtlijnen.

Voor de controle of data worden gebruikt voor andere doelen zijn de volgende specifieke waarborgen toegevoegd, mede om het risico op datamisbruik te minimaliseren:

- *De verplichting tot periodieke privacy audits;*
- *De verplichting tot logging: de deelnemers dragen zorg voor de vastlegging langs elektronische weg van bij algemene maatregel van bestuur te beschrijven verwerkingen van persoonsgegevens in geautomatiseerde systemen. De vastgelegde gegevens worden uitsluitend gebruikt voor de controle van de rechtmatigheid van de gegevensverwerking, voor interne controles, ter waarborging van de integriteit en de beveiliging van de persoonsgegevens en voor strafrechtelijke procedures;*
- *De verplichting tot instelling van een rechtmatigheidsadviescommissie, die tot taak heeft de rechtmatigheid van de verwerking van persoonsgegevens in het samenwerkingsverband structureel te beoordelen bij nieuwe verwerkingen en wijziging in verwerkingen en om voorstellen aan het samenwerkingsverband te doen om onrechtmatigheden op te lossen.*

Wat betreft deskundigheid – al dan niet op ICT-vlak – bevat het wetsvoorstel de volgende bepalingen:
- de verplichting voor deelnemers om voldoende en gekwalificeerd personeel aan te wijzen ten behoeve van de inzet in het samenwerkingsverband;
- de mogelijkheid om bij amvb opleidingseisen te stellen aan personen die zijn aangewezen ten behoeve van de inzet in het samenwerkingsverband.

11. *Schending onschuldpresumptie* door datamining en profileren (Amnesty, Platform bescherming burgerrechten, Privacy First); bovendien staat in artikel 2 sub d dat de data kunnen worden gebruikt voor het 'vervolgen van strafbare feiten of de tenuitvoerlegging van straffen', dus is onduidelijk waarom de gegevensuitwisseling binnen de samenwerkingsverbanden niet zou kunnen leiden tot een formele verdenking.

Zoals reeds toegelicht in paragraaf 3.3.4 van de memorie van toelichting wordt er nadrukkelijk op gewezen dat de uitkomst van een analyse binnen een samenwerkingsverband waaraan opsporingsdiensten of OM deelnemen, onder de voorgestelde WGS nog geen verdenking oplevert. Zij kunnen de uitkomst van een analyse meewegen bij de beslissing over het al dan niet starten van het strafrechtelijk onderzoek. Van een verandering van de voorschriften in het Wetboek van Strafvordering met betrekking tot het vorderen van gegevens is geen sprake. Wel geeft het wetsvoorstel een betere basis voor het verstrekken van informatieproducten aan OM en opsporingsdiensten uit een samenwerkingsverband waaraan zij deelnemen, in een fase waarin (nog) geen verdenking bestaat. Die blijkt nodig te zijn, omdat soms onvoldoende helder leek te zijn of en, zo ja, in welke omstandigheden opsporingsdiensten en OM op rechtmatige wijze dergelijke informatieproducten kunnen krijgen.
De zinsnede in artikel 2, onder d, die betrekking heeft op "vervolging van strafbare feiten of de tenuitvoerlegging van straffen" is overigens niet (als zodanig) meer aanwezig in het wetsvoorstel omdat de doeleinden voor vier (clusters van) samenwerkingsverbanden specifiek zijn geregeld en omdat slechts binnen een beperkte reikwijdte samenwerkingsverbanden kunnen worden aangewezen bij amvb.

12. *Ongewenste neveneffecten* (NOvA, Platform bescherming burgerrechten, Verbond van Verzekeraars, diverse burgerreacties). Genoemd worden: onjuiste persoonsgegevens kunnen een eigen leven gaan leiden terwijl onduidelijk is wie ze intussen allemaal heeft;

deelnemers kunnen de deskundigheid missen om informatie op waarde te schatten; risico van bias via machine learning, algoritmes en AI; ambtenaren hebben onvoldoende kennis om 'false positives' eruit te halen omdat zij door het gebruik van statistische verbanden moeilijk kunnen herleiden waarom de burger geselecteerd is; verstrekking aan private partijen kan leiden tot bijvoorbeeld het onthouden van een hypotheek of zorg; de verplichting tot gescheiden gegevenshuishoudingen uit artikel 8, tweede lid, kan leiden tot een forse administratieve lastenverzwaring voor private partijen.

Wat betreft de stelling "Onjuiste persoonsgegevens kunnen een eigen leven gaan leiden terwijl onduidelijk is wie ze intussen allemaal heeft" geldt dat uit artikel 5, eerste lid, onder d, AVG volgt dat verwerkingsverantwoordelijken de juistheid en actualiteit van de gegevens in het oog dienen te houden. De verwerkingsverantwoordelijke moet er ook voor zorgen dat de gegevens gedurende de bewaartermijn actueel blijven om het risico op onjuistheden te verminderen. Ook bevat het wetsvoorstel de volgende specifieke waarborgen:

- *de verplichting tot terugmelding van onjuistheden in bronbestanden;*
- *de verplichting zorg te dragen voor adequate en uniforme technische en organisatorische maatregelen voor de bevordering van de kwaliteit van de gezamenlijke geautomatiseerde gegevensanalyse en de juistheid en de volledigheid van de gegevens die daarbij worden verwerkt.*

Daarnaast volgt uit artikel 3:2 Awb dat gegevens eerst worden geverifieerd voordat ze ten grondslag worden gelegd aan een voorgenomen besluit. Het risico op fouten kan verder worden beperkt door bij het constateren van onjuistheden in de gegevens deze terug te melden bij de bron.
Uit artikel 19 AVG volgt bovendien dat een verwerkingsverantwoordelijke de eventuele ontvangers van persoonsgegevens in kennis moet stellen van een rectificatie die heeft plaatsgevonden op verzoek van betrokkene.
Artikel 5, eerste lid, onder a, AVG verplicht tot een behoorlijke gegevensverwerking. Dat gaat ook over de kwaliteit van het proces en kwaliteit van algoritmen.
Wat betreft het onthouden van een hypotheek wordt opgemerkt dat als het doel van het samenwerkingsverband fraudebestrijding is, het juist beoogd is dat verstrekking aan een (private) deelnemer mogelijk is voor het doel van dat samenwerkingsverband. In dat geval is het onthouden van een hypotheek aan bijv. een hypotheekfraudeur een goede uitkomst.
Tot slot dient de voorafgaande toetsende rol van de AP als aanvullende waarborg om ongewenste neveneffecten te voorkomen (zie paragraaf 3.5).
De verplichting tot gescheiden gegevenshuishoudingen is als zodanig geschrapt gelet op genoemd bezwaar. Indien een deelnemer tevens niet publieke doelen nastreeft, dient deze gegevensverwerking weliswaar zoveel mogelijk gescheiden te zijn van de gegevensverwerking van publieke doelen, maar daartoe is nu de bepaling opgenomen dat een private deelnemer ten behoeve van de inzet in het samenwerkingsverband slechts personen aanwijst die niet tevens worden belast met commerciële werkzaamheden voor die private partij.

13. *Harmonisatie van samenwerkingsverbanden is niet haalbaar* (Bureau Regioburgemeesters, Politie). Er moet afstemming plaatsvinden met het wetsvoorstel Verwijzingsportaal Bankgegevens (Nederlandse Vereniging van Banken). Een individuele burger merkt op dat een exclusief regime voor gegevensverwerking juist het doel van de WGS moet zijn, omdat daardoor inzichtelijk wordt wat voor samenwerkingsverbanden er zijn en wíe er allemaal gegevens verwerkt en met welk doel.

Harmonisatie is wel wenselijk en is ook mogelijk ten aanzien van de generieke bepalingen. Een exclusief regime is niet haalbaar gelet op de verscheidenheid aan samenwerkingsverbanden. Een aantal samenwerkingsverbanden kan volstaan met de bestaande grondslagen voor verwerking van persoonsgegevens, zoals de mogelijkheid om ten behoeve van wetenschappelijk onderzoek en statistiek persoonsgegevens te verwerken. Deze mogelijkheid houdt in dat verwerking van gegevens voor wetenschappelijke en statistische doeleinden als niet onverenigbaar wordt beschouwd met het oorspronkelijke doel waarvoor de desbetreffende gegevens zijn verzameld.[28]

14. *Van bijzondere categorieën van persoonsgegevens en strafrechtelijke persoonsgegevens* moet verduidelijkt worden of het wetsvoorstel daarop betrekking heeft (NOvA, Bureau Regioburgemeesters, Amnesty, Nederlandse Vereniging van Banken, Platform bescherming burgerrechten).

Het wetsvoorstel heeft in beginsel op bijzondere categorieën van persoonsgegevens geen betrekking, omdat verwerking van dergelijke gegevens verboden is tenzij daarop een uitdrukkelijke uitzondering is gemaakt. Uit de AVG en UAVG vloeit reeds voort dat de verwerking van bijzondere categorieën van persoonsgegevens en strafrechtelijke persoonsgegevens in beginsel verboden is, tenzij in de wet een uitzondering op het verwerkingsverbod is geregeld. Een dergelijke uitzondering is voor persoonsgegevens van strafrechtelijke aard gemaakt, namelijk in de artikelen uit de WGS die verstrekking op grond van de Wjsg en Wpg aan samenwerkingsverbanden mogelijk maken, evenals in artikel 5. Voor wat betreft bijzondere categorieën van persoonsgegevens bevat hoofdstuk 2 enkele uitzonderingen.

15. *De doorbreking van geheimhoudingsplichten* is wellicht niet effectief geregeld en behoeft nader onderzoek (NOvA, Bureau Regioburgemeesters). Bovendien moet worden geëxpliciteerd dat bepaalde geheimhoudingsplichten niet worden doorbroken (Koninklijke Notariële Beroepsorganisatie, Nederlandse Vereniging van Banken, Reclassering Nederland, FIU-Nederland).

Hierop is ingegaan in onder meer de artikelsgewijze toelichting bij artikel 5.

16. *De onderlinge verantwoordelijkheidsverdeling* behoeft aanscherping: de mogelijkheid om regels te stellen over verantwoordelijkheid en een contactpunt, moet worden vervangen door een verplichting (NOvA, Nederlandse Vereniging van Banken)).

Dit punt is overgenomen: artikel 4, vierde lid, onderdelen a en b, zijn dwingend worden geformuleerd naar aanleiding van deze opmerkingen.

17. *Gedwongen aanwijzing als deelnemer* moet worden uitgesloten door te regelen dat deelname aan een samenwerkingsverband uitsluitend geschiedt op vrijwillige basis (NOvA, Nederlandse Vereniging van Banken)

Met de Afdeling advisering van de Raad van State[29] zijn wij van mening dat de wetgever bij de aanwijzing van deelnemers zijn verantwoordelijkheid moet nemen gelet op de zwaarwegende publieke belangen. Als instemming van de (kandidaat-)deelnemers nodig is, om ze te kunnen aanwijzen als deelnemer, is het onzeker of partijen besluiten om toe te treden tot samenwerkingsverbanden, vanwege allerlei overwegingen van bestuurlijke of praktische aard. Daarom dient de wetgever om deelnemers van samenwerkingsverbanden te kunnen aanwijzen, niet afhankelijk te zijn van hun instemming of verzoek tot deelname.

18. *De mogelijkheid van deelname van private partijen* is een punt van aandacht of kritiek (NVvR, Piratenpartij) of gaat juist niet ver genoeg (Verbond van Verzekeraars).

Het wetsvoorstel is op dit punt in balans.

19. *Intragemeentelijke gegevensverwerking* ontbreekt in WGS (VNG, Bureau Regioburgemeesters)

Het wetsvoorstel is inderdaad niet bedoeld voor intragemeentelijke gegevensverwerking. Een conglomeraat of hybride constructie van lokale en nationale deelnemers is wel denkbaar.

---

[28] Verwezen zij naar artikel 5, eerste lid, onder b, AVG.
[29] Zie paragraaf 2, onder c, van het advies van de Afdeling advisering van de Raad van State.

20. *Overige punten*: amvb moet beëindiging van samenwerkingsverbanden regelen (OM), samenwerkingsverband zou met een ander samenwerkingsverband een nieuw samenwerkingsverband moeten kunnen aangaan (Bureau Regioburgemeesters), regel een hit/no hit systeem voor banken om juistheid gegevens te checken (Nederlandse Vereniging van Banken), voer PIA op WGS uit (Piratenpartij), de criteria voor wanneer wel/niet onderling afschermen ontbreken in artikel 8, vijfde lid (burgerreactie), uiteenlopende opmerkingen (Justid, niet-openbare reactie)

Voor de beëindiging van een samenwerkingsverband is per definitie een (intrekkings)wet, amvb of regeling nodig en dat biedt de gelegenheid om ook de afwikkeling dan te regelen.
Het is niet de bedoeling dat een samenwerkingsverband kan deelnemen aan een ander samenwerkingsverband. Dat zou te ver gaan. Wel biedt artikel 7, tweede lid, de mogelijkheid om de resultaten van de verwerking aan een derde, waaronder ook een samenwerkingsverband kan vallen.

Consultatie Samenwerkingsverband Zorg- en Veiligheidshuizen

De stakeholders van de Zorg- en Veiligheidshuizen zijn in de gelegenheid gesteld te reageren op het onderdeel van het wetsvoorstel dat betrekking heeft op de Zorg- en Veiligheidshuizen. Uitnodigingen daartoe zijn verstuurd via de werkgroep Gegevensdeling en Privacy Zorg en Veiligheid en rechtstreeks.

Reacties zijn binnengekomen van: De Landelijke Vereniging van Managers Zorg- en Veiligheidshuizen, Reclassering Nederland, openbaar ministerie, Vereniging Gehandicaptenzorg Nederland, Geestelijke Gezondheidszorg Nederland, Jeugdzorg Nederland, Raad voor de Kinderbescherming en Vereniging Nederlandse Gemeenten en Bureau Regioburgemeesters (gezamenlijke reactie).

De reacties zijn in drie categorieën te onderscheiden:
- Reacties op het proces
- Reacties de inhoud van het wetsvoorstel
- Suggesties en aanvullingen voor verduidelijking bij de artikelen

Deze laatste zijn voor zover van toepassing verwerkt, en vallen in deze paragraaf buiten beschouwing.

Reacties op het proces: tijdsdruk
Alle reacties zijn kritisch over het tempo waarin het onderdeel voor de Zorg- en veiligheidshuizen in dit wetsvoorstel tot stand moet komen. Verschillende organisaties uiten dan ook zorgen dat dit ten koste kan gaan van de zorgvuldigheid.

Deze tijdsdruk is een gegeven. Er is geprobeerd dit hanteerbaar te maken door een aantal partijen intensief bij de totstandkoming van het wetsvoorstel te betrekken. Zo heeft er meerdere malen overleg plaatsgevonden met vertegenwoordigers van de Landelijke Vereniging van Managers van Zorg- en Veiligheidshuizen en zijn onderdelen tussentijds aan hen voorgelegd, om op die manier de uitvoerbaarheid van het wetsvoorstel in de praktijk te kunnen toetsen. Ook andere partijen zijn in de gelegenheid gesteld om tussentijds feedback te geven op onderdelen. Verschillende partijen zijn positief over de inspanningen die er ondanks de tijdsdruk zijn gedaan om hen bij het wetsvoorstel te betrekken.

Reacties op de inhoud van het wetsvoorstel
Alle reacties zijn positief over het feit dat er een wettelijke regeling komt voor de gegevensverwerking in de Zorg- en veiligheidshuizen. Gegevensdeling en privacy is al vele jaren een heet hangijzer binnen de Zorg- en Veiligheidshuizen. Een wettelijke regeling biedt helderheid aan partijen wie er mogen samen werken in het Zorg- en Veiligheidshuizen, en welke gegevens daarbij mogen worden gedeeld. 'De WGS regelt een solide basis onder de gegevensdeling in de Zorg- en Veiligheidshuizen' constateert de Landelijke Vereniging van Managers van Zorg- en veiligheidshuizen.

- Wetsvoorstel als geheel sterk gericht op veiligheid en fraudebestrijding

In verschillende reacties, met name die van de zorgpartijen, wordt opgemerkt dat het wetsvoorstel als geheel erg gericht is op veiligheid en fraudebestrijding. Terwijl in de Zorg- en Veiligheidshuizen juist ook de zorg- en hulpverlening een belangrijk element van de aanpak zijn. Daarin zit ook een belangrijk verschil met de andere drie samenwerkingsverbanden die in het wetsvoorstel worden geregeld. Meerdere partijen pleiten ervoor om het belang van de zorg- en hulpverleningsketen explicieter tot uiting te laten komen in het wetsvoorstel, en ook duidelijk te maken dat het bijvoorbeeld niet de bedoeling is dat gegevens die zorgpartijen in het verband van Zorg- en Veiligheidshuizen delen, gebruikt worden voor opsporing en fraudebestrijding.

Er is inderdaad een wezenlijk verschil tussen de Zorg- en Veiligheidshuizen en de andere drie samenwerkingsverbanden die dit wetsvoorstel beoogt te regelen. Waar iCOV, RIEC en FEC vooral gericht zijn op fraudebestrijding en opsporing, zijn de Zorg- en Veiligheidshuizen gericht op de behandeling van complexe casuïstiek. Dat zijn situaties waarbij problemen op het gebied van criminaliteit, overlastgevend gedrag en veiligheidsrisico's voor een belangrijk deel hun oorzaak vinden in (een combinatie van) zorg- en sociale problematiek. De Zorg- en Veiligheidshuizen richten zich dan op de afstemming die nodig is tussen interventies uit het strafrecht, bestuurlijke maatregelen, begeleiding, zorg en hulpverlening om tot een duurzame verbetering van de situatie te komen. Het doel is daarmee niet opsporing en vervolging, maar een aanpak waarbij het eindelijk beter gaat met de persoon, vanuit de gedachte dat dan ook de problematiek op het gebied van criminaliteit, overlast en of veiligheid zullen afnemen. In de doelstelling voor de Zorg- en Veiligheidshuizen in artikel 47 en de toelichting hierop is dit nu sterker verwoord.

- Aansluiten bij hetgeen de laatste jaren is ontwikkeld m.b.t. een zorgvuldige praktijk

De meeste reacties wijzen erop dat er de afgelopen jaren al veel werk is verricht door de Zorg- en Veiligheidshuizen om tot een zorgvuldige praktijk van gegevensverwerking te komen. Een wettelijke regeling zou dan ook niet zozeer hele nieuwe gegevensverwerkingen mogelijk moeten maken, als wel een degelijke juridische basis moeten leggen onder deze zorgvuldige praktijk.

In een aantal reacties klinkt in dat verband de waarschuwing door dat een wettelijke regeling niet de indruk moet wekken dat partijen nu structureel gegevens mogen delen, of dat partijen gedwongen worden om gegevens te moeten delen, ook als dat naar het oordeel van de betreffende organisatie niet noodzakelijk is gezien de inhoud van de casus. Casusbehandeling in het Zorg- en Veiligheidshuis dient maatwerk te blijven.

Bij de totstandkoming van het onderdeel voor de Zorg- en veiligheidshuizen in dit wetsvoorstel is geprobeerd om zo goed mogelijk aan te sluiten bij de zorgvuldige praktijk die in de afgelopen jaren door een werkgroep van privacy-experts van de Zorg- en veiligheidshuizen is ontwikkeld. Mede naar aanleiding van deze reacties zijn in verschillende artikelen bepalingen geëxpliciteerd die moeten leiden tot een stapsgewijze benadering in de gegevensverwerking met het oog op het maatwerk, waarop in de reacties wordt geduid. Onder andere in artikel 49, artikel 52 en artikel 53. Ook is in artikel 50 een bepaling opgenomen die elke deelnemer de mogelijkheid geeft om voorwaarden en beperkingen te stellen aan de verdere verwerking van gegevens die hij inbrengt in het Zorg- en Veiligheidshuis. Op die manier kunnen deelnemers hun eigen verantwoordelijkheid ten aanzien van gegevensverwerking waarmaken. Dit wetsvoorstel laat onverlet dat de deelnemers aan het samenwerkingsverband invulling zullen moeten geven aan de beginselen van noodzaak, subsidiariteit en proportionaliteit. In de memorie van toelichting is daartoe, naar aanleiding van de consultatie, op verschillende punten geëxpliciteerd dat de deelnemers afspraken zullen moeten maken hoe zij dit zullen doen. De werkwijze die in de afgelopen jaren is ontwikkeld biedt daarin een belangrijk houvast.

- Mogelijke competentieconflicten

In sommige reacties komt de vraag naar voren in hoeverre de deelnemers in het samenwerkingsverband in de afwegingen van afzonderlijke deelnemers kunnen treden, bijvoorbeeld omtrent de noodzaak om gegevens in te brengen, of omtrent de beslissing om bepaalde sancties, voorzieningen of maatregelen te treffen.

Dit punt is in de memorie van toelichting verder verduidelijkt. Dit wetsvoorstel verandert niets aan de bestaande taken, bevoegdheden en verantwoordelijkheden van de individuele deelnemers. Ook creëert het wetsvoorstel geen mogelijkheden voor het samenwerkingsverband om in de bevoegdheden van deelnemers te treden. Elke deelnemer behoudt zijn eigen bevoegdheid en verantwoordelijkheid omtrent de inzet van sancties, bestuurlijke maatregelen, toe te kennen voorzieningen of in te zetten hulp, en behandeling. Dit geldt ook voor bijvoorbeeld de afweging of bepaalde gegevens wel of niet noodzakelijk zijn om te delen in een specifiek geval. De noodzakelijkheidsafweging gaat daarmee vooraf aan de verplichting om te verstrekken uit artikel 5.

- Flexibiliteit in deelnemers

Verschillende reacties, onder andere van de Landelijke Vereniging van Managers van Zorg- en Veiligheidshuizen, de VNG en het Bureau Regioburgemeesters, wijzen erop dat het aanwijzen van deelnemers aan het samenwerkingsverband bij wet ertoe leidt dat er geen regionaal maatwerk meer mogelijk is. Zij zouden de lijst van artikel 48 graag zien als een minimumlijst, met de mogelijkheid om bij convenant ook andere deelnemers toe te laten.

Deze wens wordt in dit wetsvoorstel niet gehonoreerd. Door een selecte groep deelnemers bij wet aan te wijzen wordt duidelijkheid gecreëerd over de bestuursorganen en organisaties die in de ogen van de regering verantwoordelijkheid moeten dragen voor de zorgvuldige en rechtmatige gegevensverwerking in een Zorg- en Veiligheidshuis. Dit zijn sleutelpartners die allen mede verantwoordelijk zijn voor de wijze waarop in het Zorg- en Veiligheidshuis wordt gewerkt. Het is echter duidelijk dat gezien de grote diversiteit aan problematieken die aan de orde kunnen zijn in de Zorg- en Veiligheidshuizen het onmogelijk is om op voorhand alle mogelijke deelnemers in een specifiek geval te kennen. Daarom is in artikel 52, negende lid, de mogelijkheid geopend om, indien dit naar het oordeel van de deelnemers die bij een casus zijn betrokken noodzakelijk is, op incidentele basis een derde te betrekken bij de behandeling van de casus. Hiermee wordt in de ogen van de regering voldoende ruimte geboden om in voorkomende gevallen tot maatwerk te komen. De verantwoordelijkheid voor de zorgvuldigheid waarop de beslissing om een derde te betrekken tot stand komt, is echter de verantwoordelijkheid van de deelnemers die zijn aangewezen bij deze wet. Het staat de deelnemers van Zorg- en Veiligheidshuizen overigens vrij om bij convenant op bestuurlijk niveau afspraken te maken met derden in de regio, over hun organisatorische inzet in situaties waarin hun betrokkenheid gewenst is, en hen te binden aan de werkwijze die de deelnemers hebben afgesproken met het oog op een zorgvuldige gegevensverwerking.

- Beroepsgeheim

Uit de reacties van onder andere GGZ Nederland en Vereniging Gehandicaptenzorg Nederland (VGN) blijkt dat zij tevreden zijn over de wijze waarop in het wetsvoorstel het medisch beroepsgeheim wordt gerespecteerd. Tegelijkertijd constateert VGN ook, dat hierdoor een belangrijk dilemma voor zorg- en hulpverleners met een wettelijk beroepsgeheim blijft bestaan. Immers onder de doelgroep die in de Zorg- en Veiligheidshuizen aan de orde is bevinden zich relatief vaak zorgmijders, of mensen met wie in eerste instantie geen contact kan worden gelegd. Het is dan niet mogelijk om toestemming te krijgen om het beroepsgeheim te doorbreken, terwijl het delen van informatie wel een belangrijke bijdrage zou kunnen leveren aan de aanpak. Het wetsvoorstel biedt vooralsnog geen mogelijkheden om dan desnoods informatie te delen zonder toestemming, behoudens in noodsituaties of als er acuut gevaar is voor de veiligheid van de persoon of anderen.

Het klopt dat dit wetsvoorstel in beginsel de geheimhouding op grond van de Wgbo[30], de Wet BIG en de Jeugdwet respecteert. Het wetsvoorstel geeft wel aan dat het goed hulpverlenerschap een grond kan zijn om het beroepsgeheim zonder toestemming van betrokkene te doorbreken. Daarmee wordt aangesloten bij dit begrip uit de Wgbo en de Jeugdwet. Deze beroepsgeheimen dienen een belangrijk maatschappelijk doel. Namelijk het waarborgen van de vrije toegang tot (medische) zorg en (jeugd)hulp. Het is naar de mening van de regering aan de beroepsgroepen zelf om nadere invulling te geven in

[30] Wet op de geneeskundige behandelingsovereenkomst. Dit is een wijzigingswet die aan boek 7, titel 7, van het Burgerlijk Wetboek afdeling 5 heeft toegevoegd.

welke situaties goed hulpverlenerschap van de zorg- of hulpverlener vraagt om de geheimhouding te doorbreken zonder toestemming. Indien beroepsgroepen hier een knelpunt signaleren voor hun beroepsgroep, is het in de eerste plaats aan hen om hier meer duidelijkheid en eventueel meer ruimte in te bieden.

- Rechtmatigheidscommissie, flexibiliteit en verstrekken van resultaten van het Zorg- en Veiligheidshuis aan derden

In artikel 7 en 8 van dit wetsvoorstel wordt een rol toegekend aan een rechtmatigheidsadviescommissie. Elk samenwerkingsverband dient een rechtmatigheidsadviescommissie in te stellen. Deze toetst de rechtmatigheid van nieuwe verwerkingen, en toetst of de verstrekking van resultaten aan derden is toegestaan. In verschillende reacties wordt er op gewezen dat deze rechtmatigheidscommissie in de praktijk van de Zorg- en Veiligheidshuizen niet werkbaar is. In ieder geval niet als deze tot op casusniveau uitspraken zou moeten doen over de rechtmatigheid van gegevensverwerkingen en het verstrekken van resultaten aan derden. In de Zorg- en Veiligheidshuizen is immers sprake van maatwerk. De aard van de problematiek van de betrokkene is mede bepalend voor de gegevensverwerkingen in een specifiek geval. Dit bepaalt ook of het noodzakelijk is om incidenteel een derde te betrekken bij een casus. Indien de rechtmatigheidsadviescommissie hier eerst een uitspraak over zou moeten doen leidt dat tot een onwerkbare bureaucratie en vertraging in het werk.

Omgekeerd werd in een enkele reactie kritiek geuit op de mogelijkheid om resultaten uit het Zorg- en Veiligheidshuis te kunnen verstrekken aan derden. Deze bepaling zou een te groot risico betekenen voor ongewenste verspreiding van persoonsgegevens.

De kritiek op de rechtmatigheidscommissie met betrekking tot de Zorg- en veiligheidshuizen heeft geleid tot aanpassing van het wetsvoorstel en een nadere uitleg in de memorie van toelichting over de rol en positie van deze commissie in de samenwerkingsverbanden. Het is mogelijk maakt om een rechtmatigheidscommissie voor alle Zorg- en Veiligheidshuizen aan te wijzen en bij amvb nadere regels te stellen aan de werkwijze. Het ligt in de rede dat bij verstrekkingen op casusniveau conform een in deze wet vastgelegde verwerkingswijze er geen tussenkomst van de rechtmatigheidadviescommissie nodig zal zijn. Een rechtmatigheidsadviescommissie is nodig om uitspraken te doen over nieuwe verwerkingswijzen en ook kunnen aan de rechtmatigheidscommissie kwesties voorgelegd worden, waarbij er twijfel bestaat over de rechtmatigheid van een verwerking.
Artikel 52, negende lid, biedt de mogelijkheid om, indien dit naar het oordeel van de deelnemers die bij een casus betrokken zijn noodzakelijk is, een derde te betrekken bij de casus. Dit kan bijvoorbeeld het geval zijn als een specifieke expertise nodig is gelet op de aard van de problematiek. Artikel 52, negende lid, biedt dan de mogelijkheid om tot het maatwerk te komen dat nodig is. Een derde die op basis van artikel 52, negende lid, bij een casus wordt betrokken, dient op dat moment beschouwd te worden als een deelnemer voor de duur van de casus. Hij is gehouden aan dezelfde bepalingen voor de gegevensverwerking op grond van deze wet als de deelnemers aan de Zorg- en Veiligheidshuizen. Een dergelijke derde valt daarmee niet onder de toets van de rechtmatigheidsadviescommissie zoals bedoeld in artikel 7, tweede lid. Deelnemers kunnen afspraken maken hoe zij met dergelijke situaties omgaan en een oordeel vragen aan de rechtmatigheidsadviescommissie over die afspraken. Ook kan door de deelnemers, indien er twijfel bestaat over de rechtmatigheid van een dergelijke verstrekking, een oordeel vooraf gevraagd worden aan de rechtmatigheidsadviescommissie. Bij dergelijke verstrekkingen zullen altijd de voorwaarden in acht genomen moeten worden van artikel 7, tweede lid onderdeel a en b, artikel 7, derde lid, en artikel 50, derde lid. Ook regelt artikel 7, tweede lid dat een dergelijke verstrekking geen doorgang vindt indien een deelnemer bezwaar heeft tegen de verstrekking. De regering is van mening dat hiermee voldoende waarborgen zijn tegen ongewenste en onnodige verspreiding van de resultaten.

- Bewaren en vernietigen van gegevens

Verschillende reacties wijzen erop dat het wetsvoorstel de termijn waarop vernietiging, anonimisering, dan wel verwijdering moet plaatsvinden, rekent vanaf de datum van de eerste verwerking. In de situatie van de Zorg- en Veiligheidshuizen is er regelmatig

sprake van langlopende casuïstiek. Het zou dan meer voor de hand liggen om te rekenen vanaf de datum waarop de casus is afgesloten.

Omwille van de eenduidigheid is er in dit wetsvoorstel voor gekozen om te rekenen vanaf de datum waarop de eerste verwerking heeft plaatsgevonden. De bepaling die hierop betrekking heeft in artikel 8, zevende lid, biedt echter ruimte om, indien feiten of omstandigheden het noodzakelijk maken om gelet op het doel van de Zorg- en Veiligheidshuizen een casus te heropenen, de termijn te verlengen. Dit vergt echter een duidelijke afweging van de deelnemers die bij de casus zijn betrokken. In de memorie van toelichting voor de Zorg en Veiligheidshuizen is dit mede naar aanleiding van deze reacties, nader toegelicht bij artikel 52, achtste lid.

- Gegevensuitwisseling tussen samenwerkingsverbanden

In sommige reacties wordt teleurstelling geuit over het feit dat dit wetsvoorstel geen regeling bevat voor de uitwisseling van gegevens tussen de verschillende samenwerkingsverbanden die deze wet regelt, o.a. tussen de Zorg- en Veiligheidshuizen en de RIECs.

Dit wetvoorstel bevat inderdaad niet een dergelijke regeling. Dit wetsvoorstel regelt de gegevensverwerking voor vier soorten samenwerkingsverbanden. Elke soort heeft daarbij een gelijke taak. Maar het doel, de werkwijze, en de aard van de gegevens die aan de orde kunnen zijn in de verschillende soorten samenwerkingsverbanden is daarbij soms fundamenteel verschillend. Dit speelt met name bij de Zorg- en Veiligheidshuizen ten opzichte van de andere drie samenwerkingsverbanden die dit wetsvoorstel regelt. Om die reden bevat dit wetsvoorstel geen specifieke bepalingen die het mogelijk maken om gegevens uit te wisselen tussen de Zorg- en Veiligheidshuizen en de andere soorten samenwerkingsverbanden. De doelen en werkwijzen van de samenwerkingsverbanden liggen daarvoor te ver uit elkaar om hiervoor een generieke regeling te treffen. Dit laat onverlet, dat in hele specifieke gevallen het noodzakelijk kan zijn om toch tot gegevensuitwisseling te komen tussen bijvoorbeeld een RIEC en een Zorg- en Veiligheidshuis. In dergelijke situaties zullen de mogelijkheden daartoe op basis van de inhoud van de casus en de mogelijkheden van de deelnemers aan beide samenwerkingsverbanden beoordeeld moeten worden. Het zal immers vaak voorkomen dat dezelfde deelnemers deelnemen aan meerdere samenwerkingsverbanden. Daarbij kan het aangewezen zijn dat deelnemers een casus bij zowel het RIEC als bij het Zorg- en Veiligheidshuis inbrengen. Bij twijfel kan daartoe een oordeel gevraagd worden aan de rechtmatigheidsadviescommissie. Wel regelt dit wetsvoorstel de mogelijkheid om gegevens uit te wisselen tussen Zorg- en Veiligheidshuizen onderling, als dit noodzakelijk is gelet op het doel van de Zorg- en Veiligheidshuizen.

- Opsomming van te verstrekken gegevens aan de Zorg- en Veiligheidshuizen is te star

In de reactie van onder andere de Landelijke Vereniging van Managers van Zorg- en veiligheidshuizen wordt gepleit om de lijst van persoonsgegevens in artikel 51 niet op te nemen als een limitatieve lijst. Gezien de grote diversiteit in casuïstiek die in de Zorg- en Veiligheidshuizen aan de orde kan zijn, bestaat dan immers het risico dat in sommige gevallen bepaalde gegevens niet verstrekt mogen worden omdat ze niet op de lijst staan, terwijl dit wel noodzakelijk is. Zij pleiten voor de toevoeging van een bepaling dat het mogelijk maakt om in uitzonderingsgevallen ook andere gegevens te verwerken, indien dit naar het oordeel van de bij een casus betrokken deelnemers noodzakelijk is.

Artikel 51 regelt de persoonsgegevens die vallen onder de verplichting om te verstrekken aan het Zorg- en Veiligheidshuizen uit artikel 5. Voor deze gegevens is er altijd een grondslag om te verstrekken, voor zover dit noodzakelijk is gelet op het doel van de Zorg- en Veiligheidshuizen. Artikel 51 regelt niet dat deze gegevens structureel verstrekt moeten worden aan het Zorg- en veiligheidshuis. De bedoeling van artikel 51 is om op deze gegevens rustende geheimhoudingen en doelbindingsbepalingen te doorbreken, zoals toegelicht op artikel 5, eerste lid. Artikel 51 regelt niet dat het Zorg- en Veiligheidshuis uitsluitend de in dit artikel genoemde gegevens mag verwerken. Het regelt ook niet dat deelnemers die betrokken zijn bij een casus andere gegevens niet zouden mogen verstrekken. Indien een deelnemer op basis van de inhoud van de casus

tot de conclusie komt dat ook andere gegevens noodzakelijk zijn om te verstrekken, met het oog op het doel van het Zorg- en Veiligheidshuis, dan zal deze op basis van zijn eigen juridische kader moeten beslissen of hij die gegevens in een concreet geval ook kan verstrekken. Daarbij zal onder andere aan de orde zijn of het verstrekken ten behoeve van de samenwerking in het Zorg- en Veiligheidshuis gezien zijn eigen betrokkenheid bij de casus, verenigbaar is met de doelen waarvoor hij de gegevens ooit heeft verzameld. Ook zal de deelnemer moeten toetsen of er geen geheimhoudingsbepalingen verstrekking in de weg staan. Dit wetsvoorstel bevat tevens een aantal waarborgen. Zo wordt de verstrekking van de gegevens in artikel 51 ingeperkt door artikel 5, eerste lid, dat bepaalt dat een deelnemer de gegevens niet hoeft te verstrekken indien zwaarwegende belangen zich daartegen verzetten. Artikel 50, tweede lid, stelt voorwaarden aan gegevens die vallen onder een wettelijk beroepsgeheim zoals geregeld in de Wgbo, de Wet BIG, of de Jeugdwet. En artikel 50, derde lid, geeft deelnemers aan en Zorg- en Veiligheidshuis de mogelijkheid om voorwaarden en beperkingen te stellen aan de verdere verwerking van gegevens die hij aan het Zorg- en Veiligheidshuis heeft verstrekt. De regering is van mening dat er hiermee voldoende mogelijkheden bestaan om indien noodzakelijk ook andere gegevens aan het Zorg- en Veiligheidshuis te verstrekken, en dat een nog ruimere reikwijdte van de verplichte verstrekkingen niet nodig is.

- Gegevens voor wat betreft natuurlijke personen uit de directe kring van betrokkene

Een aantal reacties geven aan dat deze bepaling in artikel 51 wel erg onbepaald is.

In de memorie van toelichting is een nadere toelichting opgenomen over welke personen hiermee worden bedoeld. Ook is opgenomen dat er alleen gegevens verwerkt mogen worden over de betreffende persoon, voor zover dat in relatie staat tot de problematiek van de betrokkene die in de casus behandeld wordt.

II. ARTIKELSGEWIJS

HOOFDSTUK 1. ALGEMENE BEPALINGEN

Artikel 1 (definities)

Een belangrijk element uit de definitie van samenwerkingsverband is dat samenwerkingsverbanden noch een bestuursorgaan, noch een natuurlijke of rechtspersoon zijn. Een samenwerkingsverband in de zin van deze wet moet worden gezien als de deelnemers tezamen. Uit het voorgestelde artikel 4 volgt dat de deelnemers gezamenlijke verwerkingsverantwoordelijken zijn in de zin van de AVG. Terwijl het bestuursrecht in beginsel het bestuursorgaan als "bouwsteen" gebruikt en het burgerlijke recht uitgaat van natuurlijke en rechtspersonen, daar gaat de AVG uit van "verwerkingsverantwoordelijken". De bevoegdheid om persoonsgegevens te verwerken komt toe aan de verwerkingsverantwoordelijken: de deelnemers van het samenwerkingsverband die bij of krachtens artikel 3 zijn aangewezen. Het kan overigens gaan om zowel een specifiek landelijk samenwerkingsverband als een specifiek stel van regionale samenwerkingsverbanden.

Volgens de definitie van deelnemers kan het gaan om overheidsinstanties, overheidsorganen en private partijen. Uiteraard kan het bij een overheidsinstantie of overheidsorganisatie ook gaan om een gemandateerde.

Het begrip sturingsinformatie is gedefinieerd omdat dit bij sommige samenwerkingsverband het beoogde resultaat van de gezamenlijke gegevensverwerking in het samenwerkingsverband is. Het gaat om handelingsperspectieven voor de deelnemers. Het kan gaan om een eerste vermoeden dat er sprake zou kunnen zijn van een strafbaar feit of een onrechtmatige handeling of overtreding.

Voor de opsporingsdiensten en het OM geldt ook dat sturingsinformatie niet direct als bewijs kan worden gebruikt zonder dat er eerst nog nader opsporingsonderzoek plaatsvindt.

Aangezien de definities zoals opgenomen in artikel 4 van de AVG rechtstreekse werking hebben vanaf 25 mei 2018, spreekt het voor zichzelf dat deze van toepassing zijn op de WGS en de daarop berustende bepalingen.

Artikel 2 (reikwijdte)

Uit het artikel volgt dat de wet uitsluitend van toepassing is op een samenwerkingsverband voor zover dit bij of krachtens deze wet is aangewezen. Op deze wijze zal geen misverstand kunnen bestaan over de vraag of een samenwerkingsverband onder de werking van de WGS valt. Duidelijk is hierdoor dat de WGS niet van toepassing is op samenwerkingsverbanden die *niet* bij of krachtens deze wet zijn aangewezen als samenwerkingsverband in de zin van de WGS. Dergelijke samenwerkingsverbanden zijn voor hun bevoegdheden inzake verwerking van gegevens afhankelijk van de mogelijkheden die andere wetgeving biedt. Er verandert dus niets voor samenwerkingsverbanden die niet worden aangewezen als samenwerkingsverband in de zin van de WGS.

Uit het tweede lid vloeit voort dat het deelnemers aan een samenwerkingsverband, dat onder de werking van de WGS valt, vrij staat om gegevens op andere, zoals bilaterale of multilaterale, wijze te verwerken voor zover daar een rechtsgrond voor is.

Indien een samenwerkingsverband wordt aangewezen bij amvb, moge het voor zich spreken dat deze amvb wordt voorgedragen door de meest betrokken bewindspersonen, zoals met name bewindspersonen onder wie deelnemers ressorteren.

Uit het wetsvoorstel vloeit overigens voort dat een bij of krachtens deze wet aangewezen samenwerkingsverband enkel kan worden opgeheven na wijziging van deze wet onderscheidenlijk de amvb.

Artikel 3 (deelnemers)

Eerste lid
Van een samenwerkingsverband kunnen zowel overheidsinstanties, overheidsorganen als private partijen deel uitmaken.
Op grond van het eerste lid kunnen partijen uitsluitend deelnemen aan een samenwerkingsverband indien die in hoofdstuk 2 of bij algemene maatregel van bestuur zijn aangewezen.

Tweede lid
Het tweede lid bepaalt dat aanwijzing als deelnemer slechts geschiedt indien deelname noodzakelijk is voor het doel van het samenwerkingsverband. Deze waarborg betekent dat de kring van partijen die aan samenwerkingsverbanden kunnen deelnemen, wordt afgebakend tot de relevante partijen. Voorkomen moet worden dat partijen 'gratuit' aan een samenwerkingsverband gaan deelnemen terwijl het doel van het samenwerkingsverband niet aansluit bij hun werkzaamheden.

Derde lid
Het derde lid opent de mogelijkheid voor deelname van private partijen. Vanwege de publieke belangen die worden nagestreefd met een samenwerkingsverband, volgt uit het derde lid dat het samenwerkingsverband niet zal kunnen bestaan uit uitsluitend private partijen, maar er altijd tevens publieke partijen deel van uitmaken. Wat zodoende onder de voorgestelde wet zou kunnen, is een samenwerkingsverband tussen politie, OM en containervervoerders ter bestrijding ladingdiefstal.

Vierde lid
Het vierde lid expliciteert dat aan het samenwerkingsverband of aan deelnemers geen nieuwe taken of bevoegdheden worden verleend. Het wetsvoorstel regelt enkel dat een samenwerkingsverband *gezamenlijk* gegevens mag verwerken voor zover dat noodzakelijk is voor een bij of krachtens deze wet vastgesteld doel van zwaarwegend algemeen belang. Dit moet worden beschouwd als een taak van algemeen belang als bedoeld in 6, eerste lid, onder e, van de AVG. Zoals de tekst van het wetsvoorstel impliceert, bestaat de taak uit gegevensverwerking. Met het wetsvoorstel is niet beoogd dat het samenwerkingsverband een geheel op zichzelf staande taak wordt verleend; de taak van het samenwerkingsverband is uiteindelijk bedoeld om de behartiging van algemene belangen van één of meer deelnemers te ondersteunen. Een samenwerkingsverband krijgt evenmin bestuursrechtelijke bevoegdheden.

Vijfde lid
Het vijfde lid stelt buiten twijfel dat een samenwerkingsverband geen rechtspersoonlijkheid heeft. Samenwerkingsverbanden die bij of krachtens deze worden aangewezen, krijgen daarmee geenszins rechtspersoonlijkheid of openbaar gezag. Dit wetsvoorstel dient slechts om te voorzien grondslagen voor de verwerkingen van gegevens door samenwerkingsverbanden. Zoals reeds is toegelicht in paragraaf 3.2.1 is het niet de bedoeling dat er een nieuw overheidsorgaan, nieuwe instantie of zelfstandige entiteit van enige vorm ontstaat. Het uitgangspunt van de gezamenlijke verwerkingsverantwoordelijkheid van de deelnemers is onverenigbaar met eigen rechtspersoonlijkheid van het samenwerkingsverband. Eigen rechtspersoonlijkheid zou een nieuwe, zelfstandige entiteit creëren, die bovendien aan de ministeriële verantwoordelijkheid onttrokken zijn. Er zijn ook overigens geen steekhoudende argumenten voor eigen rechtspersoonlijkheid van samenwerkingsverbanden in de zin van dit wetsvoorstel.

Zesde lid
Het ongedaan maken van een aanwijzing verloopt op grond van het zesde lid niet noodzakelijk via dezelfde procedure als waarmee de aanwijzing heeft plaatsgevonden. Indien deelname niet meer noodzakelijk is voor het doel van het samenwerkingsverband, is het wenselijk dat deelname van een in hoofdstuk 2 genoemde deelnemer, op korte termijn bij amvb kan worden beëindigd.

Artikel 4 (gezamenlijke verwerkingsverantwoordelijkheid)

Eerste lid
Aangezien geen sprake is van eigen rechtspersoonlijkheid van het samenwerkingsverband en het samenwerkingsverband als zodanig geen bestuursorgaan is, dient de verdeling van verantwoordelijkheid voor de verwerking van persoonsgegevens anders te worden ingericht. Daarom worden de deelnemers als gezamenlijke verwerkingsverantwoordelijken aangewezen door het onderhavige artikel.

Met het voorgestelde artikel 4 wordt uitvoering gegeven aan art. 4, zevende lid, tweede volzin, AVG: "wanneer de doelstellingen van en middelen voor deze verwerking in het (…) lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen". Het is uit een oogpunt van bescherming van persoonsgegevens van belang duidelijk vast te stellen wie met betrekking tot de gegevensverwerking als verwerkingsverantwoordelijken in de zin van de AVG zijn aan te merken. Op deze verantwoordelijken rusten immers verschillende verplichtingen, zoals de beveiligingsplicht en de verplichting betrokkenen gebruik te kunnen laten maken van hun inzage– en correctierecht. Op grond van artikel 82 AVG is in geval van gezamenlijke verwerkingsverantwoordelijken elke verwerkingsverantwoordelijke voor de gehele schade aansprakelijk die wordt veroorzaakt door een verwerking die inbreuk maakt op de AVG.
Indien een verwerkingsverantwoordelijke een bestuursorgaan is, dan worden beslissingen die genomen zijn inzake de rechten van betrokkene gelijkgesteld aan besluiten in de zin van de Awb op grond van artikel 34 van de Uitvoeringswet AVG, zodat bestuursrechtelijke

rechtsbescherming openstaat. Indien een verwerkingsverantwoordelijke geen bestuursorgaan is, dan gelden dergelijke beslissingen niet als besluiten, waardoor civielrechtelijke rechtsbescherming openstaat (artikel 35 Uitvoeringswet AVG). Overigens bepaalt artikel 26, derde lid, van de AVG dat onverminderd de onderlinge afspraken, betrokkenen hun rechten uit hoofde van de AVG tegen iedere verwerkingsverantwoordelijke kunnen uitoefenen.

Tweede lid
In het voorgestelde tweede lid is geregeld dat de deelnemers één van de functionarissen voor gegevensbescherming van de deelnemende overheidsinstanties of overheidsorganen aanwijzen als coördinerend functionaris gegevensbescherming voor het samenwerkingsverband. Dit voorkomt onduidelijkheden. Voor het samenwerkingsverband wordt uit hun midden een coördinerend functionaris voor gegevensbescherming aangewezen. Deze coördinerend functionaris voor gegevensbescherming is belast met de taken op grond van artikel 39 AVG en coördineert de voorbereiding van audits. De coördinerend functionaris voor gegevensbescherming is ook een aanspreekpunt voor deelnemers naast de eigen functionaris voor gegevensbescherming die het eerste aanspreekpunt blijft voor bestuurders van de afzonderlijke deelnemers. Deze coördinerend functionaris voor gegevensbescherming heeft een coördinerende en faciliterende taak en moet samenwerken met de andere fg's van de deelnemers om te proberen tot consensus te komen.

Derde lid
Deze bepaling verduidelijkt onder meer dat het samenwerkingsverband geen medewerkers in dienst neemt. De medewerkers blijven in dienst van de deelnemers.
Indien een deelnemer tevens niet publieke doelen nastreeft, dient deze gegevensverwerking zoveel mogelijk gescheiden te zijn van de gegevensverwerking van publieke doelen. Daartoe is de bepaling opgenomen dat een private deelnemer ten behoeve van de inzet in het samenwerkingsverband slechts personen aanwijst die niet tevens worden belast met commerciële werkzaamheden voor die private partij.

Vierde lid
Deze bepaling regelt de verplichting om bij algemene maatregel van bestuur invulling te geven aan het lidstatelijk recht, bedoeld in artikel 26 van de AVG. Daaruit volgt dat gezamenlijke verwerkingsverantwoordelijken hun respectieve verantwoordelijkheden voor de nakoming van de uit de AVG volgende verplichtingen vaststellen door middel van een onderlinge regeling, *tenzij en voor zover lidstatelijk recht dit regelt*.
Dit betekent dat in de amvb de verdeling van verantwoordelijkheid in de zin van artikel 26 van de AVG tussen de verschillende verwerkingsverantwoordelijken wordt geregeld.
Het is mogelijk om in de amvb te differentiëren naar de verschillende verwerkingen: er kan bijvoorbeeld sprake zijn van afzonderlijke verantwoordelijkheid per (deel)verwerking.

In het vierde lid, onder a, is dit geconcretiseerd doordat een wettelijke verplichting is opgenomen voor het nader uitwerken van de wijze waarop binnen het samenwerkingsverband door de deelnemers wordt samengewerkt. Het kan bijvoorbeeld zo zijn, dat er voor specifieke vragen ad hoc samenwerking plaatsvindt tussen slechts enkele deelnemers. Ook kan de uitwerking van de verantwoordelijkheden vorm krijgen door te regelen dat aan bepaalde verwerkingsactiviteiten slechts enkele deelnemers mogen meedoen.

In het vierde lid, onder b, is geregeld dat een deelnemende overheidsinstantie of een deelnemend overheidsorgaan als contactpunt moet worden aangewezen in de zin van artikel 26 AVG. Het contactpunt treedt voor burgers op als aanspreekpunt voor het uitoefenen van rechten op grond van de AVG.

Artikel 5 (verstrekking aan het samenwerkingsverband)

Er is in het wetsvoorstel sprake van drie fasen van gegevensverwerking, namelijk: 1) verstrekking aan het samenwerkingsverband, 2) verwerking binnen het samenwerkingsverband en 3) verstrekking uit het samenwerkingsverband van de resultaten van de gegevensverwerking.
In schemavorm ziet dit er als volgt uit:

Fase 1: Deelnemer verstrekt gegevens aan het samenwerkingsverband (op grond van artikel 5 en/of de voorgestelde wijziging van de Wpg, Wjsg en andere sectorale wetten)	→	**Fase 2:** Deelnemers van het samenwerkingsverband verwerken gezamenlijk gegevens voor het doel van het samenwerkingsverband (op grond van artikel 2, tweede lid, in samenhang met specifieke grondslag uit hoofdstuk 2 of amvb)	→	**Fase 3:** Het samenwerkingsverband verstrekt de resultaten van de gezamenlijke gegevensverwerking aan een deelnemer of een derde (op grond van en onder de voorwaarden van artikel 7)

Het voorgestelde artikel 5 regelt de eerste fase. Dat is nodig, want zoals in het algemeen deel van deze memorie van toelichting uitgebreid is toegelicht, bevatten sectorspecifieke regelingen niet zozeer grondslagen voor verstrekking aan meerdere partijen tegelijk (zoals verstrekking aan deelnemers van een samenwerkingsverband tegelijk) als wel grondslagen voor unilaterale verstrekking tussen twee partijen onderling. Artikel 5 voorziet in een basis voor verstrekking aan meerdere partijen tegelijk.

Het voorgestelde artikel 5, eerste lid, bevat een verplichting voor de deelnemers om de in hoofdstuk 2 of bij amvb aangewezen categorieën gegevens te verstrekken aan het samenwerkingsverband voor zover dat noodzakelijk is voor de vervulling van het doel van het samenwerkingsverband. Uit de aanwijzing van de categorieën gegevens blijkt of het gaat om persoonsgegevens en/of andere gegevens en verder om welke categorieën het dan precies gaat.

Artikel 5, eerste lid, bevat een uitzondering op de verstrekkingsplicht ingeval "zwaarwegende redenen zich daartegen verzetten". De deelnemer die gegevens zou moeten verstrekken bepaalt exclusief of er zwaarwegende redenen zijn die zich daartegen verzetten. Andere deelnemers hebben daar in juridische zin geen zeggenschap over, om te voorkomen dat daarover rechtsonzekerheid ontstaat. Zo staat het ook uitdrukkelijk in het voorgestelde artikel 5, eerste lid. Deze tenzij-clausule maakt het overigens ook mogelijk om de gegevens alleen aan *sommige* deelnemers niet te verstrekken.

Artikel 5, eerste lid, vormt de basis voor de verstrekking van gegevens aan het samenwerkingsverband en is een rechtsgrond voor de verwerking van persoonsgegevens in de zin van artikel 6, eerste lid, onder c, en derde lid, aanhef en onder b, AVG (wettelijke plicht).

Artikel 5, eerste lid, doorbreekt tevens geheimhoudingsbepalingen uit andere wetten, wanneer die de ruimte bevatten om bij wettelijk voorschrift van de geheimhoudingsplicht af te wijken. Dit is nodig omdat een dergelijke geheimhoudingsbepaling op gespannen voet kan staan met het uitgangspunt van de integrale benadering door een samenwerkingsverband.

Artikel 5, eerste lid, maakt dan ook gebruik van de ruimte die bepaalde geheimhoudingsbepalingen toelaten om daarvan bij wettelijk voorschrift af te wijken. Het gaat dan onder meer om de volgende geheimhoudingsplichten, die onder de condities van artikel 5, eerste lid, worden doorbroken:

- artikel 67 van de Algemene wet inzake rijksbelastingen;
- artikel 74 van de Wet structuur uitvoeringsorganisatie werk en inkomen;
- artikel 65 van de Participatiewet;
- artikel 2:5 Algemene wet bestuursrecht;
- Artikel 5.3.3 van de Wet maatschappelijke ondersteuning 2015;
- Artikel 8:34 van de Wet verplichte geestelijke gezondheidszorg;
- Artikel 18c, vierde lid, van de Wet zorg en dwang psychogeriatrische en verstandelijk gehandicapte cliënten.

De exceptie uit artikel 5, eerste lid, inzake de zwaarwegende redenen laat onverlet dat artikel 5, eerste lid, een wettelijke verplichting tot gegevensverstrekking is.

Artikel 5 laat echter onverlet de geheimhoudingsplichten uit sectorale wetgeving die geen afwijking bij wettelijk voorschrift toelaten. Voor een aantal van deze geheimhoudingsplichten is het wenselijk en noodzakelijk dat uitzonderingen op die geheimhoudingsplichten worden opgenomen. Dit is gebeurd in hoofdstuk 4 van de WGS. Door de voorgestelde wijzigingen van die sectorale wetten worden geheimhoudingsplichten uit de volgende wetten doorbroken:

- Wet politiegegevens;
- Wet justitiële en strafvorderlijke gegevens;
- Wet op het financieel toezicht;
- Wet toezicht accountantsorganisaties;
- Wet toezicht trustkantoren 2018;
- Wet ter voorkoming van witwassen en financieren van terrorisme;
- Sanctiewet 1977;
- de Wet toezicht financiële verslaggeving;
- de Wet handhaving consumentenbescherming.

Artikel 5, tweede lid, expliciteert het voorgaande, door te bepalen dat de verstrekking van politiegegevens, justitiële en strafvorderlijke gegevens plaatsvindt op grond van de nieuwe grondslagen die via hoofdstuk 4 van de WGS worden toegevoegd aan de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens. Door dit te expliciteren wordt beoogd om onduidelijkheden weg te nemen. Dit is temeer van belang, omdat politie, OM en (bepaalde) bijzondere opsporingsdiensten deelnemen aan alle samenwerkingsverbanden die worden aangewezen in het voorgestelde hoofdstuk 2 van deze wet.

Artikel 5, derde lid, bevat een uitzondering op het verbod om persoonsgegevens van strafrechtelijke aard te verwerken. In veel gevallen zal artikel 33, eerste lid, onder a, slotzinsnede, Uitvoeringswet AVG reeds van toepassing zijn als uitzondering op het verbod om persoonsgegevens van strafrechtelijke aard, namelijk in die gevallen waarin deelnemers aan het samenwerkingsverband dergelijke persoonsgegevens "hebben verkregen krachtens de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens". Dit is het geval wanneer de politie of het openbaar ministerie gegevens verstrekken op grond van de in hoofdstuk 4 voorgestelde grondslagen in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens.
Ook zal artikel 33, eerste lid, onder b, Uitvoeringswet AVG soms opgaan. Daarin is een uitzondering opgenomen op het verbod om persoonsgegevens van strafrechtelijke aard te verwerken als de verwerking geschiedt door en ten behoeve van publiekrechtelijke samenwerkingsverbanden.
Er is echter nog geen uitzondering op het verbod om persoonsgegevens van strafrechtelijke aard te verwerken wanneer dergelijke gegevens aan het samenwerkingsverband worden verstrekt door een deelnemer die niet onder de Wpg of Wjsg valt (te denken valt bijvoorbeeld aan een gemeente) én er geen sprake is van een samenwerkingsverband dat volledig bestaat uit publiekrechtelijke partijen. Voor

dergelijke gevallen maakt artikel 5, derde lid, een uitzondering. Deze uitzondering is relevant voor de Zorg- en Veiligheidshuizen en voor het Financieel Expertisecentrum.

Artikel 5 ziet niet op de verwerking van bijzondere categorieën van persoonsgegevens in de zin van artikel 1 van de Uitvoeringswet Algemene verordening gegevensbescherming. Paragrafen 2.3 en 2.4 van dit wetsvoorstel bevatten hierover twee artikelen met uitzonderingen op het verwerkingsverbod (de artikelen 34 en 50). Op bijzondere categorieën persoonsgegevens zijn de AVG en andere wetten, zoals de Uitvoeringswet AVG van toepassing, die een aantal uitzonderingen bevatten op het verbod dergelijke persoonsgegevens te verwerken. Een relevante uitzondering is het bestaande artikel 23, onder c, Uitvoeringswet AVG. Daarin is geregeld dat het verbod om bijzondere categorieën van persoonsgegevens te verwerken niet van toepassing, indien "de verwerking noodzakelijk is in aanvulling op de verwerking van persoonsgegevens van strafrechtelijke aard voor de doeleinden waarvoor deze gegevens worden verwerkt". Het gaat hierbij om de situatie waarin persoonsgegevens van strafrechtelijke aard mogen worden verwerkt, én dat deze gegevens tevens betrekking hebben op een bijzonder persoonsgegeven. Voor zover daarbij persoonsgegevens van strafrechtelijke aard moeten worden vastgelegd, laat het bestaande artikel 23, onder c, dat toe.

Artikel 6 (verwerking binnen het samenwerkingsverband)

Artikel 6, eerste lid, beschrijft op beknopte wijze de verwerkingen binnen het samenwerkingsverband en sluit nauw aan bij de definitie van samenwerkingsverband.
Artikel 6, tweede lid, stelt buiten twijfel dat persoonsgegevens van strafrechtelijke aard die op grond van artikel 5 zijn ontvangen, vervolgens mogen worden verwerkt binnen het samenwerkingsverband. Aldus regelen de artikelen 5, 6 en 7 voor alle samenwerkingsverbanden dat dergelijke persoonsgegevens mogen worden verwerkt, zowel in de fase van verstrekking aan het samenwerkingsverband, verwerking binnen het samenwerkingsverband als verstrekking van de resultaten door het samenwerkingsverband.

Artikel 7 (verstrekking van de resultaten aan deelnemers en derden)

Eerste lid
Artikel 7, eerste lid, is een rechtsgrond voor de verwerking van persoonsgegevens in de zin van artikel 6, eerste lid, onder c, en derde lid, aanhef en onder b, AVG (wettelijke plicht).

Met het voorgestelde artikel 7, eerste lid, wordt geregeld dat deelnemers beschikken over de resultaten van de verwerking uit het samenwerkingsverband voor zover verstrekking noodzakelijk is voor:

a. de vervulling van een publiekrechtelijke taak die aan de deelnemer is opgedragen, wanneer deze verenigbaar is met het doel van het samenwerkingsverband, of
b. de behartiging van de gerechtvaardigde belangen of de uitvoering van wettelijke verplichtingen van een private deelnemer, wanneer deze verenigbaar zijn met het doel van het samenwerkingsverband. Dat verstrekking ook kan vanwege de wettelijke verplichtingen van private deelnemers houdt verband met het feit dat het bij private deelnemers ook om wettelijke verplichtingen kan gaan, zoals voor de banken o.g.v. de Wwft.

Na de ontvangst van de resultaten is artikel 6, eerste lid, onder e of f AVG de rechtsgrond voor de verwerking: heeft de (ontvangende) deelnemer een taak van algemeen belang, dan kan deze de resultaten verwerken op grond van een (in sectorale wetgeving gedefinieerde) taak van algemeen belang, bedoeld in artikel 6, eerste lid, onder e, AVG. Betreft het een private deelnemer (zonder taak van algemeen belang), dan mag die de resultaten verwerken voor een gerechtvaardigd belang als bedoeld in artikel 6, eerste lid, onder f, AVG.

De verstrekkende verwerkingsverantwoordelijken binnen het samenwerkingsverband zijn verantwoordelijk voor de verstrekking en zijn dus verantwoordelijk voor de beoordeling of in concreto voldaan is aan de voorwaarden van artikel 7. De zinsnede "Tenzij naar het oordeel van een deelnemer zwaarwegende redenen zich daartegen verzetten worden" vereist niet in elk individueel geval een aparte beoordeling; voldoende is een algemene beoordeling voor de start van een project. De tenzij-clausule maakt het onder meer mogelijk om de gegevens alleen aan bepaalde partijen niet te verstrekken.

Tweede lid
Deze bepaling regelt dat de resultaten kunnen worden verstrekt aan derden, voor zover dat noodzakelijk is voor het doel van het samenwerkingsverband, op voorwaarde dat deze verstrekking (krachtens het tweede lid) bij amvb mogelijk is gemaakt (of in hoofdstuk 2 van de WGS). Doorgaans zal de grond voor gegevensverwerking door de ontvanger artikel 6, eerste lid, onder e, AVG zijn. De tenzij-clausule dient op dezelfde wijze te worden geïnterpreteerd als hierboven bij het eerste lid is toegelicht.

Vierde en vijfde lid
Deze bepalingen betreffen de verplichting voor ontvangers van resultaten van de gegevensverwerking van het samenwerkingsverband om terug te koppelen wat de effectiviteit en bruikbaarheid van de resultaten was. De deelnemers van het samenwerkingsverband evalueren hiermee de gehanteerde werkwijze. Om bij te dragen aan de kwaliteit van de gegevens is het van belang dat er een terugkoppeling moet zijn: wat wordt gedaan met de meldingen die zijn gedaan met gebruikmaking van bijvoorbeeld data-analysetechnieken? Hebben die daadwerkelijk witwasconstructies aan het licht gebracht of waren het onterechte meldingen? Deze feedback is nodig om te toetsen of de gegevensverwerking noodzakelijk en effectief is. Feitelijk is dit een kwaliteitscirkel. Een constante aanscherping van de werkwijze, en indien van toepassing de gehanteerde patronen en indicatoren, is wezenlijk.

Zevende lid
Het zevende lid stelt buiten twijfel dat persoonsgegevens van strafrechtelijke aard die op grond van artikel 5 zijn ontvangen, en die op grond van artikel 6, tweede lid, vervolgens mogen worden verwerkt binnen het samenwerkingsverband, eveneens mogen worden verwerkt bij de verstrekking van de resultaten door het samenwerkingsverband, onder de voorwaarden van artikel 7, waarvan met name het eerste en tweede lid van belang zijn.

Artikel 8 (waarborgen)

Deze bepaling schept een aantal waarborgen in aanvulling op de waarborgen van de AVG - om bij te dragen aan de zorgvuldige verwerking daarvan.

Het eerste lid geeft de mogelijkheid om nadere voorwaarden en beperkingen te verbinden aan de gegevensverwerking. Zo kan bijvoorbeeld bij algemene maatregel van bestuur worden geregeld dat de verstrekking, bedoeld in artikel 5 of 7, niet of niet zonder meer geschiedt aan bepaalde deelnemers (bijvoorbeeld niet aan private partijen) of aan derden.

Volledigheidshalve wordt opgemerkt dat artikel 8, eerste lid, ook de mogelijkheid omvat om te regelen dat aan bepaalde verwerkingsactiviteiten als bedoeld in artikel 30 AVG slechts enkele deelnemers mogen meedoen.

In het voorgestelde artikel 8 is voorts voorzien in een aantal specifieke waarborgen:
- een systeem van autorisaties, dat wil zeggen de verlening van toegang tot de systemen waarin de samenwerkingsverbanden gegevens verwerken aan uitsluitend door de deelnemers geautoriseerde medewerkers (tweede lid);
- een verplichting tot screening van medewerkers (derde lid);
- het verplichting tot het loggen van gegevens die noodzakelijk zijn voor controle en toezicht (vierde lid)

- een verplichting tot het instellen van een rechtmatigheidsadviescommissie die de rechtmatigheid van de verwerking van persoonsgegevens door het samenwerkingsverband beoordeelt (zesde lid)
- een vernietigingstermijn (zevende lid);
- een adequaat beveiligingsniveau overeenkomstig richtlijnen van de minister van BZK (zevende lid). Bij dat laatste kan worden gedacht aan de Baseline Informatiebeveiliging Overheid (BIO), die de ministerraad op 14 december 2018 heeft vastgesteld voor het Rijk en in het interbestuurlijk verkeer met het Rijk. De BIO is een gemeenschappelijk normenkader, gebaseerd op de internationale norm ISO 27001/2 voor de beveiliging van de informatie(systemen) van de overheid en bevat een concretisering van een aantal normen tot verplichte overheidsmaatregelen. Ten aanzien van de beveiliging van bijzondere categorieën persoonsgegevens in de zin van artikel 9 AVG en persoonsgegevens van strafrechtelijke aard in de zin van artikel 10 AVG gelden hogere beveiligingsvereisten dan ten aanzien van de beveiliging van reguliere persoonsgegevens in de zin van artikel 4, onderdeel 1, AVG.

De rechtmatigheidsadviescommissie dient om te adviseren over grondslagen en over te treffen technische en organisatorische maatregelen. Wat betreft de rechtmatigheidsadviescommissie geldt dat de precieze inrichting van deze commissie en de gehanteerde werkwijze niet in de wet geregeld behoeven te worden. Een rechtmatigheidsadviescommissie bestaat doorgaans uit privacy-experts en compliance deskundigen en beoordeelt in ieder geval de rechtmatige verwerking van persoonsgegevens in het samenwerkingsverband. Meer specifiek kan een rechtmatigheidsadviescommissie bijvoorbeeld de volgende taken hebben:

- Het voeren van structureel overleg over privacy met alle deelnemers;
- Het toetsen van gegevensbeschermingseffectbeoordelingen (PIA's), het – voor zover noodzakelijk – begeleiden bij de uitvoering daarvan en het uitbrengen van advies daarover aan de functionarissen voor gegevensbescherming en de gezamenlijke verwerkingsverantwoordelijken;
- Het in beeld brengen van de privacyissues die er zijn en het doen van voorstellen te doen voor mitigerende maatregelen aan de deelnemers;
- Het door middel van interne controlemechanismen, zoals de beoordeling van gegevensuitwisselingen door de rechtmatigheidsadviescommissie, contractuele afspraken alsook door het stimuleren van bewustzijn onder medewerkers en technische beheersmaatregelen, waarborgen dat de verzamelde gegevens enkel voor de vooraf vastgestelde doeleinden worden verwerkt;
- Bij concrete verwerkingen vooraf een rechtmatigheidsbeoordeling verrichten, opdat bij de verstrekking van het resultaat een aanduiding van de toepasselijke rechtmatigheidsbeoordeling kan worden gegeven.

Artikel 8a (bijzondere waarborgen inzake geautomatiseerde gegevensanalyse)

Met geautomatiseerde gegevensanalyse wordt gedoeld op verwerkingsprocessen waarbij bijvoorbeeld wiskundige en statistische procedures worden gehanteerd.

Het eerste lid verplicht de deelnemers tot het treffen van technische en organisatorische maatregelen om de kwaliteit van de gezamenlijke gegevensverwerking te bevorderen. Ook schept dit artikel een aantal specifieke waarborgen in aanvulling op de waarborgen van de AVG, om bij te dragen aan de kwaliteit van de gegevens: van belang is met name dat er een terugkoppeling moet zijn bij het gebruik van gezamenlijke data-analysetechnieken: wat wordt gedaan met de meldingen die zijn gedaan met gebruikmaking van de data-analysetechnieken? Hebben die daadwerkelijk witwasconstructies aan het licht gebracht of waren het onterechte meldingen? Deze feedback is nodig om te toetsen of de gegevensverwerking noodzakelijk en effectief is. Feitelijk is dit een kwaliteitscirkel. Een constante aanscherping van de werkwijze, en indien van toepassing gehanteerde patronen en indicatoren, is wezenlijk.

Het derde lid verplicht het samenwerkingsverband tot transparantie over de gehanteerde patronen en indicatoren of andere onderliggende logica. Dit is een belangrijke waarborg, zoals ook blijkt uit de rechtbank-uitspraak in de SyRI-zaak.

Het vierde lid gaat over de terugmelding door het samenwerkingsverband van onjuistheden aan de deelnemende organisatie waarvan de persoonsgegevens afkomstig zijn. Deze bepaling is het spiegelbeeld van artikel 19 AVG, dat juist betrekking heeft op de communicatie (over correcties) in de omgekeerde richting: door verstrekker aan ontvanger. Artikel 19 AVG regelt dat een verwerkingsverantwoordelijke iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis stelt van elke rectificatie, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt.

Voor het geval dat het samenwerkingsverband persoonsgegevens geautomatiseerd analyseert, schrijft het vijfde lid voor dat dit voor bij amvb vastgestelde fasen gepseudonimiseerd plaatsvindt. Pseudonimiseren is volgens artikel 4, onderdeel 5, AVG het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld *zonder dat er aanvullende gegevens worden gebruikt,* mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.
Om van gepseudonimiseerde persoonsgegevens te kunnen spreken moeten de aanvullende gegevens apart worden bewaard en moeten technische en organisatorische maatregelen zijn genomen om ervoor te zorgen dat de gepseudonimiseerde gegevens niet aan een natuurlijk persoon kunnen worden gekoppeld. De toepassing van pseudonimisering op persoonsgegevens kan de risico's voor de betrokkenen verminderen en kan de verwerkingsverantwoordelijken en de verwerkers helpen om hun verplichtingen inzake gegevensbescherming na te komen.
Voor deze waarborg is gekozen, omdat bij geautomatiseerde analyse van persoonsgegevens doorgaans relatief veel persoonsgegevens worden verwerkt en de risico's voor de bescherming van persoonsgegevens navenant groter kunnen zijn. Van de samenwerkingsverbanden die onder de WGS vallen, past iCOV al geautomatiseerde gegevensanalyse voor het opstellen van haar rapportages toe.

Artikel 8b (auditbepaling)

Deze auditbepaling is een extra waarborg uit de richtlijn gegevensbescherming opsporing en vervolging. De formulering is afkomstig uit de Wet politiegegevens en dient om een kwaliteitssysteem te waarborgen. Door deze formulering aan te laten sluiten bij de auditbepaling voor de deelnemers die voor de uitoefening van hun wettelijke taken vallen onder de reikwijdte van de Wpg is het voor die deelnemers mogelijk om de auditverplichtingen inhoudelijk op elkaar te laten aansluiten. Dit is efficiënter en een minder grote belasting. Blijkens artikel 39, eerste lid, onder b, AVG hebben de FG's ook een functie bij de betreffende audits. Ook de AP heeft aangegeven een expliciete rol van de FG's te zien bij dergelijke audits.

Artikel 9 (geheimhouding)

Het voorgestelde artikel 9, eerste lid, bevat een geheimhoudingsplicht voor degenen die die betrokken zijn bij de uitoefening van de taak van het samenwerkingsverband en daarbij de beschikking krijgen over persoonsgegevens en voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift ter zake van die gegevens een geheimhoudingsplicht geldt, behoudens voor zover artikel 7 of enig ander wettelijk voorschrift in verstrekking van de gegevens voorziet.
Een derde exceptie op de geheimhoudingsplicht is de situatie waarin de gegevensverstrekking noodzakelijk is voor het afleggen van verantwoording door een medewerker aan de deelnemer die hem heeft aangewezen voor de inzet in het samenwerkingsverband. Deze exceptie is toegevoegd naar aanleiding van het advies van

de Afdeling advisering van de Raad van State (paragraaf 4): "Het wetsvoorstel bevat geen concrete regels om te verzekeren dat het samenwerkingsverband en de deelnemende partijen voor de burger en voor degene die politiek verantwoordelijk is, effectief aanspreekbaar is. Dat probleem wordt versterkt doordat de medewerkers die namens hun organisatie binnen het samenwerkingsverband samenwerken, op grond van het wetsvoorstel in beginsel geheimhouding verschuldigd zijn aan hun eigen organisatie. Die geheimhoudingsplicht, hoewel uit een oogpunt van bescherming van persoonsgegevens begrijpelijk, kan het voor de deelnemende organisaties gecompliceerder maken om hun (gezamenlijke) verantwoordelijkheid voor de gegevensverwerking in de praktijk te effectueren omdat zij niet steeds over alle relevante informatie zullen kunnen beschikken."

Artikel 9, tweede lid, bevat een (afgeleide) geheimhoudingsplicht voor de ontvangers van de resultaten, voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift ter zake van die gegevens een geheimhoudingsplicht geldt, behoudens voor zover enig wettelijk voorschrift in verstrekking van de gegevens voorziet.

Artikel 9, derde lid, regelt de geheimhouding van "andere gegevens waarvan degene die betrokken is bij de werkzaamheden van het samenwerkingsverband het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden". Het gaat hier om overige gegevens die niet bekend mogen worden zoals bedrijfsgeheimen, informatiebeveiligingsmaatregelen, geheimen over aanstaande interventies en te vergaande details over de algoritmen.

Artikel 9a (jaarverslag)

Omwille van de transparantie van de gegevensverwerking en de democratische legimitatie wordt voorgesteld dat samenwerkingsverband jaarlijks een jaarverslag publiceren inzake de effectiviteit en bruikbaarheid van de resultaten van de gegevensverwerking.

HOOFDSTUK 2. BEPALINGEN INZAKE SPECIFIEKE SAMENWERKINGSVERBANDEN

Paragraaf 2.1 Financieel Expertisecentrum (FEC)

Artikel 11 (doel)

Artikel 11 bevat een omschrijving van het doel van de gegevensverwerking door het FEC waaronder alle huidige verwerkingsactiviteiten vallen. Centraal staat de versterking van de integriteit van het financiële stelsel. Het FEC kan samenwerken en gegevens verwerken met alle partijen die betrokken kunnen zijn of worden bij het voorkomen en bestrijden van financieel-economische criminaliteit en andere ernstige vormen van criminaliteit of van terrorismefinanciering, alsmede risico's met betrekking tot de integriteit van natuurlijke of rechtspersonen die binnen het financiële stelsel werkzaam zijn.
Het financiële stelsel is een breed begrip. Daaronder wordt niet alleen verstaan de banken en andere financiële ondernemingen als gedefinieerd in artikel 1:1 van de Wet op het financieel toezicht, zoals geldtransactiekantoren, beleggings- en verzekeringsmaatschappijen, maar ook overige bijvoorbeeld eveneens de meldplichtige Wwft-instellingen van de Wwft, zoals notarissen, advocaten en makelaars.
Daarbij kan het FEC samenwerken en gegevens uitwisselen met zowel publieke als private partijen voor zover dat noodzakelijk is voor de uitoefening van publiekrechtelijke taken en bevoegdheden van die (publieke of private) partijen, die als deelnemer bij of krachtens de wet zijn aangewezen.
Ook private partijen kunnen een bijdrage leveren aan het uitoefenen van publiekrechtelijke taken en bevoegdheden, zoals bedoeld in artikel 11. Zo is bijvoorbeeld het voorkomen van witwassen en terrorismefinanciering een publiekrechtelijke taak, waarin niet alleen diverse publieke partijen, zoals de in artikel 12 genoemde deelnemers aan het FEC, een rol hebben maar eveneens meerdere private partijen een rol kunnen vervullen. In dit kader vervullen die laatste, zoals banken, verzekeraars, notarissen, de

zogenoemde poortwachtersfunctie. Ook andere private partijen dan die een poortwachtersfunctie vervullen, leveren een bijdrage aan een publiekrechtelijke taak wanneer zij aan een project of andere activiteiten van het FEC deelnemen, bijvoorbeeld een project met het oog op het uitoefenen van publiekrechtelijke taken en bevoegdheden gericht op het voorkomen van corruptie of witwassen en terrorismefinanciering, en kunnen derhalve als deelnemer bij amvb worden aangewezen.

Het Financieel Expertisecentrum verwerkt gegevens, voor zover dat noodzakelijk is voor de uitoefening van publiekrechtelijke taken en bevoegdheden van de deelnemers. Met deze formulering wordt aangesloten op het noodzakelijkheidsvereiste van artikel 6 van de Algemene verordening gegevensbescherming. De huidige wijze van gegevensverstrekking in het FEC, waaronder één van de basiskenmerken van het FEC waarbij getoetst wordt of bepaalde informatie van de ene partner van belang kan zijn voor een andere FEC partner, is essentieel en daarmee noodzakelijk om de doelstellig van het FEC te bereiken.
In lid 2 dient de zinsnede "doen en nalaten" breed uitgelegd te worden. In de eerste plaats gaat het daarbij om het bewust faciliteren van financieel-economische criminaliteit en andere ernstige vormen van criminaliteit of van terrorismefinanciering. Het gaat echter ook om het onbewust faciliteren daarvan wanneer crimineel geld bijvoorbeeld van de ene rekening op een andere wordt overgemaakt, zonder dat de financiële instelling weet of kan vermoeden dat het om criminele of terroristische gelden gaat. Ten slotte valt hier ook onder dat private partijen in bepaalde gevallen barrières op kunnen werpen, of dit juist niet of onvoldoende doen, om criminele handelingen te voorkomen.

Bij risico's met betrekking tot de integriteit van natuurlijk of rechtspersonen die binnen het financiële stelsel werkzaam zijn, moet men denken aan onder andere risico's met betrekking tot betrouwbaarheid en geschiktheid van bestuurders, (mede)beleidsbepalers en personen die toezicht houden op het beleid van ondernemingen die actief zijn binnen het financiële stelsel. Voor het maatschappelijke vertrouwen in het financiële stelsel, is het immers van groot belang dat de personen die binnen het financiële stelsel actief zijn, integer zijn. Een ander voorbeeld van een dergelijk risico, is het risico van het niet naar behoren functioneren van de poortwachtersfunctie. Op het moment dat enkele (rechts)personen die werkzaam zijn binnen het financiële stelsel tekortschieten bij het voorkomen van fraude of witwaspraktijken, kan dit het vertrouwen in het gehele financiële stelsel schaden.

Artikel 12 (deelnemers)

In de FEC-raad is er sprake van partners enerzijds. Dit zijn partijen die een vaste positie hebben in de FEC-raad. De lijst van deelnemers in het voorgestelde artikel komt overeen met de bestaande "partners" van het FEC. De deelnemers aan het FEC hebben alle een taak bij het versterken van de integriteit van de financiële sector.
Anderzijds zijn er bij het FEC participanten: dit zijn organisaties die geen vaste positie hebben in de FEC-raad. Het betreft partijen die alleen aan enkele verwerkingsactiviteiten van het FEC deelnemen. Participanten schuiven alleen aan in de FEC-raad wanneer er sprake is van een onderwerp waar ze zich mee bezighouden. Het voorgestelde onderdeel h is opgenomen omdat er flexibiliteit nodig is en biedt de basis om bij of krachtens amvb ook de participanten aan te wijzen als deelnemer, voor daarbij te omschrijven specifieke verwerkingen of onderdelen daarvan. Er zijn momenteel vier participanten: de Koninklijke marechaussee, IND, AIVD en BFT (Bureau Financieel Toezicht). Voorgesteld wordt om de drie partners aan te wijzen in de amvb, bedoeld in onderdeel h, voor in die amvb te omschrijven specifieke verwerkingen of onderdelen daarvan.

Artikel 13 (verstrekking van gegevens aan het samenwerkingsverband)

Niet genoemd zijn de gegevens die worden verstrekt op grond van de Wpg of Wjsg, want die verstrekking geschiedt niet op grond van artikel 5, maar op grond van de voorgestelde wijzigingen van de Wpg of Wjsg, welke niet het vereiste kennen om in de WGS aan te wijzen welke categorieën gegevens moeten worden verstrekt.

Artikel 14 (activiteiten)

Het FEC voert binnen de kaders van de huidige wetgeving de volgende verwerkingsactiviteiten uit:

- Signalenoverleg t.b.v. "FEC-regulier"
- Signalenoverleg en Gegevensanalyse t.b.v. Programma Terrorismefinanciering
- Signalenoverleg t.b.v. Taskforce Terrorismefinanciering
- Signalenoverleg t.b.v. Taskforce Serious Crime.

Er zijn geen verwerkingsactiviteiten die het FEC onder de WGS niet meer zou kunnen uitvoeren. Met de zgn. non-regressiebepaling die in het wetsvoorstel is opgenomen (artikel 2, tweede lid), wordt ook in juridische zin verankerd dat de bestaande verwerkingsactiviteiten die op bilaterale leest zijn geschoeid, onverkort in stand kunnen blijven.
Nieuw is de mogelijkheid om voortaan ook t.b.v. "FEC-regulier" gegevensanalyses uit te voeren.

Artikel 15 (signalenoverleg)

Als er sprake is van een complex probleem, dan gaan de deelnemers over tot signalenoverleg. Het proces begint met een signaal van een probleem (zie de definitie van signaal in artikel 1 van het wetsvoorstel).
Nadat een signaal is ingebracht door een van de partners gaan de overige partners na of zij over relevante informatie beschikken om het in het signaal beschreven probleem nader te analyseren. Die informatie wordt op beveiligde wijze met elkaar gedeeld en door de partners geanalyseerd op bruikbaarheid. Daarna kan één van de partners hulp vragen of kan de partner aangeven het signaal zelf niet te kunnen gebruiken en eventueel dat het voor een andere deelnemer van het FEC relevant lijkt.
Periodiek worden alle lopende signalen met elkaar besproken in het signalenoverleg, waaraan vaste personen per deelnemer deelnemen. In het signalenoverleg wordt besproken of alle relevante informatie gedeeld is, of deze informatie vragen oplevert, wat de informatie aan nieuwe inzichten heeft opgeleverd en of er en zo ja, welke interventiemogelijkheden bestaan. Waar mogelijk en passend vindt onderlinge afstemming plaats over te ondernemen interventies. Als een signaal complex of omvangrijk is, leent het periodieke signalenoverleg zich niet voor een goede inhoudelijke bespreking van het signaal. In dat geval kan een extra signalenoverleg (dit wordt binnen het FEC een dataroom genoemd) specifiek voor dat signaal georganiseerd worden. In dat signalenoverleg vinden dezelfde activiteiten plaats als in het periodieke signalenoverleg, alleen is meer tijd beschikbaar voor behandeling van een signaal. Naast de vaste personen die ook aan het periodieke signalenoverleg deelnemen, kunnen ook inhoudelijk experts van de partners deelnemen.

Artikel 16 (gegevensanalyse)

Dit artikel heeft geen betrekking op profilering. Profiling is in het geval van FEC niet nodig. Het FEC doet dit nu ook niet en de noodzaak daarvan is niet gebleken. Er wordt geen gebruik gemaakt van algoritmes. Alles wordt per subject bekeken. Er worden ook in deze situatie geen personen met groepskenmerken verbonden. De groepskenmerken worden apart bekeken en worden niet gebruikt om een persoon in kaart te brengen.
Binnen het FEC beschikt alleen het Programma FEC-TF (specifiek op het thema terrorismefinanciering) over een team van analisten die de in het kader van dit programma aan het samenwerkingsverband verstrekte gegevens verder verwerken (onder meer ordenen, rangschikken, verrijken, analyseren en registreren in een signalendatabase). Bij analyse moet gedacht worden aan netwerkanalyse, inkomens- en vermogensanalyse, SWOT[31], SNA (sociale netwerk analyse), etc. Bij de analyse wordt gebruik gemaakt van analysetools waarmee grotere hoeveelheden vooral relationele informatie visueel doorzocht kunnen worden. Hierbij wordt geen gebruik gemaakt van

[31] SWOT staat voor Strengths, Weaknesses, Opportunities en Threats (sterktes, zwaktes, kansen en bedreigingen). Een SWOT-analyse is een hulpmiddel dat intern de sterktes en zwaktes en in de omgeving de kansen en bedreigingen analyseert en overzichtelijk weergeeft; op basis hiervan wordt vervolgens de strategie bepaald.

profilering. De informatie wordt verder uitgewerkt tot informatieproducten zoals rapportages en interventiemogelijkheden.

Artikel 17 (verstrekking van het resultaat)

Voor de definitie van sturingsinformatie wordt verwezen naar artikel 1.

Paragraaf 2.2 Infobox Crimineel en Onverklaarbaar Vermogen (iCOV)

Artikel 21 (doel)

De omschrijving van het doel komt overeen met het huidige doel van iCOV.
Met het oog op het in kaart brengen van onverklaarbaar of crimineel vermogen, het bestrijden van witwas- of fraudeconstructies, het kunnen innen van overheidsvorderingen die oninbaar dreigen te worden en het uitoefenen van toezicht op de goede werking van de markt, verwerkt iCOV in opdracht van een of meer deelnemers gegevens voor zover dat noodzakelijk is voor de uitoefening van publiekrechtelijke taken en bevoegdheden van de deelnemers. Het overkoepelende doel is dat geld terugvloeit naar de plek waar het werkelijk hoort: de maatschappij.

Het doel van iCOV dient een zwaarwegend algemeen belang, te weten het voorkomen van wanordelijkheden en strafbare feiten als bedoeld in artikel 8, tweede lid, EVRM. Dat belang is gediend met de activiteiten van iCOV. Er zijn veel aanwijzingen dat een substantieel deel van de financiële geldstromen in of via Nederland crimineel of onverklaarbaar zijn en dat daarmee zwaarwegende maatschappelijke, financiële en economische belangen worden geschaad. Witwassen betreft een ernstig strafbaar feit. Het gebruik van crimineel verkregen vermogen stimuleert het begaan van strafbare feiten voor geldelijk gewin, en de omloop van crimineel verkregen vermogen ondermijnt en ontwricht het financieel stelsel. Ook fraudeconstructies betreffen ernstige strafbare feiten. Deze staan veelal niet op zichzelf en vormen een middel om inkomsten uit andere illegale activiteiten te verhullen of om het plegen van andere vormen van fraude mogelijk te maken.
Een goede informatiepositie is daarbij noodzakelijk om van daaruit ten behoeve van opsporing, toezicht en handhaving, alsmede de daaraan verbonden incassotaken, overheidsbreed keuzes op maat te kunnen maken (integrale aanpak). Met een goede informatiepositie kan beter gestuurd worden op het afpakken van crimineel vermogen, opdat misbruik en misdaad niet lonen. De deelnemers van iCOV hebben gezamenlijk beter zicht op crimineel of onverklaarbaar vermogen. Ten behoeve van een goede informatiepositie over criminele of onverklaarbare vermogens is het noodzakelijk om door samenwerking op een effectieve en efficiënte manier een integraal beeld over de vermogenspositie van (groepen) personen samen te stellen om zo toezicht, handhaving en incasso te verbeteren.
De analyses van iCOV leiden tot verschillende typen rapportages die in het bijzonder inzicht geven in onverklaarbaar of crimineel vermogen, witwassen en fraudeconstructies. Door goede analyse en combinatie van verschillende data - zowel binnen een individuele organisatie als tussen overheidspartijen - kunnen kwetsbaarheden omtrent fraude tijdig zichtbaar worden gemaakt en kan bloot worden gelegd dat een bepaalde frauduleuze handeling vaak onderdeel is van een breder handelingspatroon.
Aan de hand van de rapportages van iCOV kunnen organisaties die zijn belast met de opsporing van strafbare feiten of toezicht op de naleving van wettelijke voorschriften, gerichter optreden en efficiënter en effectiever hun middelen inzetten. Met behulp van de analyses van iCOV kunnen bovendien interventiestrategieën worden ontwikkeld om ondermijnende criminaliteit beter te herkennen en te bestrijden. Aan de hand van het resultaat van het onderzoek kan bijvoorbeeld gerichter worden geïntervenieerd tegen netwerken die witwasdiensten aanbieden.

Het doel van iCOV dient subsidiair, voor zover het doel van iCOV is gericht op het uitoefenen van toezicht op de goede werking van de markt, het belang van het "handhaven van het economisch welzijn van het land" als bedoeld in artikel 8, tweede lid,

EVRM. Dit belang is gediend met gezamenlijke gegevensverwerking door de Belastingdienst (waarvan de missie een financieel gezond Nederland inhoudt), door DNB (dat gericht is op een stabiel financieel stelsel) en door ACM (dat als missie heeft om bij te dragen aan een gezonde economie door markten goed te laten werken).

Artikel 22 (deelnemers)

De lijst van deelnemers komt overeen met de huidige deelnemers van iCOV. Omwille van de flexibiliteit is aanvulling bij of krachtens amvb mogelijk van overheidsinstanties en overheidsorganen die belast zijn met toezicht op de naleving, opsporing of de inning van overheidsvorderingen.

Artikel 23 (door deelnemers te verstrekken gegevens)

De opsomming van door deelnemers te verstrekken gegevens komt in hoge mate overeen met de op dit moment door deelnemers te verstrekken gegevens op basis van de protocollen voor gegevensverwerking (Stcrt. 2019, 11303 en Stcrt. 2019, 11305).
Niet genoemd zijn in het voorgestelde artikel de gegevens die worden verstrekt op grond van de Wpg of Wjsg, want die verstrekking geschiedt niet op grond van artikel 5, maar op grond van de voorgestelde wijzigingen van de Wpg of Wjsg, welke niet het vereiste kennen om in de WGS aan te wijzen welke categorieën gegevens moeten worden verstrekt.

Het verstrekken van de gevraagde categorieën gegevens is naar ons oordeel proportioneel en subsidiair. Hoewel het voorgestelde artikel de te verstrekken categorieën gegevens noemt, laat dat onverlet dat de leverende deelnemers zelf bepalen welke gegevens, vergaard vanuit de eigen taakstelling, concreet noodzakelijk zijn om beschikbaar te stellen, zodat er een goede invulling gegeven kan worden aan de doelstelling van iCOV.

Deze toets op proportionaliteit en subsidiariteit van de levering van gegevens ziet er bij iCOV als volgt uit. Elke gegevenslevering bij iCOV wordt voorafgegaan door een zogenaamde proeflevering nadat door de leverende deelnemer is besloten dat bepaalde informatie relevant is voor het doel van het iCOV samenwerkingsverband. Deze proeflevering heeft tot doel om de kwaliteit van de data te laten beoordelen door experts van iCOV en om vast te kunnen stellen of de data geschikt en passend zijn om opgenomen te worden in een informatieproduct van iCOV. Indien blijkt dat de data van onvoldoende kwaliteit zijn, zal geconcludeerd moeten worden dat de gegevens niet geschikt zijn om te gebruiken voor de totstandkoming van de informatieproducten. De gegevens waarvoor een proeflevering heeft plaatsgevonden, zullen in dat geval dan ook verwijderd worden. Indien de experts van iCOV daarentegen oordelen dat de data geschikt zijn om opgenomen te worden in een informatieproduct van iCOV, leggen zij deze bevinding voor aan de leden van de rechtmatigheidsadviescommissie. Zij adviseren vervolgens aan het samenwerkingsverband over de vraag of het acceptabel is dat de data daadwerkelijk opgenomen kunnen worden in een informatieproduct van iCOV. Hierbij houdt de rechtmatigheidsadviescommissie rekening met de proportionaliteit, subsidiariteit en doorkruising van het opsporingsbelang. Bij een positief advies worden de data geleverd naar een beveiligde omgeving. Bij een negatief advies worden de data verwijderd uit de productieomgeving en wordt de leverende organisatie op de hoogte gesteld van het feit dat de data ongeschikt zijn om kwalitatief hoogwaardige producten te kunnen vervaardigen.

Uit de genoemde categorieën gegevens kan een beter beeld worden verkregen van structuren rond ondermijnende criminaliteit, zoals de kenmerken van de groep personen, bedrijven en stichtingen die betrokken zijn bij ondermijnende criminaliteit. Daarnaast kunnen uit die gegevens niet eerder geïdentificeerde op crimineel geld gebaseerde relaties in beeld worden gebracht. Er is op voorhand een veelheid aan persoonsgegevens noodzakelijk om een representatieve en valide thematische benadering van een problematiek samen te stellen. Immers door een representatieve groep te onderzoeken

op een specifiek fenomeen kunnen afwijkingen zichtbaar worden die van belang zijn voor opsporing, handhaving, inning, executie, toezicht of bestuursrechtelijke maatregelen.

Er bestaan redelijkerwijs geen alternatieve informatiebronnen waaruit deze gegevens kunnen worden afgeleid die een lichtere inbreuk zouden maken op de persoonlijke levenssfeer. Het doel van het beoogde onderzoek kan niet worden bereikt door het verstrekken van minder gegevens over als verdacht aangemerkte transacties. Minder gegevens zijn onvoldoende representatief en kunnen een vertekend en onbetrouwbaar beeld geven. Daarvoor is van belang dat witwasstromen kunnen veranderen.

De gegevens betreffen veel personen, maar daartegenover staat dat door de wijze waarop het onderzoek is vormgegeven de persoonlijke levenssfeer van betrokkenen niet onevenredig wordt geschaad.

Artikel 24 (activiteiten)

Dit artikel beschrijft de vier typen rapportages die iCOV opstelt voor de deelnemers. Voor de operationele doeleinden (productie genoemd) kan iCOV vier standaardrapportages vervaardigen. Deze rapportages bevatten sturingsinformatie: (financiële) informatie bezien in onderling verband.

Het gaat om vier soorten rapportages:

De iCOV Rapportage Vermogen en Inkomen (iRVI)
Dit is een financieel paspoort van een persoon of bedrijf. Voor een uitgebreide toelichting wordt verwezen naar paragraaf 4.2 van het algemeen deel. Een voorbeeld, om toe te lichten wat dit concreet betekent: de Belastingdienst controleert de btw-aangifte van een ondernemer die in 2018 is begonnen met zijn zaak. In het laatste kwartaal noteert hij plots een omzet van enkele miljoenen. Uit de eigen Belastingdienstsystemen blijken echter geen inkomsten. In een rapportage van iCOV blijkt dat de betrokkene woont op een adres dat toebehoort aan een persoon die vele geplofte bv's op naam heeft staan. De overgebleven belastingschuld is nooit terugbetaald omdat er ogenschijnlijk geen vermogen meer aanwezig was. De schade voor de samenleving bestaat in dit voorbeeld uit miljoenen euro's. Het resultaat is in deze zaak dat de zaak aan de FIOD kan worden overgedragen door middel van sturingsinformatie.

De iCOV Rapportage Relaties (iRR):
Dit is een overzicht van de financiële en zakelijke relaties van een persoon of bedrijf of tussen personen of bedrijven. Een voorbeeld: de politie is een familie op het spoor die betrokken lijkt bij de handel in synthetische drugs. De familie heeft grote auto's, een groot huis en winkelt bij de duurste zaken. Ogenschijnlijk zijn er geen legale inkomsten, in de vorm van een baan of bezit van een bedrijf. De vraag is ook waar het geld gestald is. Het politieteam dat onderzoek doet, vraagt een rapportage aan bij iCOV. De officier van justitie geeft daarvoor schriftelijke toestemming. Uit de rapportage van iCOV blijkt dat de familie gebruikmaakt van een bankrekening van een lang geleden opgeheven BV. Een reguliere zoekslag via de Kamer van Koophandel had dat opgeheven bedrijf niet in het vizier gebracht. Dankzij de rapportage wordt niet alleen duidelijk hóe dat geld de legale economie instroomt, maar ook wat de werkwijze van de familie is. De geldstromen vertoonden namelijk connecties met landen die erom bekend staan dat ze verhullende constructies mogelijk maken. Het verhullen van de herkomst van geld is een van de eerste stappen bij witwassen.

De iCOV Rapportage Thema (iRT):
Deze zogenoemde 'themascan' geeft bijvoorbeeld inzicht in de risico's op witwassen via vastgoed in een bepaald geografisch gebied. Het kan hierbij gaan om geldstromen rondom vastgoed in een bepaald geografisch gebied. Te denken valt aan een aanpak waarbij kennis over witwassen en ondermijning wordt gecombineerd met onderzoek aan de hand van data. Dit biedt opvallende inzichten in de verschillende facetten van de problematiek in het specifieke gebied en daarmee direct handvatten om deze aan te pakken.

De iCOV Rapportage Thema compact (iRT compact):
Deze rapportage is reeds toegelicht in paragraaf 4.2.

Rapportages alleen op verzoek
Zoals de aanhef van het artikel beschrijft, gaat aan de rapportage altijd vooraf een verzoek van één of meer deelnemers. Dat past bij het uitgangspunt dat iCOV slechts in opdracht van zijn deelnemers gegevens verwerkt. Dit betekent dat iCOV alleen een rapportage kan opstellen als zij hiervoor een rechtsgeldig verzoek heeft ontvangen dat in relatie staat tot het doel van het samenwerkingsverband én de bijhorende taak van de verzoekende deelnemer, zoals omschreven in artikel 22. Het verzoek tot een rapportage moet een verantwoording geven met het oog op welke publiekrechtelijke taak de deelnemer een rapportage vraagt.

De rapportages die door iCOV gegenereerd worden, vergen altijd een menselijke beoordeling en een toetsing bij de authentieke bron. Artikel 8a, tweede lid, voorziet hierin.

Wetenschap en Innovatie
Naast de rapportages is er binnen iCOV ook een tak Innovatie en Wetenschap, zoals nader is toegelicht in paragraaf 4.2 van de memorie van toelichting. Zoals aldaar is toegelicht vinden de verwerkingen in het kader van wetenschap en innovatie plaats onder het regime van de artikelen 89 AVG, 22 Wpg en 39g juncto 15 Wjsg.

Artikel 25 (delegatiegrondslag)
Dit artikel dient als delegatiegrondslag om een aantal specifieke waarborgen bij of krachtens amvb te regelen.

Artikel 26 (verstrekking van het resultaat)

Eerste lid
Nadat een rapportage is vervaardigd, wordt deze via een beveiligde omgeving beschikbaar gesteld voor de aanvrager. Zodra de aanvrager het product in ontvangst heeft genomen, valt dit product onder het wettelijk regime van de deelnemende partij en daarmee ook niet meer onder de gezamenlijke verwerkingsverantwoordelijkheid van het samenwerkingsverband. Hiermee gaat dus de verwerkingsverantwoordelijkheid over naar de aanvragende/ontvangende deelnemer van het samenwerkingsverband. De aanvrager heeft met dit product sturingsinformatie ontvangen, waarmee hij kan bepalen hoe hij de zaak opvolgt. Voor de definitie van sturingsinformatie wordt verwezen naar artikel 1.

De sturingsinformatie geeft de aanvrager de mogelijkheid om capaciteit in te zetten voor bijvoorbeeld verder onderzoek en interventiebepaling. De informatie dient nader geanalyseerd te worden: de informatie kan op zichzelf geen vergaande conclusies voor personen opleveren gezien het feit dat iCOV niet over eventuele aanvullende relevante informatie of bevoegdheden beschikt om verdere validatie mogelijk te maken. Vanaf het moment van levering dient dit onderzoek te worden vervolgd door de aanvragende/ ontvangende organisatie.
Op de deelnemer die het resultaat ontvangt, rust volgens artikel 9, tweede lid, van dit wetsvoorstel een geheimhoudingsplicht, behoudens voor zover enig wettelijk voorschrift voorziet in de bevoegdheid of verplichting om de gegevens te verstrekken.

Tweede lid
Resultaten van iCOV kunnen onder de voorwaarden van artikel 7, tweede lid, ook verstrekt worden aan derden. Het huidige juridische kader waarbinnen iCOV werkt, staat niet toe dat er informatie wordt gedeeld met derden. Terwijl dat juist noodzakelijk kan zijn om een integraal beeld van een casus of problematiek te verkrijgen.

Paragraaf 2.3 De regionale informatie- en expertisecentra

Artikel 30 (Aanwijzing)

Eerste lid

Door de aanwijzing van de regionale informatie- en expertisecentra als samenwerkingsverbanden in de zin van deze wet wordt geregeld dat de deelnemers aan de regionale expertisecentra ten behoeve van de uitoefening van hun bestaande wettelijke taken en bevoegdheden, gezamenlijk persoonsgegevens en andere relevante gegevens kunnen verwerken. Naast de algemene bepalingen van hoofdstuk 1, worden in deze paragraaf aanvullende regels gesteld over de gezamenlijke verwerking van persoonsgegevens en andere relevante gegevens in het kader van de regionale informatie- en expertisecentra.

De aanwijzing heeft uitsluitend betrekking op het mogelijk maken en reguleren van de gezamenlijke verwerking van persoonsgegevens en andere relevante gegevens in de bestaande samenwerking tussen deelnemers.

Duidelijkheidshalve wordt benadrukt dat de aanwijzing in de zin van deze bepaling nadrukkelijk niet tot gevolg heeft dat er een nieuwe overheidsorgaan, instantie of zelfstandige entiteit van enige vorm ontstaat, waarmee er eventueel nieuwe juridische verhoudingen zouden ontstaan tussen de deelnemers of ter zake van het samenwerkingsverband als zodanig. Aan het wetsvoorstel ligt het uitgangspunt ten grondslag dat de gezamenlijke verwerking van persoonsgegevens en andere relevante gegevens ten dienste staat aan de uitoefening van de bestaande wettelijke taken en bevoegdheden van de deelnemers. Er worden met de aanwijzing of enige andere bepaling in dit wetsvoorstel derhalve geen nieuwe taken of bevoegdheden aan de deelnemers of aan de samenwerkingsverbanden als zodanig toegekend. Voor zover dit wetsvoorstel regels bevat over de juridische verhoudingen tussen de deelnemers, hebben die uitsluitend betrekking op de nadere uitwerking van de eisen die de Algemene verordening gegevensbescherming stelt ter zake van de gezamenlijke verwerking, zoals de gezamenlijke verwerkingsverantwoordelijkheid.

Evenmin regelt dit wetsvoorstel de organisatie, inrichting, positionering en het beheer van de samenwerkingsverbanden. De regeling daarvan is voorbehouden aan de deelnemers. Een samenwerkingsverband vraagt om ondersteuning in de vorm van huisvesting, ICT-voorzieningen, ondersteuning en personeel. De deelnemers maken onderling afspraken over de wijze waarop het samenwerkingsverband wordt ingericht, taken stellen, prioriteiten vaststellen en zorgdragen voor financiering en beheer. Ook kan sprake zijn van mandaatverlening in de zin van afdeling 10.1.1 van de Algemene wet bestuursrecht.

Tweede lid

In artikel 30, tweede lid, is geregeld dat bij of krachtens algemene maatregel van bestuur regels kunnen worden gesteld over de territoriale werkgebieden van de regionale informatie- en expertisecentra. De regionale informatie- en expertisecentra zijn regionaal georganiseerd en omvatten elk een separaat territoriaal werkgebied. Omwille van de transparantie van de gezamenlijke gegevensverwerking in een specifieke regio, is het wenselijk deze regio's te duiden in de lagere regelgeving. Hiermee wordt namelijk duidelijkheid geboden aan de betrokkenen over wie gegevens worden verwerkt en tot welk RIEC zij zich kunnen wenden voor het uitoefen van hun rechten op grond van de AVG, bijvoorbeeld om geïnformeerd te worden.

Bij het bepalen van nadere regels over de territoriale werkgebieden, zal in beginsel worden aangesloten bij de regionale indeling zoals die op dat moment geldt op basis van afspraken tussen de deelnemers. Door de territoriale werkgebieden bij algemene maatregel van bestuur te bepalen, kan na de initiële vaststelling worden ingespeeld op regionale veranderingen in de toekomst, bijvoorbeeld als het werkgebied van een RIEC aangepast moet worden in verband met gemeentelijke herindeling. Ook kan het zijn dat

de RIEC's op grond van regionale omstandigheden zelf komen tot voorstellen voor een andere territoriale indeling.

Artikel 31 (doel)

In artikel 31 is het doel bepaald met het oog waarop de deelnemers aan de RIEC's gezamenlijk gegevens verwerken. Het oogmerk van de samenwerking tussen de deelnemers is de gezamenlijke aanpak van georganiseerde criminaliteit. Het verbeteren van de informatiepositie van de afzonderlijke partners en het op elkaar afstemmen van eventuele interventies en handhavingsmaatregelen maakt mogelijk dat iedere afzonderlijke deelnemer de eigen wettelijke taken en bevoegden optimaal kan toepassen, zo mogelijk in samenhang met de interventies en handhavingsmaatregelen van andere partners. Het doel dat met de samenwerking tussen deze partijen wordt gediend, betreft het gezamenlijk invulling geven aan:

- Een bestuurlijke en geïntegreerde aanpak van de georganiseerde criminaliteit door naast het strafrechtelijk laten vervolgen van individuele betrokkenen en het ontmantelen van criminele samenwerkingsverbanden ook bestuursrechtelijke interventies en fiscale handhaving aan te wenden om de georganiseerde criminaliteit te bestrijden;
- Het identificeren van gelegenheidsstructuren binnen die economische sectoren en publieke voorzieningen die vatbaar zijn voor beïnvloeding door de georganiseerde criminaliteit opdat, middels het treffen van maatregelen ter bescherming, wordt voorkomen dat criminelen of criminele organisaties bewust of onbewust worden gefaciliteerd door de overheden en daardoor de democratische rechtsstaat wordt ondermijnd.

Om een nadere focus aan te brengen binnen de deze doelen is een aantal verschijningsvormen benoemd waar de samenwerkende partners specifiek aandacht aan besteden. Het betreft op dit moment:

- Mensenhandel en –smokkel,
- Georganiseerde hennepteelt,
- Fraude in de vastgoedsector,
- Misbruik binnen de vastgoedsector,
- Witwassen en daaraan gerelateerde vormen van financieel-economische criminaliteit,
- Verschijningsvormen van georganiseerde criminaliteit zoals die door de minister van Justitie en Veiligheid worden benoemd op basis van het 4-jaarlijks door de minister van Justitie en Veiligheid vast te stellen Nationaal Dreigingsbeeld,
- Door iedere Stuurgroep RIEC te bepalen verschijningsvormen van georganiseerde criminaliteit en de bestrijding van handhavingsknelpunten.

Daarnaast wordt vanuit het RIEC-samenwerkingsverband ondersteuning geboden aan bestuursorganen bij de toepassing van de Wet Bibob. Dat vindt plaats op grond van en binnen de kaders van art. 28, tweede lid, sub d, van de Wet Bibob.

Het doel waarvoor regionale informatie- en expertisecentra persoonsgegevens kunnen uitwisselen is gekoppeld aan de uitoefening van de bestaande wettelijke taken en bevoegdheden van de deelnemers. Hiermee wordt uitvoering gegeven aan de verplichting uit de artikelen 5, 6, eerste lid, onderdeel e, in samenhang bezien met het derde en vierde lid, van de Algemene verordening gegevensbescherming. Artikel 5, onderdelen a en b, van de AVG bepaalt dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is, alsmede voor welbepaalde uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden

verzameld en niet verder mogen worden verwerkt op een met die doeleinden onverenigbare wijze.

Artikel 6, eerste lid, onderdeel e, van de AVG bepaalt dat de verwerking van persoonsgegevens alleen rechtmatig is indien de verwerking noodzakelijk is voor een taak van algemeen belang of van een taak in het kader van de uitoefening van openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Artikel 6, derde lid, onderdeel b, van de AVG bepaalt dat de rechtsgrond moet worden vastgesteld bij lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is. Het doel van de verwerking moet bij de rechtsgrond worden vastgesteld of is noodzakelijk voor de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend. Het lidstatelijke recht moet beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde gerechtvaardigde doel.

De grondslagen voor gezamenlijke verwerking van persoonsgegevens bij of krachtens de WGS zijn gericht op een doel van zwaarwegend algemeen belang dat niet op voorhand verenigbaar is met de doelen waarvoor de deelnemers de te verstrekken gegevens hebben verzameld. Artikel 6, vierde lid, aanhef, AVG staat ook verdere verwerking voor een niet-verenigbaar doel toe, mits wettelijk geregeld en in het kader van een zwaarwegend algemeen belang. Het wetsvoorstel beoogt zo'n grondslag te bieden. Het lidstatelijk recht moet dan wel één van de belangen van artikel 23, eerste lid, AVG beschermen. Dat is hier het geval, zoals toegelicht aan het slot van paragraaf 3.3.1 van het algemeen deel van de memorie van toelichting. De RIEC's hebben tot doel het verwerken van gegevens, voor zover dat noodzakelijk is voor de uitoefening van de wettelijke taken en bevoegdheden van de deelnemers op het terrein van strafrechtelijke, bestuursrechtelijke en fiscaalrechtelijke handhaving in het belang van de bestrijding van georganiseerde criminaliteit. Het doel van de RIEC's en de regulering van de gezamenlijke gegevensverwerking voor dat doel in dit wetsvoorstel, vormt daarmee een noodzakelijke en evenredige maatregel als bedoeld in de artikel 23, eerste lid, onderdelen a, c en d, van de AVG, ter waarborging van de nationale veiligheid, de openbare veiligheid en de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

De regionale informatie- en expertisecentra verwerken uitsluitend gegevens voor zover dat noodzakelijk is voor de uitoefening van de wettelijke taken en bevoegdheden van de deelnemers op het terrein van strafrechtelijke, bestuursrechtelijke en fiscaalrechtelijke handhaving in het belang van de bestrijding van georganiseerde criminaliteit. Uit de bestaande wettelijke taken en bevoegdheden van de deelnemers vloeit reeds voort dat de verwerking van persoonsgegevens en andere relevante gegevens voor de uitoefening daarvan noodzakelijk is. Deze bepaling bouwt daarop voort door de informatiepositie van afzonderlijke deelnemers in aanvulling daarop te versterken door de mogelijkheid te creëren om onder voorwaarden persoonsgegevens en andere relevante gegevens met andere relevante deelnemers uit te wisselen en in gezamenlijkheid te verwerken. Het wetsvoorstel creëert immers geen nieuwe taken en bevoegdheden voor de deelnemers of de samenwerkingsverbanden als zodanig. Doordat de verwerking altijd noodzakelijk moet zijn voor de uitoefening van hun bestaande wettelijke taken en bevoegdheden, zijn het doel en de grenzen daarvan, duidelijk afgebakend, welbepaald en uitdrukkelijk omschreven. Gelet op het feit dat de gezamenlijke gegevensverwerking uitsluitend is toegestaan in het belang van het zwaarwegend algemeen belang van het bestrijden van georganiseerde criminaliteit, is sprake van een gerechtvaardigd belang.

Bij toepassing van alle bevoegdheden tot persoonsgegevensverwerking die de deelnemers krijgen op grond van dit wetsvoorstel, moet telkens worden getoetst of de persoonsgegevensverwerking noodzakelijk is het met oog op het doel van artikel 30. Elke separate persoonsgegevensverwerking moet daarnaast voldoen aan de rechtmatigheidseisen van de AVG. Het is aan elk RIEC zelf om een zorgvuldige procedure in te richten voor het gezamenlijk verwerken van gegevens, waarmee invulling gegeven wordt aan de beginselen van noodzaak, proportionaliteit en subsidiariteit uit de AVG.

Artikel 31a (activiteiten)

Eerste lid

In artikel 31a, eerste lid, wordt geregeld welke drie activiteiten de regionale informatie- en expertisecentra verrichten met het oog op het doel dat is omschreven in artikel 31 en waartoe zij gezamenlijk gegevens verwerken. De grondslag voor de verwerking van gegevens in het kader van deze activiteiten is opgenomen in artikel 36. Het gaat om de volgende activiteiten.

Onderdeel a: het aanwijzen en analyseren van handhavingsknelpunten

Het RIEC is erop gericht om de georganiseerde en ondermijnende criminaliteit aan te pakken en te voorkomen, de toepassing van de integriteitsbeoordelingen door het openbaar bestuur te bevorderen en handhavingsknelpunten te bestrijden. In artikel 1 van dit wetsvoorstel is een handhavingsknelpunt als volgt gedefinieerd: "door de deelnemers van een regionaal informatie- en expertisecentrum aangewezen personen, groepen van personen, economische sector, gebied of branches, waarover bij de deelnemers van het samenwerkingsverband dusdanige aanwijzingen zijn dat de vigerende wet- en regelgeving structureel niet wordt nageleefd, dat dit duidt op verschijningsvormen van georganiseerde criminaliteit". Alvorens de stuurgroep van een regionaal informatie- en expertisecentrum overgaat tot het aanwijzen van een handhavingsknelpunt dienen verschillende deelnemers aanwijzingen (schriftelijk vastgelegde feiten, omstandigheden en waarnemingen gedaan tijdens de uitoefening van hun respectievelijke wettelijke taken en bevoegdheden) te hebben, die erop duiden dat vigerende regelgeving structureel niet wordt nageleefd. Handhavingsknelpunten kunnen vanwege de regionale verscheidenheid per regionaal informatie- en expertisecentrum verschillend zijn. Afhankelijk van het aangewezen handhavingsknelpunt is het van belang vast te stellen of het knelpunt is ontstaan door een "handhavingstekort" of dat het knelpunt is ontstaan door onvoldoende zicht op de problematiek, gelet op onder andere de locatie, de doelgroep, het type overtredingen, de mate van non-compliance en de achterliggende maatschappelijke problematiek. De gezamenlijke gegevensverwerking in het kader van de analyse van een handhavingsknelpunt resulteert in een statistisch beeld, dat geen persoonsbeelden bevat, en een interventieadvies dat de betrokken deelnemers in staat stelt hun wettelijke taken en bevoegdheden uit te oefenen of kan resulteren in het inbrengen van de casus in het casusoverleg.

Onderdeel b: het voeren van casusoverleggen

De regionale informatie- en expertisecentra voeren met het oog op het doel van artikel 31 casusoverleggen ten behoeve van het bepalen en uitvoeren van gezamenlijke strategieën voor de uitvoering van de wettelijke taken en de inzet van hun wettelijke bevoegdheden door de deelnemers. De aanleiding voor het voeren van een casusoverleg kan zijn gelegen in een signaal dat één of meer deelnemers inbrengt of inbrengen in het regionale informatie- en expertisecentrum of opschaling vanuit de activiteiten van het aanwijzen en analyseren van handhavingsknelpunten of het verrichten van een gebiedscan of thematische scan. Signalen kunnen alleen door de betreffende deelnemer of deelnemers bij de regionale informatie- en expertisecentra worden ingediend wanneer het signaal betrekking heeft op feiten en omstandigheden die naar voren zijn gekomen naar aanleiding van waarnemingen die zijn gedaan tijdens de uitoefening van hun respectievelijke wettelijke taken en bevoegdheden, en die erop duiden dat vigerende regelgeving structureel niet wordt nageleefd. Het casusoverleg gebeurt met ondersteuning van het bureau van een regionaal informatie- en expertisecentrum in de vorm van een informatieoverleg waaraan betrokken deelnemers deelnemen of een thematische werkgroep. De gezamenlijke gegevensverwerking in het kader van het casusoverleg resulteert in een interventieadvies dat de betrokken deelnemers in staat stelt hun wettelijke taken en bevoegdheden uit te oefenen. Het advies wordt gebruikt om te bepalen of interventie noodzakelijk is, of interventie in afstemming tussen bepaalde deelnemers moet gebeuren en welke deelnemers betrokken moeten zijn alsmede welke

deelnemer verantwoordelijk is voor de te verrichten interventie of interventies of de coördinatie op zich neemt.

Onderdeel c: het verrichten van gebiedscans en thematische scans

De regionale informatie- en expertisecentra verrichten als activiteit gebiedscans en thematische scans ten behoeve van het bepalen en uitvoeren van gezamenlijke strategieën voor de uitvoering van de wettelijke taken en de inzet van hun wettelijke bevoegdheden door de deelnemers bij misstanden in maatschappelijke sectoren en publieke voorzieningen die vatbaar zijn voor innesteling van georganiseerde criminaliteit.

Aanleiding voor een gebiedscan of een thematische scan kan zijn een door het lokaal bestuur geselecteerd en benoemd gebied, branche of thema. De georganiseerde criminaliteit opereert over grenzen heen, maar wortelt en investeert vrijwel altijd lokaal. Het detecteren van signalen van criminele investeringen en activiteiten, waaronder verwevenheid met de bovenwereld, is vaak de eerste stap om zicht en inzicht te verkrijgen op of over georganiseerde criminaliteit. Criminelen gebruiken vaak onroerend goed voor het faciliteren van criminele activiteiten. Gelet hierop en met inachtneming van de beginselen van proportionaliteit en subsidiariteit is een zogenaamde gebiedscan of thematische scan een gepaste methodiek voor het detecteren van dit fenomeen. Het specifieke doel van een gebiedscan en een thematische scan is het signaleren van misstanden in de onroerend goed-sector en om deze signalen door samenwerking tussen deelnemende partijen bestuursrechtelijk aan te pakken. Het gaat daarbij om de integrale aanpak van transacties in onroerende zaken die zijn gefinancierd met vermogen dat met criminele activiteiten is verkregen en de aanpak van het gebruik van onroerende zaken voor witwassen van crimineel vermogen, het tegengaan van mensenhandel en –smokkel, georganiseerde hennepteelt en andere door de minister van Justitie en Veiligheid en de regionale stuurgroep RIEC te bepalen verschijningsvormen.
De gezamenlijke gegevensverwerking in het kader van het gebiedscan of thematische scan resulteert in een statistisch beeld, dat geen persoonsbeelden bevat, en een bestuurlijk interventieadvies dat de betrokken deelnemers in staat stelt hun wettelijke taken en bevoegdheden uit te oefenen. Ook kan een gebiedscan of thematische scan aanleiding geven tot het inbrengen van de casus in het casusoverleg.

Tweede lid

Het tweede lid bepaalt dat bij of krachtens algemene maatregel van bestuur nadere regels kunnen worden gesteld over de activiteiten, bedoeld in het eerste lid, en dat aanvullende activiteiten kunnen worden aangewezen, waaronder vormen van geautomatiseerde gegevensanalyse, zoals profilering, voor zover die noodzakelijk zijn voor het doel, bedoeld in artikel 31. De georganiseerde criminaliteit verandert constant en vindt voortdurend nieuwe manieren voor het plegen van misdaden. Het is daarom noodzakelijk dat de gezamenlijke verwerking van gegevens door de regionale informatie- en expertisecentra daarop geactualiseerd kan worden en er in de toekomst nieuwe activiteiten kunnen worden aangewezen. Deze bepaling strekt daartoe. Nieuwe activiteiten van de RIEC's die leiden tot een betere aanpak van de georganiseerde misdaad en waarvoor de deelnemers gezamenlijk gegevens moeten kunnen verwerken, moeten snel kunnen worden geïmplementeerd. Het bieden van een grondslag op het niveau van een algemene maatregel van bestuur of ministeriële regeling biedt die mogelijkheid.

Artikel 32 (deelnemers)

Eerste lid

In artikel 32, eerste lid, worden de deelnemers aan de regionale informatie- en expertisecentra aangewezen.

Iedere aan het RIEC-samenwerkingsverband deelnemende partij is een bestuursorgaan waaraan de uitvoering van een of meer wettelijke taken en bevoegdheden is opgedragen. Die zijn uiteenlopend; in de praktijk kan één bestuursorgaan meerdere bevoegdheden uitoefenen. Privaatrechtelijke rechtspersonen nemen op dit moment niet deel aan de regionale informatie- en expertisecentra.

Zoals hiervoor is aangegeven, is het doel waarvoor regionale informatie- en expertisecentra persoonsgegevens kunnen uitwisselen gekoppeld aan de uitoefening van de bestaande wettelijke taken en bevoegdheden van de deelnemers. Hiermee wordt uitvoering gegeven aan de verplichting uit de artikelen 5, 6, eerste lid, onderdeel e, in samenhang bezien met het derde en vierde lid, van de Algemene verordening gegevensbescherming. Bij de aanwijzing van de deelnemers wordt tevens bepaald met het oog op welke bestaande wettelijke taken en bevoegdheden zij gezamenlijk gegevens kunnen verwerken in het RIEC. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld over de wettelijke taken en bevoegdheden waarvoor door de deelnemers gegevens kunnen worden verwerkt binnen het RIEC. Dit betekent onder andere dat waar nodig een nadere concretisering kan plaatsvinden van de aangewezen wettelijke taken en bevoegdheden, dat deze bij wijziging van wetgeving daarop kunnen worden geactualiseerd en er zo nodig ook aanvullende wettelijke taken en bevoegdheden kunnen worden aangewezen waarvoor de deelnemers gegevens kunnen verwerken in het RIEC. Zoals opgemerkt verandert de georganiseerde criminaliteit voortdurend. Om die reden moet het mogelijk zijn ook de instrumenten voor de aanpak daarop te actualiseren.

Gelet op artikel 4, eerste lid, zijn de deelnemers gezamenlijke verwerkingsverantwoordelijken als bedoeld in artikel 26, eerste lid, van de Algemene verordening gegevensbescherming. Duidelijkheidshalve wordt opgemerkt dat de gezamenlijke verwerkingsverantwoordelijkheid als bedoeld in artikel 26 van de AVG betrekking heeft op de persoonsgegevensverwerking in het kader van het samenwerkingsverband. Elke deelnemer (of het bestuursorgaan waaronder de deelnemer ressorteert) blijft onverkort verwerkingsverantwoordelijke voor de persoonsgegevensverwerking die geschiedt bij de uitoefening van de wettelijke taken en bevoegdheden van die deelnemer. Dit wetsvoorstel brengt daarin geen wijzigingen aan.

De deelnemers die op grond van het eerste lid worden aangewezen zijn:

Onderdeel a: Immigratie en naturalisatiedienst

De Immigratie- en naturalisatiedienst (IND) neemt deel voor de uitvoering van de wettelijke taken en bevoegdheden op het terrein van toezicht en handhaving bij of krachtens de Vreemdelingenwet 2000 en de Rijkswet op het Nederlanderschap. De IND is onderdeel van het Ministerie van Justitie en Veiligheid. De Staatssecretaris van Justitie en Veiligheid is verantwoordelijk voor de uitvoering van de Vreemdelingenwet 2000 en de Rijkswet op het Nederlanderschap. De IND is de uitvoeringsorganisatie die verantwoordelijk is voor de uitvoering van het vreemdelingenbeleid in Nederland. Dat houdt in dat de IND alle aanvragen beoordeelt van vreemdelingen die in Nederland willen verblijven of Nederlander willen worden. De IND levert als de toelatingsorganisatie van Nederland een bijdrage aan de aanpak van migratiecriminaliteit waaronder mensenhandel en -smokkel. Daartoe werkt de IND nauw samen met de andere deelnemers aan het RIEC en wisselt de IND gericht informatie uit. Informatie die beschikbaar komt binnen het RIEC kan een bijdrage leveren aan een effectievere aanpak van vormen van migratiecriminaliteit, bijvoorbeeld:
- het voorkomen van mensenhandel door het tijdig onderkennen van signalen;
- de bestrijding van fraude en misbruik in toelatingsprocedures; en
- samenwerking ter voorkoming en bestrijding van mensenhandel en -smokkel.

Dergelijk misbruik moet zoveel mogelijk worden voorkomen dan wel in een zo vroeg mogelijk stadium worden herkend, onderkend en tegengegaan.
De IND is voor de herkenning van de hiervoor beschreven situaties in belangrijke mate afhankelijk van informatie die aanwezig is bij de andere deelnemers. Deze informatie kan aanleiding geven tot de inzet van toezicht- en handhavingsbevoegdheden voor het

tegengaan van migratiecriminaliteit. De IND kan bijvoorbeeld op grond van artikel 55a van de Vreemdelingenwet 2000 een bestuurlijke boete opleggen bij overtreding van enkele bepalingen van de Vreemdelingenwet 2000 die zien op het referentschap in de zin van artikel 2a Vreemdelingenwet 2000. Verder kan de IND het erkend referentschap intrekken of schorsen. Ook kan de IND op grond van de Rijkswet op het Nederlanderschap in bepaalde gevallen overgaan tot het intrekken van het Nederlanderschap. Er kan ook worden overgaan tot intrekking van een verblijfsvergunning indien fraude in de toelatingsprocedure is aangetoond dan wel indien er strafbare feiten zijn gepleegd.

Onderdeel b: de rijksbelastingdienst

De rijksbelastingdienst, met in begrip van alle onderdelen daarvan, bedoeld in de op artikel 3 van de Algemene wet inzake rijksbelastingen gebaseerde ministeriële regeling, neemt deel voor het uitvoeren van de wettelijke taken en bevoegdheden bij of krachtens de belastingwet, genoemd in artikel 2, eerste lid, onderdeel a, van de Algemene wet inzake rijksbelastingen, de Invorderingswet 1990, de wettelijke taken en bevoegdheden bij of krachtens de Algemene douanewet en het Douanewetboek van de Unie, en hoofdstuk 2 van de Algemene wet inkomensafhankelijke regelingen.

In de Algemene wet inzake rijksbelastingen (AWR) en de Invorderingswet 1990 (Iw 1990) is een aantal bevoegdheden voor de rijksbelastingdienst opgenomen die kunnen worden toegepast om informatie bij belastingplichtigen, inhoudingsplichtigen en bij derden op te vragen en te gebruiken. Op deze manier kan de Belastingdienst de materiële en de formele belastingschuld vaststellen.
De douane is als onderdeel van de rijksbelastingdienst onder meer belast met de uitvoering van het Douanewetboek van de Unie (DWU), de Algemene douanewet (Adw) en de Algemene wet inzake rijksbelastingen (AWR). De douane voert hiertoe onder andere de volgende werkzaamheden uit: controles op goederen en aangiften, administratieve controle en klantmanagement. Tijdens de uitoefening van haar controletaken richt de douane zich naast haar fiscale taken op goederen die een bedreiging vormen voor veiligheid, gezondheid, economie en milieu (VGEM). Deze VGEM-taken richten zich op een groot spectrum van goederen zoals het illegaal in- en uitvoeren van verdovende middelen, wapens, ivoor, beschermde diersoorten, merk vervalste producten, strategische goederen, sigaretten, en afval. De douane werkt risicogericht en heeft daarbij oog voor risicogoederen, risicolanden, risicolocaties en risicozendingen. Behalve toezichthoudende bevoegdheden heeft de douane op grond van hoofdstuk 9 uit Adw ook bevoegdheid tot het opleggen van bestuurlijke boete en op grond van hoofdstuk 11 van de Adw ook opsporingsbevoegdheden.

De rijksbelastingdienst, onderdeel toeslagen, is op grond van artikel 11 van de Algemene wet inkomensafhankelijke regelingen (Awir) belast met het toekennen, uitbetalen en terugvorderen van tegemoetkomingen. Een tegemoetkoming is een financiële bijdrage van het Rijk op grond van een inkomensafhankelijke regeling. Er worden vier inkomensafhankelijke regelingen door de rijksbelastingdienst, onderdeel toeslagen, uitgevoerd: de huur-, zorg- en kinderopvangtoeslag en het kindgebonden budget, die hun wettelijke basis vinden in respectievelijk de Wet op de huurtoeslag, de Wet op de zorgtoeslag, de Wet kinderopvang en kwaliteitseisen peuterspeelzalen, en de Wet op het kindgebonden budget. De rijksbelastingdienst, onderdeel toeslagen, beschikt op grond van de artikelen 40 en 41 Awir over de mogelijkheid om voor bepaalde overtredingen bestuurlijke boetes op te leggen.
De verantwoordelijkheid voor de uitvoering van de inkomensafhankelijke regelingen ligt bij het ministerie van Financiën. De verantwoordelijkheid voor de inhoud van de inkomensafhankelijke regelingen, en de terbeschikkingstelling van het budget, ligt echter bij de zgn. beleidsdepartementen: het ministerie van BZK (huurtoeslag), het ministerie van VWS (zorgtoeslag), en het ministerie van SZW (kinderopvangtoeslag en kindgebonden budget). Aangezien de rijksbelastingdienst zich bezighoudt met de fiscaalrechtelijke handhaving en uit de praktijk blijkt dat in geval van georganiseerde criminaliteit er praktisch altijd sprake is van het verzwijgen van inkomsten bij de

rijksbelastingdienst en derhalve van belastingfraude, is het voor de rijksbelastingdienst van belang om als deelnemer aan de regionale informatie- en expertisecentra te worden aangewezen. In de regionale informatie- en expertisecentra wordt de relevante informatie bijeengebracht zodat de rijksbelastingdienst via het raadplegen en het voorbereiden met de andere deelnemers beslissingen kan nemen om wel of niet over te gaan tot het toepassen van fiscaalrechtelijke handhaving, zoals bijvoorbeeld het opleggen van een navorderingsaanslag dan wel een boete.

Onderdeel c: Fiscale inlichtingen- en opsporingsdienst

De Fiscale inlichtingen- en opsporingsdienst (FIOD) neemt deel voor de uitvoering van de wettelijke taken, bedoeld in artikel 3 van de Wet op de bijzondere opsporingsdiensten en de daaruit voortvloeiende bevoegdheden. De FIOD is de bijzondere opsporingsdienst van de rijksbelastingdienst. De FIOD werkt aan het bestrijden van fiscale, financieel-economische en goederenfraude, levert een bijdrage aan het waarborgen van de integriteit van het financiële stelsel en de bestrijding van de georganiseerde criminaliteit, in het bijzonder de financiële component daarvan.
De FIOD is een van de vier bijzondere opsporingsdiensten als bedoeld in artikel 2 van de Wet op de bijzondere opsporingsdiensten (Wet BOD). De FIOD is, op grond van artikel 3 Wet BOD, belast met:
a. de strafrechtelijke handhaving van de rechtsorde op de beleidsterreinen waarvoor de Minister van Financiën verantwoordelijkheid draagt;
b. de strafrechtelijke handhaving van de rechtsorde op een beleidsterrein waarvoor een andere minister dan de hiervoor bedoelde, verantwoordelijkheid draagt en die door die minister in overeenstemming met Onze betrokken Minister (van Financiën) en Onze Minister van Justitie aan die bijzondere opsporingsdienst is opgedragen;
c. opsporingshandelingen in verband met strafbare feiten die zijn geconstateerd in het kader van de taakuitoefening bedoeld onder a. en b., en die met die taakuitoefening verband houden;
d. de opsporing van andere strafbare feiten, indien de bijzondere opsporingsdienst daarmee is belast door de officier van justitie.
Vanuit zijn wettelijke taakstelling (artikel 3 Wet BOD) ziet de FIOD het belang om een bijdrage te leveren aan de integrale aanpak van georganiseerde criminaliteit. Daarbij gaat het met name om de strafrechtelijke handhaving en opsporing van die criminaliteit die onder het beleidsterrein van de FIOD valt.

Onderdeel d: Koninklijke marechaussee

De Koninklijke marechaussee (KMar) neemt deel voor de uitvoering van de wettelijke taken en bevoegdheden bij of krachtens artikel 4 van de Politiewet 2012. De politietaken van KMar zijn limitatief vastgelegd in artikel 4 van de Politiewet 2012. Een aanzienlijk onderdeel van deze taken vormt de uitvoering van de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken. Voor het doel van de regionale informatie- en expertisecentra zijn de volgende taken van de KMar relevant:
• de uitvoering van krachtens de Vreemdelingenwet 2000 opgedragen taken waaronder het mobiel toezicht veiligheid (Schengen binnengrenzen) en grenscontrole en grensbewaking aan de buitengrenzen;
• het voorkomen en bestrijden van illegale migratie, mensensmokkel, fraude met reis- en identiteitsdocumenten;
• de bestrijding van criminaliteit op, rond, en in relatie tot luchthavens en militaire terreinen;
• het verlenen van bijstand en samenwerking met de politie bij de bestrijding van de grensoverschrijdende criminaliteit;
• het verlenen van samenwerking en bijstand in het kader van de nationale veiligheid en terrorismebestrijding.
Vanuit haar wettelijke taakstelling en handhavings- en opsporingsprioriteiten, ziet de KMar het belang om bij te dragen aan de integrale aanpak van de georganiseerde criminaliteit. Daarbij gaat het met name om de taken die verband houden met

grenspassage en het tegengaan van mensensmokkel en -handel met als doel de daarbij behorende ketenaanpak te versterken en aan te vullen.

Onderdeel e: Uitvoeringsinstituut werknemersverzekeringen

Het Uitvoeringsinstituut werknemersverzekeringen (UWV), neemt deel voor de uitvoering van de wettelijke taken en bevoegdheden bij of krachtens hoofdstuk 5 van de Wet structuur uitvoeringsorganisatie werk en inkomen. Het UWV is een zelfstandig bestuursorgaan en verzorgt in opdracht van het ministerie van Sociale Zaken en Werkgelegenheid de uitvoering van werknemersverzekeringen (zoals WW, WIA (IVA en WGA), Wajong, WAO, WAZ, Wazo en Ziektewet), arbeidsmarkt- en gegevensdienstverlening. Binnen UWV is de directie Handhaving de eerstaangewezen afdeling als het gaat om het vaststellen van mogelijk misbruik van uitkeringen of subsidies, aangezien het UWV moet zorgen voor het verstrekken van rechtmatige uitkeringen. Hiertoe werkt het UWV samen met andere overheidsinstanties zoals de rijksbelastingdienst, de Inspectie SZW, de Sociale Verzekeringsbank, gemeenten, de politie en het openbaar ministerie, maar ook met private instellingen zoals verzekeraars. Handhaving is gericht op een effectieve aanpak van individuele vormen van fraude zoals zwartwerken naast een uitkering, naast het bestrijden van systeemfraudes zoals PGB-fraude, faillissementsfraude, schijnconstructies, hennepteelt naast een uitkering en dergelijke. Fraudezaken worden afgedaan door het opleggen van terugvorderingen en boetes, of het doen van aangifte bij het OM bij ernstige fraudes.

Onderdeel f: politie

De politie neemt deel voor de uitvoering van de taak bedoeld in artikel 3 van de Politiewet 2012.
De politie heeft op grond van artikel 3 van de Politiewet 2012 tot taak in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde (opsporing en openbare orde) en het verlenen van hulp aan hen die deze behoeven.
Het RIEC is erop gericht om de georganiseerde en ondermijnende criminaliteit aan te pakken en te voorkomen, de toepassing van de integriteitsbeoordelingen door het openbaar bestuur te bevorderen en handhavingsknelpunten te bestrijden. De bijdrage van de politie is erop gericht om voldoende informatie over een signaal te verkrijgen zodat gefundeerd een selectie kan worden gemaakt. Op basis van het verkregen inzicht in de (mogelijke) aard en omvang van de georganiseerde criminaliteit wordt een integraal interventieadvies geformuleerd. Met inachtneming van dit interventieadvies neemt de politie, na overleg en afstemming met de andere deelnemers een beslissing - wederom zo nodig in overleg met het OM - over het wel of niet overgaan tot een opsporingsonderzoek.
Ongeacht of een interventieadvies leidt tot een strafrechtelijke, bestuursrechtelijke, fiscale en/of privaatrechtelijke aanpak, vindt in de navolgende uitvoeringsfase – binnen de wettelijke mogelijkheden – een voortdurende informatie-uitwisseling plaats tussen de deelnemers met als doel het complementeren en actualiseren van de informatiepositie ten behoeve van de aanpak door de daartoe geëigende deelnemers. De voortgang van de gemaakte afspraken kunnen in het RIEC worden gevolgd. Deze redenen maken het voor de politie noodzakelijk om deel te nemen aan het RIEC.

Onderdeel g: openbaar ministerie

Het openbaar ministerie (OM) neemt deel voor de in artikel 124 van de Wet op de rechterlijke organisatie opgedragen taak. Het OM is op grond van artikel 124 van de Wet op de rechterlijke organisatie belast met de strafrechtelijke handhaving van de rechtsorde en andere bij wet opgedragen taken. Het OM heeft mede op grond van artikel 12 Politiewet 2012 het gezag over de opsporing van strafbare feiten en is verantwoordelijk voor het vervolgen daarvan, alsmede voor de tenuitvoerlegging van opgelegde straffen.
Het OM heeft op grond van artikel 148 Wetboek van Strafvordering (Sv) het gezag en de verantwoordelijkheid over de opsporing door de politie en de overige participerende opsporingsinstanties zoals FIOD en Inspectie SZW. In het RIEC wordt de relevante informatie bijeengebracht zodat het OM via het raadplegen en het voorbereiden met de andere deelnemers een beslissing kan nemen over het wel of niet overgaan tot het

starten van een opsporingsonderzoek en daarna uiteindelijk het instellen van strafrechtelijke vervolging.

Onderdeel h: Burgemeester

De burgemeester is op grond van artikel 172 van de Gemeentewet belast met de handhaving van de openbare orde en beschikt in dat verband over verschillende bevoegdheden die zijn opgenomen in hoofdstuk XI van titel III van de Gemeentewet., Het gaat hier onder andere om de bevoegdheden tot sluiten van inrichtingen en woningen (art. 174 en 174a Gemeentewet), het opleggen van gebiedsverboden (art. 172a) en het geven van bevelen ter handhaving van de openbare orde (art. 175 Gemeentewet). Daarnaast bevatten de door gemeenteraden vastgestelde Algemene Plaatselijke Verordening en andere verordeningen bevoegdheden ter handhaving van de openbare orde. Uit paragraaf 2.3 van de Politiewet 2012 volgt dat indien de politie in een gemeente optreedt ter handhaving van de openbare orde en ter uitvoering van de hulpverleningstaak, zij onder het gezag staat van de burgemeester. Op grond van artikel 13b van de Opiumwet is de burgemeester bevoegd drugspanden te sluiten.
De burgemeester heeft verder taken op het gebied van vergunningverlening, toezicht en handhaving ("VTH-taken") bij de uitvoering van verschillende taken en bevoegdheden die uit de uitvoering van verschillende wetten en gemeentelijke regels voortvloeien. Het gaat hierbij om VTH-taken ingevolge onder meer de Drank- en Horecawet en de Wet op de kansspelen.
De burgemeester heeft specifieke taken in de verstrekking van paspoorten en reisdocumenten (artikel 26 tot en met 28 van de Paspoortwet). Voornoemde wettelijke taken en bevoegdheden van de burgemeester zijn belangrijke instrumenten bij de aanpak van georganiseerde criminaliteit.

Onderdeel i: College van burgemeester en wethouders

Het college van burgemeester en wethouders neemt deel voor de uitvoering van zijn wettelijke taken en bevoegdheden bij of krachtens hoofdstuk X van titel III, van de Gemeentewet, titels I, Ia en VIb van de Wet op de kansspelen, artikelen 5, 10, 10b en 10c van de Wet bijzondere maatregelen grootstedelijke problematiek, Participatiewet, paragraaf 2.1 en de hoofdstukken 3 en 5 van de Wet algemene bepalingen omgevingsrecht, artikel 17 en hoofdstuk VI van de Woningwet, de artikelen 8, 21, 22, 25 en 26 en hoofdstuk 6 van de Huisvestingswet, artikel 3.38 van de Wet ruimtelijke ordening, een gemeentelijke verordening en artikel 1.4, eerste lid, van de Wet basisregistratie personen.

Onderdeel j: Provinciebestuur

Het provinciebestuur neemt deel voor de uitvoering van de wettelijke taken en bevoegdheden bij of krachtens de Provinciewet, de hoofdstukken 2, 3 en 5 van de Wet algemene bepalingen omgevingsrecht of een provinciale verordening;

In het licht van de VTH-taken van de provincie, zijn de bevoegdheden als in hoofdstukken 2, 3 en 5 van de Wet algemene bepalingen omgevingsrecht van belang. Het bevoegd gezag heeft tot taak zorg te dragen voor bestuursrechtelijke handhaving, waarvoor ook relevante gegevens worden verzameld en geregistreerd (art. 5.2, lid 1, sub b, Wet algemene bepalingen omgevingsrecht).
Tevens oefent het provinciebestuur diverse wettelijke taken en bevoegdheden uit op grond van de Provinciewet die bijdragen aan de aanpak van georganiseerde criminaliteit, zoals de verordenende bevoegdheid (art. 145 Provinciewet), het vaststellen van de milieuverordening in de zin van artikel 1.2 van de Wet milieubeheer) alsmede de bevoegdheid tot het overgaan tot bestuursdwang evenals het optreden tegen overtredingen.

Onderdeel k: de Inspectie Sociale Zaken en Werkgelegenheid

De Inspectie Sociale Zaken en Werkgelegenheid (SZW) neemt deel voor de uitvoering van de wettelijke taken, bedoeld in artikel 3 van de Wet op de bijzondere opsporingsdiensten en de daaruit voortvloeiende bevoegdheden alsmede voor de uitvoering van de wettelijke taken en bevoegdheden artikel 24 van de Arbeidsomstandighedenwet, artikel 8:1 van de Arbeidstijdenwet, de Warenwet, artikel 13 van de Wet allocatie arbeidskrachten door intermediairs, artikel 14 van de Wet arbeid vreemdelingen, de Wet gelijke behandeling van mannen en vrouwen, artikel 18a van de Wet minimumloon en minimumvakantiebijslag, de Wet op de loonvorming en artikel 5 van de Wet arbeidsvoorwaarden gedetacheerde werknemers in de Europese Unie. De Inspectie SZW bestaat uit toezicht i.c. de Directie Arbeidsmarktfraude, de Directie Arbeidsomstandigheden (Arbo) en de Directie Major Hazard Control (MHC) en uit de bijzondere opsporingsdienst: de Directie Opsporing. De Inspectie SZW is belast met de volgende taken:

- toezicht houden op de naleving van de Wet arbeid vreemdelingen, de Wet minimumloon en minimumvakantiebijslag en de Wet allocatie arbeidskrachten door intermediairs (ter bestrijding van illegale arbeid, ontduiking van het minimumloon, arbeidsuitbuiting, malafide arbeidsbemiddeling en andere vormen van arbeidsmarktfraude);
- toezicht houden op de naleving van de Arbeidsomstandighedenwet en de Arbeidstijdenwet (ter bevordering van veilige en gezonde werkomstandigheden en werk- en rusttijden voor werknemers);
- toezicht houden op de naleving van het Besluit risico´s zware ongevallen 1999 en de Aanvullende risico-inventarisatie en -evaluatie (ter beperking van de risico's voor werknemers en de omgeving van bedrijven die werken met grote hoeveelheden gevaarlijke stoffen);
- opsporen van fraude, uitbuiting en georganiseerde criminaliteit binnen de keten van werk en inkomen (arbeidsuitbuiting, mensensmokkel en grootschalige fraude op het gebied van de sociale zekerheid). Dit gebeurt onder aansturing van het Openbaar Ministerie;
- signaleren van ontwikkelingen en risico's op het werkveld van Sociale Zaken en Werkgelegenheid en deze melden aan belanghebbende partijen.

De Directie Opsporing van de Inspectie SZW is een van de vier bijzondere opsporingsdiensten als genoemd artikel 2, onder d, van de Wet op de bijzondere opsporingsdiensten (Wet BOD). Op grond van artikel 3 Wet BOD is de Directie Opsporing van de Inspectie SZW belast met:

a. de strafrechtelijke handhaving van de rechtsorde op de beleidsterreinen waarvoor de Minister van SZW verantwoordelijkheid draagt;
b. de strafrechtelijke handhaving van de rechtsorde op een beleidsterrein waarvoor een andere minister dan de hiervoor bedoelde, verantwoordelijkheid draagt en die door die minister in overeenstemming met Onze betrokken Minister (van SZW) en Onze Minister van Justitie aan die bijzondere opsporingsdienst is opgedragen;
c. opsporingshandelingen in verband met strafbare feiten die zijn geconstateerd;
d. in het kader van de taakuitoefening bedoeld onder a. en b., en die met die taakuitoefening verband houden;
e. de opsporing van andere strafbare feiten, indien de bijzondere opsporingsdienst daarmee is belast door de officier van justitie.

Vanuit zijn wettelijke taakstelling op grond van artikel 3 van de Wet op de bijzondere opsporingsdiensten ziet de Directie Opsporing het belang om een bijdrage te leveren aan de integrale aanpak van georganiseerde criminaliteit. Daarbij gaat het met name om de strafrechtelijke handhaving en opsporing van die criminaliteit die onder het beleidsterrein vallen van de Directie Opsporing van de Inspectie SZW. Voor wat betreft de overige directies geldt dat toezicht op de naleving en handhaving van voornoemde wetten van de onder de minister van SZW ressorterende wetten eveneens bijdraagt aan de aanpak van georganiseerde criminaliteit.

Onderdeel I: de Nederlandse Voedsel- en Warenautoriteit

De Nederlandse Voedsel- en Warenautoriteit (NVWA) neemt deel voor de uitvoering van de wettelijke taken, bedoeld in artikel 3 van de Wet op de bijzondere opsporingsdiensten en de daaruit voortvloeiende bevoegdheden. Een bijzondere opsporingsdienst is onder gezag van de officier van justitie belast met:

a. de strafrechtelijke handhaving van de rechtsorde op de beleidsterreinen waarvoor Onze betrokken Minister verantwoordelijkheid draagt;

b. de strafrechtelijke handhaving van de rechtsorde op een beleidsterrein waarvoor een andere minister dan de onder a. bedoelde, verantwoordelijkheid draagt en die door die minister in overeenstemming met Onze betrokken Minister en Onze Minister van Veiligheid en Justitie aan die bijzondere opsporingsdienst is opgedragen;
c. opsporingshandelingen in verband met strafbare feiten die zijn geconstateerd in het kader van de taakuitoefening bedoeld onder a. en b., en die met die taakuitoefening verband houden;
d. de opsporing van andere strafbare feiten, indien de bijzondere opsporingsdienst daarmee is belast door de officier van justitie.

Tweede lid

In het tweede lid wordt geregeld dat bij of krachtens algemene maatregel van bestuur nadere regels kunnen worden gesteld over de wettelijke taken en bevoegdheden waarvoor persoonsgegevens kunnen worden verwerkt binnen de regionale informatie- en expertisecentra. Zoals hiervoor is aangegeven volgt hier onder andere uit dat in de amvb waar nodig een nadere concretisering kan plaatsvinden van de aangewezen wettelijke taken en bevoegdheden, dat deze bij wijziging van wetgeving daarop kunnen worden geactualiseerd en er zo nodig ook aanvullende wettelijke taken en bevoegdheden kunnen worden aangewezen waartoe de deelnemers gegevens kunnen verwerken in het RIEC. Zoals opgemerkt verandert de georganiseerde criminaliteit voortdurend. Om die reden moet het mogelijk zijn ook de instrumenten voor de aanpak daarop te actualiseren.

Voor de reikwijdte van dit wetsvoorstel is bepalend dat de wettelijke taken en bevoegdheden waarvoor de deelnemers met het oog op doel, bedoeld in artikel 31, gezamenlijk gegevens kunnen verwerken, voldoende zijn afgebakend. De deelnemers zijn belast met een veelheid aan taken en bevoegdheden, die ook voortdurend aan wetswijziging onderhevig zijn. Om die reden acht de regering het noodzakelijk om de afbakening van wettelijke taken en bevoegdheden ook op een lager niveau van regelgeving te kunnen concretiseren en vast te stellen. Dat doet geen afbreuk aan het uitgangspunt van dit artikel dat de deelnemers uitsluitend gezamenlijk gegevens kunnen verwerken in het kader van de regionale informatie- en expertisecentra voor zover dat noodzakelijk is voor de uitoefening van hun bestaande wettelijke taken en bevoegdheden in belang van de bestrijding van georganiseerde criminaliteit.

Derde lid

In het derde lid wordt geregeld dat bij of krachtens algemene maatregel van bestuur andere overheidsorganen of overheidsinstanties of privaatrechtelijke rechtspersonen als deelnemer kunnen worden aangewezen, voor zover dat noodzakelijk is voor het doel, bedoeld in artikel 31, en het om daarbij beschreven specifieke verwerkingen of onderdelen daarvan gaat.
Op grond van artikel 7, tweede lid, in samenhang bezien met artikel 36, achtste lid, kunnen de resultaten van de verwerking aan een derde worden verstrekt. Daarbij kan het ook gaan om een private partij. Bij de verstrekking aan derden zal moeten worden voldaan aan de criteria die daarvoor op grond van de artikelen 7, tweede lid, gelden en die op grond van artikel 36, negende lid, bij of krachtens algemene maatregel van bestuur kunnen worden gesteld.

Artikel 33 (onderlinge gegevensuitwisseling)

Eerste lid

Artikel 33, eerste lid, maakt het mogelijk dat de deelnemers van de regionale informatie- en expertisecentra onderling gegevens kunnen uitwisselen voor zover dat noodzakelijk is voor het doel, bedoeld in artikel 31. Vanwege de regionale werkgebieden waarin onderscheidenlijke regionale informatie- en expertisecentra actief zijn, kan het voorkomen dat het ter zake van een betrokkene die in beeld is bij een regionaal informatie- en expertisecentrum nodig is om informatie uit te wisselen met een ander

regionaal informatie- en expertisecentrum, bijvoorbeeld omdat de verschijningsvorm van georganiseerde criminaliteit die in beeld is bij een van de regionale informatie- en expertisecentrum zich in meerdere regio's tegelijk manifesteert. Ook kan het voorkomen dat een betrokkene die onderwerp is van een casusoverleg en die in beeld is bij een regionaal informatie- en expertisecentrum in een bepaald werkgebied actief is of wordt in het werkgebied van een ander regionaal informatie- en expertisecentrum. Met het oog op de efficiëntie van het werk van de regionale- informatie- en expertisecentra moet het mogelijk zijn gegevens onderling uit te wisselen. Gelet op het overkoepelende doel van artikel 31 moet deze doorverstrekking beschouwd worden als vallend binnen dit doel. Zoals aangegeven moeten alle concrete verwerkingen van persoonsgegevens voldoen aan de rechtmatigheidseisen uit artikel 5 van de AVG. Het is aan de RIEC's zelf om een zorgvuldige procedure in te richten voor het onderling uitwisselen van gegevens, waarmee invulling gegeven wordt aan de beginselen van noodzaak, proportionaliteit en subsidiariteit uit de AVG.

Tweede lid

Indien toepassing wordt gegeven aan het eerste lid, geldt daarbij als waarborg voor de fundamentele belangen van betrokkene dat de verstrekking van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard aan een ander regionaal informatie- of expertisecentrum uitsluitend plaatsvindt nadat de deelnemer of deelnemers die deze persoonsgegevens aan het regionale informatie- of expertisecentrum heeft of hebben verstrekt, hiermee heeft of hebben ingestemd. Deze waarborg doet tevens recht aan de verantwoordelijkheid die elke deelnemer afzonderlijk heeft voor de rechtmatige verwerking van persoonsgegevens in het kader van de uitoefening van de taken en bevoegdheden van de deelnemer die deze gegevens verstrekt.

Artikel 34 (verwerking bijzondere categorieën van persoonsgegevens en identificatienummers)

Eerste lid

Gelet op artikel 9, tweede lid, onderdeel g, van de Algemene verordening gegevensbescherming, kunnen de regionale expertisecentra, voor zover dit noodzakelijk is voor het doel, bedoeld in artikel 31, persoonsgegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid verwerken. De deelnemers kunnen voor het doel, bedoeld in artikel 31, gebruikmaken van het burgerservicenummer, bedoeld in artikel 1 van de Wet algemene bepalingen burgerservicenummer.
Het is noodzakelijk om deze bijzondere persoonsgegevens over het seksueel gedrag of seksuele gerichtheid te kunnen verwerken, gezien het doel en activiteiten van de RIEC's – het bevorderen van de bestuurlijke en geïntegreerde aanpak van georganiseerde criminaliteit welke zich richt op zowel individuele daders en criminele samenwerkingsverbanden als op de achterliggende gelegenheidsstructuren of factoren die de misdaad (kunnen) faciliteren. In dat verband is het noodzakelijk om zowel van individuele personen als van leden van groepen en daarmee in verband te brengen zakelijke relaties alle relevante persoonsgegevens te kunnen verwerken.

Artikel 34 heeft geen betrekking op persoonsgegevens van strafrechtelijke aard omdat reeds in de artikelen 5, 6 en 7 voor alle samenwerkingsverbanden is geregeld dat deze mogen worden verwerkt, zowel in de fase van verstrekking aan het samenwerkingsverband, verwerking binnen het samenwerkingsverband en verstrekking van de resultaten door het samenwerkingsverband. Voor de aanpak van georganiseerde criminaliteit is essentieel dat ook persoonsgegevens van strafrechtelijke aard kunnen worden verwerkt. Bij de aanpak van mensenhandel kunnen in RIEC-verband ook onderzoeken plaatsvinden naar illegale prostitutie en uitbuiting, waarbij gegevens over seksueel gedrag verwerkt (moeten) worden.
Voor de bescherming van deze gegevens biedt dit wetsvoorstel voldoende adequate waarborgen, zoals de geheimhoudingsplicht en voorwaarden die aan doorverstrekking

worden gesteld. Uiteraard geldt ook de eis uit de AVG dat de verwerking daarvan niet leidt tot discriminatie of stigmatisering.
Zoals aangegeven moeten alle concrete verwerkingen van persoonsgegevens voldoen aan de rechtmatigheidseisen uit artikel 5 van de AVG. Het is aan de RIEC's zelf om een zorgvuldige procedure in te richten voor het gezamenlijke verwerken van bijzondere categorieën van persoonsgegevens, waarmee invulling gegeven wordt aan de beginselen van noodzaak, proportionaliteit en subsidiariteit uit de AVG.

Tweede lid

Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld over de wijze van verwerking van bijzondere categorieën van persoonsgegevens en het burgerservicenummer.

Artikel 35 (verstrekking van gegevens aan het samenwerkingsverband na ontvangst van een signaal)

Eerste lid

Artikel 35, eerste lid, bepaalt welke categorieën gegevens, met het oog op de activiteiten, bedoeld in artikel 31a, aan het samenwerkingsverband worden verstrekt na ontvangst van een signaal.

Onderdeel a

Onderdeel a bepaalt dat over de betrokkene of betrokkenen over wie of een rechtspersoon of rechtspersonen waarover een signaal als bedoeld in artikel 36 is ontvangen, en die subject is of zijn van het signaal, de volgende categorieën gegevens kunnen worden verstrekt.

1°
- identificerende en contactgegevens;
- het burgerservicenummer;
- gegevens betreffende de verblijfsstatus;
- gegevens omtrent de woonsituatie;
- voertuiggegevens;
- financiële gegevens;
- kadastrale gegevens;
- bedrijfsgegevens;
- inkomensgegevens;
- gegevens betreffende zakelijke relaties;
- gegevens betreffende vergunning- of subsidieaanvragen, hierop genomen besluiten en juridische procedures;
- gegevens inzake toezicht en handhaving alsmede getroffen bestuurlijke maatregelen;

2°
- fiscale gegevens;
- persoonsgegevens van strafrechtelijke aard in de zin van de artikelen 8, en 13 van de Wet politiegegevens die krachtens artikel 20, derde lid, van de Wet politiegegevens aan de deelnemers worden verstrekt;
- persoonsgegevens van strafrechtelijke aard die door het openbaar ministerie op grond van de artikelen 8b, 39fa, en 51ca, van de Wet justitiële en strafvorderlijke gegevens aan de deelnemers worden verstrekt;

3°
- gegevens over het seksueel gedrag of seksuele gerichtheid;
- persoonsgegevens van strafrechtelijke aard in de zin van de artikelen 9 en 10, eerste lid, onderdelen a en c, van de Wet

politiegegevens die op grond van artikel 20, derde lid van de Wet politiegegevens aan de deelnemers kunnen worden verstrekt.

Verstrekking van het burgerservicenummer aan het samenwerkingsverband is van belang om te kunnen borgen dat de te verwerken persoonsgegevens van de verschillende deelnemers betrekking hebben op dezelfde persoon. De deelnemers zoals benoemd in artikel 32 zijn allen reeds gehouden om het burgerservicenummer te verwerken op grond van hun eigen wettelijke taken en bevoegdheden.

Onder persoonsgegevens van strafrechtelijke aard als bedoeld in de artikelen 8 en 13 van de Wet politiegegevens worden onder meer verstaan de gegevens die voorkomen in politiemutaties en die verband houden met door een of meer deelnemers ingebrachte signalen. De gegevens kunnen ook dienen voor de politie om een signaal in het samenwerkingsverband in te brengen, waarna zij door de deelnemers in het samenwerkingsverband verder worden verwerkt als persoonsgegevens van strafrechtelijke aard.

De verstrekking van politiegegevens zoals bedoeld in artikel 9 en 10 eerste lid, onderdelen a en c, vindt plaats met in achtneming van wat daarover is bepaald de Wet politiegegevens en het Besluit politiegegevens. Op de verstrekking van politiegegevens zoals bedoeld in artikel 9 en 10 eerste lid, onderdelen a en c, die oorspronkelijk zijn verzameld met behulp van de inzet van bijzondere opsporingsbevoegdheden zoals bedoeld in het Wetboek van Strafvordering, is artikel 126dd Sv van toepassing. Dit betekent dat voorafgaand aan de verstrekking van deze politiegegevens eerst toestemming moet worden gevraagd aan de officier van justitie voor de verstrekking aan het RIEC-samenwerkingsverband omdat dit valt onder doelafwijkend gebruik in de zin van artikel 126dd Sv.

De onderverdeling tussen de drie typen categorieën gegevens, komt voort uit de relatieve zwaarte van de gegevens en de mate waarin het verwerken van die gegevens een inbreuk maakt op de persoonlijke levenssfeer van een betrokkene. Het eerste type gegevens ziet op reguliere gegevens waarover de deelnemers beschikken. Het tweede type gegevens betreft gegevens waarvan de verwerking een zwaardere inbreuk vormt op de persoonlijke levenssfeer dan het eerste type gegevens en die in de regel uitsluitend kunnen worden verkregen van bepaalde deelnemers, zoals de rijksbelastingdienst, politie of openbaar ministerie, namelijk fiscale gegevens en persoonsgegevens van strafrechtelijke aard, als bedoeld in de artikelen 8 en 13 van de Wet politiegegevens alsmede justitiële en strafvorderlijke gegevens in de zin van de Wet justitiële en strafvorderlijke gegevens. Het derde type gegevens betreft persoonsgegevens die de zwaarste inbreuk maken op de persoonlijke levenssfeer, namelijk persoonsgegevens van strafrechtelijke aard, bedoeld in de artikelen 9 en 10, eerste lid, onderdelen a en c, van de Wet politiegegevens. De deelnemers dienen bij de uitvoering van hun activiteiten telkens een zorgvuldige afweging te maken of het verwerken van deze categorieën gegevens wel noodzakelijk is voor het doel, gelet op de zwaarte van de inbreuk op de persoonlijke levenssfeer. Wanneer dat niet het geval is, dienen de deelnemers van de verwerking af te zien. Zoals aangegeven moeten alle concrete verwerkingen van persoonsgegevens voldoen aan de rechtmatigheidseisen uit artikel 5 van de AVG. Het is aan de RIEC's zelf om een zorgvuldige procedure in te richten voor het gezamenlijke verwerken van gegevens, waarmee invulling gegeven wordt aan de beginselen van noodzaak, proportionaliteit en subsidiariteit uit de AVG.

Onderdeel b

Onderdeel b bepaalt dat ter zake van personen uit de directe kring van betrokkene of betrokkenen of personen die in direct verband staan met de rechtspersoon of rechtspersonen, voor zover dat noodzakelijk is ten behoeve van het doel, bedoeld in artikel 31, de te verstrekken categorieën gegevens hetzelfde zijn als in onderdeel a.

Om wetstechnische redenen is onderdeel b een separaat onderdeel, dat net als onderdeel a in drieën is opgesplitst. Dit maakt het mogelijk om in artikel 36 naar de juiste categorieën gegevens te verwijzen.

Onderdeel c

Ter zake van medewerkers van deelnemers is het noodzakelijk om binnen het samenwerkingsverband hun identificerende en contactgegevens te kunnen verwerken, alsmede gegevens met betrekking tot hun persoon over hun autorisatieniveau en de wijze waarop deze medewerker is gescreend.

Tweede lid

Het tweede lid bepaalt dat bij algemene maatregel van bestuur nadere regels worden gesteld over de categorieën van gegevens en de concretisering daarvan, bedoeld in het eerste lid en de bronnen van waaruit die gegevens afkomstig zijn en kunnen aanvullende categorieën gegevens worden aangewezen, voor zover dat noodzakelijk is voor het doel, bedoeld in artikel 31. In dit artikel is een gelaagdheid beoogd van de beschrijving van de categorieën gegevens die de regionale informatie- en expertisecentra op grond van deze paragraaf verwerken. De regering kiest ervoor de categorieën gegevens in het wetsvoorstel te benoemen en om de nadere concretisering daarvan en de bronnen van waaruit de gegevens afkomstig te zijn bij lagere regelgeving vast te stellen. Op deze manier wordt recht gedaan aan het uitgangspunt dat bij wet in formele zin moet worden vastgelegd ter zake van welke gegevens betrokkene kan verwachten dat die ten aanzien van zijn persoon worden verwerkt in het kader van het samenwerkingsverband. Op de vaststelling van deze algemene maatregel van bestuur is de voorhangprocedure van toepassing.

Artikel 36 (grondslag verwerkingsactiviteiten)

Eerste tot en met zesde lid

Artikel 36, eerste tot en met zesde lid, biedt de grondslag voor de gezamenlijke verwerking van gegevens in het kader van de activiteiten, namelijk:

a. het aanwijzen en analyseren van handhavingsknelpunten;
b. het voeren van casusoverleggen;
c. het verrichten van gebiedscans en thematische scans bij misstanden in maatschappelijke sectoren en publieke voorzieningen die vatbaar zijn voor innesteling van georganiseerde criminaliteit.

Zoals bij artikel 31a is toegelicht verrichten de regionale informatie- en expertisecentra met het oog op het doel van artikel 31 de voornoemde activiteiten waarvoor zij gezamenlijk (persoons)gegevens verwerken. De gezamenlijke gegevensverwerking in het kader van deze activiteiten geschiedt op dezelfde wijze. Om die reden volstaat dit artikel als de verwerkingsgrondslag voor alle drie voornoemde activiteiten.

De aanleiding voor het verrichten van een van deze activiteit kan zijn gelegen in een signaal dat of signalen die één of meer deelnemers inbrengt of inbrengen in het regionale informatie- en expertisecentrum. Signalen kunnen alleen door de betreffende deelnemer of deelnemers bij de regionale informatie- en expertisecentra worden ingediend wanneer het signaal feiten en omstandigheden betreft die voortkomen uit waarnemingen die zijn gedaan tijdens de uitoefening van hun respectievelijke wettelijke taken en bevoegdheden en die erop duiden dat sprake is van een verschijningsvorm van georganiseerde criminaliteit. De gezamenlijke gegevensverwerking in het kader van de voornoemde activiteiten resulteert in een interventieadvies dat de betrokken deelnemers beter in staat stelt hun wettelijke taken en bevoegdheden op effectieve en adequate wijze uit te oefenen. Het advies wordt gebruikt om te bepalen of interventie noodzakelijk is, of interventie in afstemming tussen bepaalde deelnemers moet gebeuren en welke deelnemers betrokken moeten zijn alsmede welke deelnemer verantwoordelijk is voor de

te verrichten interventie of interventies dan wel welke deelnemer de coördinatie op zich neemt van gezamenlijk te verrichten interventies.
Bij monodisciplinaire interventies, bijv. alleen fiscale maatregelen ligt de coördinatie bij de Belastingdienst, bij strafrechtelijke interventies liggen de verantwoordelijkheden zoals die zijn benoemd in het wetboek van Strafvordering en heeft het OM het gezag over de opsporing. Bij multidisciplinaire interventies van zowel strafrechtelijke als bestuursrechtelijke en fiscale maatregelen moet van geval tot geval worden bepaald waar de coördinatie komt te liggen, maar met respect voor de bevoegdheden van alle partijen. Deelnemers treden niet in elkaars bevoegdheden.

In deze bepaling wordt richting gegeven aan het stapsgewijze proces voor de verwerking van persoonsgegevens en andere relevante gegevens bij de uitvoering van de activiteiten, bedoeld in artikel 31a. Het stapsgewijze proces is gekoppeld aan de drie typen categorieën gegevens die in artikel 35, eerste lid, worden onderscheiden. Zoals in de toelichting bij artikel 35 is aangegeven, komt de onderverdeling tussen de drie typen categorieën gegeven voort uit de relatieve zwaarte van de gegevens en de mate waarin het verwerken van die gegevens een inbreuk maakt op de persoonlijke levenssfeer van een betrokkene. De bedoeling van artikel 36 is dat de deelnemers telkens een afweging maken of het verwerken van deze onderscheidenlijke drie typen categorieën gegevens noodzakelijk is voor het doel, bedoeld in artikel 31. Uitgangspunt is daarom dat die afweging als volgt plaatsvindt, rekening houdend met de zwaarte van de categorieën gegevens:

1) in de eerste fase kunnen gegevens worden verwerkt die worden ingebracht door de deelnemers en die geen bijzondere categorieën van persoonsgegevens, persoonsgegevens van strafrechtelijke aard betreffen of fiscale gegevens betreffen;
2) in de tweede kunnen fiscale gegevens, persoonsgegevens van strafrechtelijke aard worden verwerkt, zijnde gegevens in de zin van artikel 8 en 13 van de Wet politiegegevens en gegevens bedoeld in de Wet justitiële en strafvorderlijke gegevens;
3) in de derde fase kunnen bijzondere categorieën van persoonsgegevens, persoonsgegevens van strafrechtelijke aard worden verwerkt, zijnde gegevens in de zin van artikel 9 en 10 van de Wet politiegegevens.

Met dit stapsgewijze proces waarin verschillende categorieën van persoonsgegevens naar de mate van zwaarte worden verwerkt voor zover dat noodzakelijk is voor het doel, bedoeld in artikel 31, wordt invulling gegeven aan de beginselen van subsidiariteit en proportionaliteit.

Artikel 36, eerste tot en met zesde lid, regelt het stapsgewijze proces als volgt:

1) Een deelnemer kan bij de regionale informatie- en expertisecentra een signaal melden, en daartoe gegevens verwerken (eerste lid).
2) De deelnemers beoordelen vervolgens of het signaal in overeenstemming is met het doel, bedoeld in artikel 31 (tweede lid).
3) Bij de afweging of een signaal voldoende aanleiding geeft tot gezamenlijke verwerking van gegevens in het regionaal informatie- en expertisecentrum, toetsen de deelnemers aan:
    a. het type signaal;
    b. het aantal signalen alsmede de aard en omvang daarvan;
    c. het gewicht van het signaal en de reeds gepleegde interventies ter zake van het signaal of de signalen, en
    d. het aantal deelnemers dat overeenkomstige signalen meldt, alsmede het verband tussen de signalen.
4) Pas wanneer het signaal naar het oordeel van de deelnemers aanleiding geeft tot het verrichten van een van de voornoemde activiteiten in het RIEC en dit noodzakelijk is met het oog op het doel, bedoeld in artikel 31, kunnen de deelnemers overgaan tot verzameling en uitwisseling van en samenvoeging

met andere relevante gegevens, bedoeld in artikel 35, die beschikbaar zijn bij andere deelnemers (vierde lid).

5) De deelnemers beoordelen vervolgens welke deelnemers met het oog op het doel van artikel 31 moeten worden betrokken bij de te verrichten activiteit en daarbij gegevens mogen verwerken (vijfde lid). Niet alle deelnemers worden automatisch betrokken: er wordt een zorgvuldige afweging gemaakt welke deelnemers moeten worden betrokken gelet op hun onderscheidenlijke taken en bevoegdheden. Hierdoor wordt de gezamenlijke verwerking beperkt tot die deelnemers wier deelname gelet op het doel van artikel 31 daadwerkelijk noodzakelijk is.
6) De verwerking van gegevens in het kader van een activiteit, bedoeld in artikel 31a, eerste lid, vindt plaats overeenkomstig de volgende stappen:
    a. Indien een signaal aanleiding geeft tot gezamenlijke verwerking van gegevens in het kader van een activiteit, bedoeld in artikel 31a, eerste lid, met het oog op het doel, bedoeld in artikel 31, kunnen de betrokken deelnemers overgaan tot het verder verzamelen en uitwisselen van en samenvoegen met andere relevante gegevens die beschikbaar zijn bij andere deelnemers op de wijze zoals hiervoor is toegelicht (zesde lid). Daarbij kunnen de deelnemers relevante gegevens, bedoeld in artikel 35, eerste lid, onderdeel a, onderdeel 1° en onderdeel b, onderdeel 1°, verwerken.
    b. Indien deelnemers gezamenlijk gegevens verwerken ter uitvoering van een activiteit, bedoeld in artikel 31a, eerste lid, onderdelen a of b en dat met het oog op het doel, bedoeld in artikel 31, noodzakelijk is, kunnen de deelnemers in aanvulling op de gegevens, bedoeld in onderdeel a van dit artikellid, gegevens verwerken, bedoeld in artikel 35, eerste lid, onderdeel a, onderdeel 2°, en onderdeel b, onderdeel 2°.
    c. Indien de deelnemers gezamenlijk gegevens verwerken ter uitvoering van een activiteit, bedoeld in artikel 31a, eerste lid, onderdelen a of b, en dat noodzakelijk is met het oog op het doel, bedoeld in artikel 31, kunnen de deelnemers in aanvulling op de gegevens, bedoeld in onderdelen a en b van dit artikellid, de gegevens verwerken, bedoeld in artikel 35, eerste lid, onderdeel a, onderdeel 3°, en onderdeel b, onderdeel 3°.

Het kan in de praktijk van de RIEC's voorkomen dat een signaal al na ontvangst als dusdanig ernstig wordt beschouwd, dat het noodzakelijk kan zijn al direct over te gaan tot het gezamenlijk verwerken van de zwaardere typen categorieën gegevens. Deze bepaling staat dat toe, mits de deelnemers zich ervan rekenschap geven dat zij daartoe pas overgaan na zorgvuldige afweging. Duidelijkheidshalve wordt hier herhaald dat alle concrete verwerkingen van persoonsgegevens moeten voldoen aan de rechtmatigheidseisen uit artikel 5 van de AVG. Het is aan de RIEC's zelf om een zorgvuldige procedure in te richten voor het gezamenlijke verwerken van gegevens, waarmee invulling gegeven wordt aan de beginselen van noodzaak, proportionaliteit en subsidiariteit uit de AVG.

Zevende lid

De gezamenlijke verwerking op grond van dit artikel kan, zoals hiervoor aangegeven, resulteren in een interventieadvies dat de betrokken deelnemers in staat stelt hun wettelijke taken en bevoegdheden uit te oefenen. Het advies kan worden gebruikt om de bepalen of interventie wenselijk en noodzakelijk is, of deze in afstemming tussen bepaalde deelnemers moet gebeuren en welke deelnemers betrokken moeten zijn alsmede welke deelnemer verantwoordelijk is voor de gezamenlijk te verrichten interventie of interventies. Het zevende lid regelt dat de deelnemers daartoe gegevens mogen verwerken. Bij het verstrekking van resultaten aan de deelnemers wordt artikel 7, eerste lid, in acht genomen.

Achtste lid

Het achtste lid bepaalt, in samenhang bezien met artikel 7, tweede lid, dat resultaten van de gezamenlijke verwerking van gegevens in het kader van de regionale informatie- en expertisecentra aan een derde kunnen worden verstrekt. Het kan hierbij gaan om andere overheden, een private partij of de deelnemers van een ander samenwerkingsverband. Voor gegevens van de rijksbelastingdienst geldt een uitzondering: die kunnen niet aan private partijen worden verstrekt ter behartiging van een gerechtvaardigd belang.

De verstrekking die hier geregeld wordt, is incidenteel van aard: bij elke verstrekking moeten de deelnemers beoordelen of de verstrekking verenigbaar is met het doel, bedoeld in artikel 31. Daarbij moet ook worden voldaan aan de eisen van artikel 6, vierde lid, van de AVG. Bij de verstrekking aan derden zal voorts moeten worden voldaan aan de criteria die daarvoor op grond van artikel 36, negende lid, bij of krachtens algemene maatregel van bestuur kunnen worden gesteld.

De resultaten bestaan uit een advies de eigen bevoegdheden of mogelijkheden te benutten om bij te dragen aan het doel van het RIEC-samenwerkingsverband. Het advies bevat slechts die gegevens die nodig zijn om het gegeven advies te onderbouwen en een gedegen afweging van de mogelijke interventies te maken.

Negende lid
In het negende lid is bepaald dat bij of krachtens algemene maatregel van bestuur nadere regels kunnen worden gesteld over de gezamenlijke verwerking van gegevens op grond van dit artikel, waaronder over de criteria waaraan een signaal moet voldoen en de criteria voor verstrekking van de resultaten van de gezamenlijke verwerking van gegevens aan een derde.

Paragraaf 2.4 De Zorg- en Veiligheidshuizen

Artikel 46 (aanwijzing)

In artikel 46, eerste lid, worden de Zorg- en Veiligheidshuizen aangewezen als samenwerkingsverbanden in de zin van deze wet. Het Zorg- en Veiligheidshuis is een samenwerkingsverband waarin instanties verantwoordelijk voor strafrechtelijke of bestuursrechtelijke handhaving alsmede begeleiding, zorg en hulpverlening tot eenduidige regie komen bij de samenwerking rond complexe casussen in het zorg- en veiligheidsdomein. De samenwerking in het Zorg- en Veiligheidshuis heeft tot doel een bijdrage te leveren aan het voorkomen, verminderen en bestrijden van criminaliteit en ernstige overlast en het bieden van passende zorg, in situaties waarin sprake is van complexe (zorg)problematiek die zonder interventie leidt of kan leiden tot onveilige situaties voor personen of binnen een gebied. De deelnemers doen dat door te komen tot een persoonsgerichte aanpak, waarbij instrumenten op het gebied van het strafrecht en het bestuursrecht, bestuurlijke maatregelen en noodzakelijke zorg en ondersteuning op elkaar zijn afgestemd. Zij doen dat vanuit de wetenschap dat (potentieel) crimineel en overlastgevend gedrag veelal zijn oorzaak vindt in sociale- en zorgproblematiek. Samenwerking tussen deelnemers uit de strafrechtketen, het bestuurlijk domein en het sociale en zorgdomein is dan noodzakelijk om tot een duurzame verbetering van de situatie te komen, zowel voor de betrokkene zelf, als voor de omgeving waarin deze woont, leeft en werkt. Welke deelnemers in een concreet geval noodzakelijk zijn wordt bepaald door de casus en de aard van de problematiek.

Door de aanwijzing van de Zorg- en Veiligheidshuizen als samenwerkingsverbanden in de zin van deze wet wordt geregeld dat de deelnemers aan de Zorg- en Veiligheidshuizen gegevens waarover zij in het kader van de uitoefening van hun bestaande wettelijke taken en bevoegdheden, de uitvoering van een behandelovereenkomst als bedoeld in de Wet geneeskundige behandelovereenkomst of diensten op grond van de Jeugdwet, en andere relevante gegevens gezamenlijk kunnen verwerken, om tot de hier boven

genoemde persoonsgerichte aanpak te kunnen komen. Naast de algemene bepalingen van hoofdstuk 1, worden in deze paragraaf aanvullende regels gesteld over de gezamenlijke verwerking van persoonsgegevens en andere relevante gegevens in het kader van de Zorg- en Veiligheidshuizen.

De aanwijzing heeft uitsluitend betrekking op het mogelijk maken en reguleren van de gezamenlijke verwerking van persoonsgegevens en andere relevante gegevens in de samenwerking tussen deelnemers. Duidelijkheidshalve wordt benadrukt dat de aanwijzing in de zin van deze bepaling nadrukkelijk niet tot gevolg heeft dat er een nieuw overheidsorgaan, instantie of zelfstandige entiteit van enige vorm ontstaat, waarmee er eventueel nieuwe juridische verhoudingen zouden ontstaan tussen de deelnemers of ter zake van het samenwerkingsverband als zodanig. Aan het wetsvoorstel ligt het uitgangspunt ten grondslag dat de gezamenlijke verwerking van persoonsgegevens en andere relevante gegevens ten dienste staat aan de uitoefening van de bestaande wettelijke taken en bevoegdheden van de deelnemers. Er worden met de aanwijzing of enige andere bepaling in dit wetsvoorstel derhalve geen nieuwe taken of bevoegdheden aan de deelnemers of aan de samenwerkingsverbanden als zodanig toegekend. Artikel 3, vierde en vijfde lid, bepaalt dat aanwijzing als deelnemer geen wijziging aanbrengt in de publiekrechtelijke taken en bevoegdheden van de deelnemers alsmede dat de deelnemers een samenwerkingsverband zonder rechtspersoonlijkheid vormen. Voor zover dit wetsvoorstel regels bevat over de juridische verhoudingen tussen de deelnemers, hebben die uitsluitend betrekking op de nadere uitwerking van de eisen die de Algemene verordening gegevensbescherming stelt ter zake van de gezamenlijke verwerking, zoals de gezamenlijke verwerkingsverantwoordelijkheid.

Evenmin regelt dit wetsvoorstel de organisatie, inrichting, positionering en het beheer van de samenwerkingsverbanden. De regeling daarvan is voorbehouden aan de deelnemers. Een samenwerkingsverband vraagt om ondersteuning in de vorm van huisvesting, ICT-voorzieningen, ondersteuning en personeel. De deelnemers maken onderling afspraken over de wijze waarop het samenwerkingsverband wordt ingericht, taken stelt, prioriteiten vaststelt en zorgdraagt voor financiering en beheer. Dat de deelnemers op grond van artikel 3, vijfde lid, een samenwerkingsverband vormen zonder rechtspersoonlijkheid, heeft betrekking op de gezamenlijke verwerking van gegevens op grond van dit wetsvoorstel en laat verder onverlet dat het de deelnemers vrij staat indien nodig voor de invulling (op onderdelen) van deze ondersteuning gebruik te maken van hierop toegesneden rechtsvormen, zoals bijvoorbeeld een stichting of een gemeenschappelijke regeling. Ook kan als er betrokkenheid gewenst is van meerdere deelnemers, zoals bijvoorbeeld meerdere gemeenten in een bepaalde regio, sprake zijn van mandaatverlening in de zin van afdeling 10.1.1 van de Algemene wet bestuursrecht.

In artikel 46, tweede lid, is geregeld dat bij of krachtens algemene maatregel van bestuur regels kunnen worden gesteld over de territoriale werkgebieden van de Zorg- en Veiligheidshuizen. De Zorg- en Veiligheidshuizen zijn regionaal georganiseerd en omvatten elk een separaat territoriaal werkgebied. Omwille van de transparantie van de gezamenlijke gegevensverwerking in een specifieke regio, is het wenselijk deze regio's te duiden in de lagere regelgeving. Hiermee wordt namelijk duidelijkheid geboden aan de betrokkenen over wie gegevens worden verwerkt en tot welk Zorg- en Veiligheidshuis zij zich kunnen wenden voor het uitoefenen van hun rechten op grond van de AVG, bijvoorbeeld om geïnformeerd te worden.

Bij het bepalen van nadere regels over de territoriale werkgebieden, zal in beginsel worden aangesloten bij de regionale indeling zoals die op dat moment geldt op basis van afspraken tussen de deelnemers. Door de territoriale werkgebieden bij algemene maatregel van bestuur te bepalen, kan na de initiële vaststelling worden ingespeeld op regionale veranderingen in de toekomst, bijvoorbeeld als het werkgebied van een Zorg- en Veiligheidshuis aangepast moet worden in verband met gemeentelijke herindeling. Ook kan het zijn dat Zorg- en Veiligheidshuizen op grond van regionale omstandigheden zelf komen tot voorstellen voor een andere territoriale indeling.

Artikel 47 (doel)
In artikel 47 is het doel bepaald met het oog waarop de Zorg- en Veiligheidshuizen persoonsgegevens en andere relevante gegevens verwerken. Zorg- en Veiligheidshuizen focussen zich op complexe casuïstiek. Van complexe casuïstiek is sprake in de volgende gevallen.
- Indien bij een betrokkene meerdere problemen op meer dan één leefgebied[32] spelen en die (naar verwachting) leiden tot crimineel en/of overlastgevend gedrag of maatschappelijke teloorgang;
- en samenwerking tussen meerdere ketens (minimaal dwang en drang) nodig is om tot een effectieve aanpak te komen; het is in de reguliere samenwerking tussen partners binnen één keten niet mogelijk om deze problematiek effectief aan te pakken;
- en de problematiek beïnvloed wordt door, en impact heeft op het (gezins)systeem en/of de directe sociale leefomgeving (of wordt verwacht dat te gaan hebben);
- of er sprake is van ernstige lokale of gebiedsgebonden (veiligheids)problematiek, die vraagt om een ketenoverstijgende aanpak.
Daarbij kan het gaan om personen met een hoog veiligheidsrisico, ernstige multi-probleemgezinnen of zorgmijders die strafbare feiten plegen, ernstige overlast veroorzaken of weigeren mee te werken aan hulpverlening, en waarachter een complexe problematiek schuilgaat.

Voor een succesvolle en duurzame oplossing van deze problematiek is het noodzakelijk dat er samenwerking tot stand kan komen tussen de verschillende deelnemers die zijn belast met strafrechtelijke of bestuursrechtelijke handhaving alsmede begeleiding, zorg en hulpverlening. Onder hulpverlening wordt ook verstaan de ondersteuning die de gemeente biedt vanuit haar taken op het terrein van het sociaal domein. Het doel is om criminaliteit en ernstige overlast te voorkomen en de veiligheidsrisico's voor betrokkene en de omgeving waar hij woont, werkt en leeft, te verkleinen. Daarbij richten de Zorg- en Veiligheidshuizen zich zowel op bestaande overtreders van de wet (voorkomen recidive) als op individuen binnen groepen met groot risico op afglijden richting crimineel en ernstig overlastgevend gedrag.

Samenwerking in het Zorg- en Veiligheidshuis door de deelnemers draagt bij aan de effectiviteit en de kwaliteit van de gepleegde interventies doordat informatie van deelnemers bij elkaar komt. Op die manier ontstaat er een beter begrip van de achterliggende problematiek, kunnen interventies op elkaar worden afgestemd en in samenhang worden uitgevoerd. Door de gezamenlijke inzet van de deelnemers kan de strafrechtelijke aanpak als stok achter de deur dienen voor effectieve zorg- en hulpverlening. Op haar beurt wint de strafrechtelijke aanpak aan effectiviteit door aanvulling met zorg- en hulpverlening. Om dat te kunnen realiseren is gezamenlijke gegevensverwerking noodzakelijk.

De Zorg- en Veiligheidshuizen verwerken gegevens in het belang van het voorkomen, verminderen en bestrijden van criminaliteit en ernstige overlast en het bieden van passende zorg in situaties waarin sprake is van complexe (zorg)problematiek, die zonder interventie leidt of kan leiden tot onveilige situaties voor personen of binnen een gebied. Zij doen dat uitsluitend voor zover dat noodzakelijk is voor de uitoefening, afstemming en coördinatie van de inzet van de wettelijke taken en bevoegdheden waarmee deelnemers zijn belast en de daaraan gerelateerde noodzakelijke activiteiten van deelnemers op het terrein van strafrechtelijke en bestuursrechtelijke handhaving alsmede begeleiding en zorg- en hulpverlening.

Voor de publiekrechtelijke deelnemers aan de Zorg- en Veiligheidshuizen geldt dat artikel 6, eerste lid, onderdelen c (voldoen aan een wettelijke verplichting) en e (noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag) van de AVG de grondslag vormen om

[32] Hierbij gaat het om leefgebieden met criminogene factoren, zoals deze ook in diverse instrumenten worden gehanteerd, zoals: werk en inkomen, financiën, onderwijs, psychische en fysieke gezondheid, wonen, relaties.

persoonsgegevens te verwerken. Aan de Zorg- en Veiligheidshuizen nemen naast publiekrechtelijke partijen, ook private partijen deel (zie hierna). De grondslag voor deze partijen om persoonsgegevens te verwerken is gelegen in artikel 6, eerste lid, onderdelen b (uitvoering van een overeenkomst), c (voldoen aan een wettelijke verplichting) en f (de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde).

Uit de bestaande wettelijke taken, bevoegdheden en activiteiten van de deelnemers vloeit reeds voort dat de verwerking van persoonsgegevens en andere relevante gegevens voor de uitoefening daarvan noodzakelijk is. Deze bepaling bouwt daarop voort door de informatiepositie van afzonderlijke deelnemers in aanvulling daarop te versterken door de mogelijkheid te creëren om onder voorwaarden persoonsgegevens en andere relevante gegevens met relevante deelnemers uit te wisselen en in gezamenlijkheid te verwerken. Het wetsvoorstel creëert immers geen nieuwe taken en bevoegdheden voor de deelnemers of de samenwerkingsverbanden als zodanig. Doordat de verwerking altijd noodzakelijk moet zijn voor de uitoefening van hun bestaande wettelijke taken en bevoegdheden, of de activiteiten op het gebied van begeleiding, hulp of ondersteuning, zijn het doel en de grenzen daarvan duidelijk afgebakend, welbepaald en uitdrukkelijk omschreven. Gelet op het feit dat de gezamenlijke gegevensverwerking uitsluitend is toegestaan in het belang van het zwaarwegend algemeen belang van het voorkomen, verminderen en bestrijden van criminaliteit, en ernstige overlast waarbij sprake is van een combinatie van complexe (zorg)problematiek die zonder interventie leidt of kan leiden tot onveilige situaties voor personen of binnen een gebied, is sprake van een gerechtvaardigd belang.
Bij alle bevoegdheden tot persoonsgegevensverwerking die de deelnemers krijgen op grond van deze paragraaf, moet worden getoetst of de persoonsgegevensverwerking noodzakelijk is het met oog op het doel van artikel 47. Elke separate persoonsgegevensverwerking moet daarnaast voldoen aan de eisen van de AVG. Onderdeel daarvan is ook dat bij elke casus steeds een afweging zal moeten worden gemaakt welke deelnemers op welk moment betrokken moeten worden bij een casus en dus gezamenlijk gegevens verwerken.
Het doel waarvoor Zorg- en Veiligheidshuizen persoonsgegevens kunnen uitwisselen is, zoals hiervoor aangegeven, gekoppeld aan de uitoefening van de bestaande wettelijke taken en bevoegdheden van de deelnemers en daaraan gerelateerde noodzakelijke activiteiten die worden verricht door een aantal specifieke deelnemers (private partijen zoals hiervoor vermeld). Hiermee wordt uitvoering gegeven aan de verplichting uit de artikelen 5, 6, eerste lid, onderdelen c en e, in samenhang met het derde lid, van de Algemene verordening gegevensbescherming. Artikel 5, onderdelen a en b, van de AVG bepalen dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is, alsmede voor welbepaalde uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld en niet verder mogen worden verwerkt op een met die doeleinden onverenigbare wijze. Artikel 6, eerste lid, onderdelen c en e, van de AVG bepalen dat de verwerking van persoonsgegevens alleen rechtmatig is indien de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust is of voor een taak van algemeen belang of van een taak in het kader van de uitoefening van openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Artikel 6, derde lid, onderdeel b, van de AVG bepaalt dat de rechtsgrond moet worden vastgesteld bij lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is. Het doel van de verwerking moet bij de rechtsgrond worden vastgesteld of is noodzakelijk voor de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend. Het lidstatelijke recht moet beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde gerechtvaardigde doel.

De grondslagen voor gezamenlijke verwerking van persoonsgegevens bij of krachtens de WGS zijn gericht op een doel van zwaarwegend algemeen belang dat niet op voorhand verenigbaar is met de doelen waarvoor de deelnemers de te verstrekken gegevens hebben verzameld. Artikel 6, vierde lid, aanhef, AVG staat ook verdere verwerking voor

een niet-verenigbaar doel toe, mits wettelijk geregeld en in het kader van een zwaarwegend algemeen belang. Het wetsvoorstel beoogt zo'n grondslag te bieden. Het lidstatelijk recht moet dan wel één van de belangen van artikel 23, eerste lid, AVG beschermen. Dat is hier het geval, zoals toegelicht aan het slot van paragraaf 3.3.1 van het algemeen deel van de memorie van toelichting. De Zorg- en Veiligheidshuizen hebben tot doel bij de behandeling van complexe casuïstiek gegevens te verwerken ten aanzien van een betrokkene voor zover dat noodzakelijk is voor de uitoefening, afstemming en coördinatie van de inzet van de wettelijke taken en bevoegdheden waarmee de deelnemers zijn belast en daaraan gerelateerde noodzakelijke activiteiten op het terrein van strafrechtelijke en bestuursrechtelijke handhaving alsmede begeleiding en zorg- en hulpverlening in het belang van het voorkomen, verminderen en bestrijden van criminaliteit en ernstige overlast en het voorkomen en verminderen van onveilige situaties voor personen of binnen een gebied. Het doel van de Zorg- en Veiligheidshuizen en de regulering van de gezamenlijke gegevensverwerking voor dat doel in dit wetsvoorstel, vormt daarmee een noodzakelijke en evenredige maatregel als bedoeld in de artikel 23, eerste lid, onderdelen c, d en e, van de AVG, ter waarborging van de openbare veiligheid en de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid alsmede in het belang van de volksgezondheid.

Artikel 47a (activiteiten)
In artikel 47a wordt geregeld welke twee activiteiten de Zorg- en Veiligheidshuizen verrichten met het oog op het doel dat is omschreven in artikel 47. Het gaat daarbij om het voeren van casusoverleggen en/of het vaststellen van lijsten met geprioriteerde casussen. Het is aan de deelnemers van het desbetreffende Zorg- en Veiligheidshuis voorbehouden te bepalen aan welke van deze twee activiteiten uitvoering wordt gegeven en of zij daarbij gezamenlijk gegevens verwerken. Indien dat het geval is, geldt daarvoor het bepaalde bij of krachtens dit wetsvoorstel. De grondslagen voor de verwerking van gegevens in het kader van deze activiteiten zijn opgenomen in respectievelijk de artikelen 52 en 53.

Onderdeel a: het voeren van casusoverleggen
De Zorg- en Veiligheidshuizen faciliteren en regisseren casusoverleggen waar afspraken worden gemaakt over een persoonsgerichte aanpak bij complexe casuïstiek. Bij het voeren van casusoverleggen maken betrokken deelnemers afspraken over interventies die ten aanzien van een betrokkene worden ingezet, de uitvoering, evaluatie en zo nodig het bijstellen van die afspraken, alsmede over de afsluiting van de casus. Op die manier ontstaat een gezamenlijke strategie voor de uitoefening van de wettelijke taken en bevoegdheden van de deelnemers en de daaraan gerelateerde noodzakelijke activiteiten die worden verricht door de deelnemers. Alvorens tot een casusoverleg te komen toetsen de deelnemers de casus aan het doel van het samenwerkingsverband, en stellen zij een persoonsbeeld op om te kunnen wegen of een casus besproken dient te worden in het casusoverleg. Daarbij verkennen zij tegelijk welke vaste en incidentele deelnemers bij het casusoverleg dienen te worden betrokken. Indien een casus niet in aanmerking komt voor bespreking in het casusoverleg, wordt de melder daarover geïnformeerd en indien mogelijk van advies voorzien voor verdere behandeling.

Tijdens een casusoverleg bespreken de deelnemers de casus. Daarbij wordt indien nodig dieper ingegaan op de karakteristieken van het gedrag én de omstandigheden van een persoon: welke oorzakelijke factoren zijn er? Hoe kan het ongewenste (criminele, overlastgevende) gedrag verklaard worden? Zo ontstaat er een brede blik op de persoon en zijn leefwereld, waarin aangrijpingspunten besloten liggen voor een effectieve aanpak. In een casusoverleg worden er geen beslissingen door het casusoverleg als geheel genomen over de aanpak van personen of uitoefening van taken of de aanwending van bevoegdheden door deelnemende partijen. De beslissing over de inzet van eigen bevoegdheden berust immers exclusief bij elke deelnemer zelf. Het casusoverleg strekt uitsluitend tot het creëren van een beter inzicht in de problematiek, en afstemming

tussen interventies en activiteiten van deelnemers met het oog op het in artikel 47 gestelde doel.

Onderdeel b: het vaststellen van lijsten met geprioriteerde casussen
Soms is er binnen een regio sprake van een bepaalde vorm van criminaliteit die veel voorkomt of bijzondere overlast veroorzaakt. Ook kan er sprake zijn van een veiligheidsprobleem dat sterk lokaal en gebiedsgebonden is, of specifieke veiligheidsrisico's. Om in dergelijke situaties focus en slagkracht te realiseren binnen de aanpak van het probleem is het nodig om extra aandacht te schenken aan personen die het meest bijdragen aan de betreffende vorm van criminaliteit, de onveiligheid of het veiligheidsrisico. Dit artikel creëert de mogelijkheid om in dergelijke situaties op basis van objectieve criteria, een lijst samen te stellen met personen die prioriteit moeten krijgen bij de aanpak van het probleem. Deze aanpak wordt ook wel 'Top X' aanpak genoemd. De lijst stelt deelnemers in staat om beschikbare middelen bij voorrang in te zetten op de aldus geselecteerde casussen. Het prioriteren van casussen aan de hand van het opstellen en gebruiken van een dergelijke lijst, draagt bij aan het bepalen en uitvoeren van een gezamenlijke strategie voor de uitoefening van de taken en bevoegdheden waarmee de deelnemers zijn belast.

Artikel 48 (deelnemers)

Eerste en tweede lid

In artikel 48 worden de deelnemers aan de Zorg- en Veiligheidshuizen aangewezen. Deelnemers aan een Zorg- en Veiligheidshuis hebben op basis van deze wet een grondslag voor de verwerking van persoonsgegevens in het kader van de activiteiten van artikel 47a, voor zover dat noodzakelijk is voor het doel van artikel 47.

Aanwijzing als deelnemer aan het Zorg- en Veiligheidshuis betekent onder andere dat het bestuursorgaan, de organisatie of de instelling betrokken wordt en mede zeggenschap heeft over de wijze waarop de samenwerking wordt georganiseerd en de wijze waarop de gegevensverwerking in het Zorg- en Veiligheidshuis wordt ingericht.

Het feit dat een bestuursorgaan, organisatie of instelling is aangewezen als deelnemer aan het Zorg- en Veiligheidshuis, betekent niet dat deze deelnemer bij alle casussen die in het Zorg- en Veiligheidshuis behandeld worden, of bij alle activiteiten zoals geschetst in artikel 52 of 53, ook daadwerkelijk deel zal nemen aan de verwerking van gegevens. Welke deelnemers in een specifieke casus noodzakelijk zijn om te komen tot een persoonsgerichte aanpak is immers afhankelijk van de aard van de problematiek. Het standaard betrekken van alle deelnemers bij elke casus die zich aandient, in alle fasen van het proces, zou op gespannen voet staan met de beginselen van noodzaak, subsidiariteit en proportionaliteit uit de AVG. De deelnemers in de Zorg- en Veiligheidshuizen zullen daarom afspraken moeten maken hoe zij bij de uitvoering van hun activiteiten invulling geven aan de beginselen van noodzaak, subsidiariteit en proportionaliteit van de AVG, om zo de persoonlijke levenssfeer van de betrokkene te beschermen.

De aanwijzing van de deelnemers wordt onderverdeeld in twee groepen. In artikel 48, eerste lid, worden de publiekrechtelijke deelnemers of overheidsinstanties aangewezen die zijn belast met de uitoefening van wettelijke taken of bevoegdheden. In artikel 48, tweede lid, wordt een aantal private partijen als deelnemer aangewezen die bij of krachtens de wet taken of bevoegdheden uitoefenen of daartoe door een bestuursorgaan gemandateerd zijn, of daaraan gerelateerde noodzakelijke activiteiten verrichten, en die verband houden met het doel, bedoeld in artikel 47. Met laatstgenoemde activiteiten wordt onder andere gedoeld op instellingen voor geestelijke gezondheidszorg. Hieronder wordt daar nader op ingegaan.

Voor alle deelnemers geldt dat zij gezamenlijk gegevens kunnen verwerken in het samenwerkingsverband, voor zover dat noodzakelijk is voor het doel, bedoeld in artikel

47 en verder uitgewerkt in de artikelen 52 en 53. Ook de privaatrechtelijke deelnemers zijn daartoe gerechtigd.

De reden voor de tweedeling tussen publiekrechtelijke deelnemers of overheidsinstanties enerzijds en privaatrechtelijke deelnemers anderzijds, is gelegen in de toekenning van de gezamenlijke verwerkingsverantwoordelijkheid als bedoeld in artikel 26 van de AVG alsmede in de verduidelijking van de positie van private partijen die deelnemen aan een samenwerkingsverband, zoals een Zorg- en Veiligheidshuis. In navolging van de Afdeling advisering van de Raad van State meent de regering dat de primaire verantwoordelijkheid voor de persoonsgegevensverwerking in het kader van het samenwerkingsverband moet berusten bij de publiekrechtelijke deelnemers of overheidsinstanties en niet bij de private deelnemers. Het doel van het samenwerkingsverband is immers het behartigen van een zwaarwegend algemeen publiek belang en de publiekrechtelijke deelnemers of overheidsinstanties dragen – vanuit hun onderscheidenlijke wettelijke taken en bevoegdheden die eveneens in het algemeen publiek belang zijn toegekend – daar de primaire verantwoordelijkheid voor. Het voor de uitoefening van die wettelijke taken en bevoegdheden verantwoordelijke bestuursorgaan, kan daar op worden aangesproken door het volksvertegenwoordigend orgaan. De rechten en plichten die uiting geven aan deze verantwoordelijkheid en die zijn verbonden aan de gezamenlijke gegevensverwerking die op grond dit wetsvoorstel, in het bijzonder deze paragraaf, mogelijk worden gemaakt, worden om voornoemde redenen dan ook voorbehouden aan de publiekrechtelijke deelnemers of overheidsinstanties, bedoeld in het eerste lid. De gezamenlijke verwerkingsverantwoordelijkheid als bedoeld in artikel 26 van de AVG voor de gezamenlijke verwerking van gegevens wordt daartoe exclusief toegekend aan de publiekrechtelijke deelnemers of overheidsinstanties (artikel 48, derde lid) .

Duidelijkheidshalve wordt opgemerkt dat de gezamenlijke verwerkingsverantwoordelijkheid als bedoeld in artikel 26 van de AVG betrekking heeft op de persoonsgegevensverwerking *in het kader van het samenwerkingsverband*. Elke deelnemer (of het bestuursorgaan waaronder de deelnemer ressorteert) blijft onverkort verwerkingsverantwoordelijke voor de persoonsgegevensverwerking die geschiedt bij de uitoefening van de wettelijke taken en bevoegdheden van die deelnemer, *dus buiten het kader van het samenwerkingsverband*. Dit wetsvoorstel brengt daarin geen wijzigingen aan.
De regering acht het essentieel dat private partijen wel moeten kunnen deelnemen aan de Zorg- en Veiligheidshuizen. Het tweede lid van dit artikel regelt de mogelijkheid voor private partijen om deelnemer te zijn aan het Zorg- en Veiligheidshuis, voor zover zij uitvoering geven aan wettelijke taken en bevoegdheden, of gemandateerd zijn om deze namens een bestuursorgaan uit te oefenen of daaraan gerelateerde noodzakelijke activiteiten verrichten, zoals bijvoorbeeld activiteiten in het kader van het verlenen van gezondheidszorg. Waar in deze paragraaf wordt geregeld dat persoonsgegevens mogen worden verwerkt, wordt geregeld dat alle deelnemers daartoe gerechtigd zijn voor zover hun betrokkenheid noodzakelijk is. Zoals hiervoor aangegeven, worden rechten en plichten die betrekking hebben op de verantwoordelijkheid voor de persoonsgegevensverwerking, voorbehouden aan de deelnemers, bedoeld in het eerste lid. Het gaat daarbij onder andere om de beslissing om persoonsgegevens te delen met een ander Zorg- en Veiligheidshuis en de beoordeling of een melding geschikt is voor casusoverleg.

Eerste lid

De publiekrechtelijke deelnemers of overheidsinstanties die op grond van het eerste lid worden aangewezen zijn:

De Raad voor de Kinderbescherming (onderdeel a)

De Raad voor de Kinderbescherming neemt deel voor de uitvoering van de wettelijke taken en bevoegdheden op grond van de artikelen 240, 255 en 257 van Boek 1 van het

Burgerlijk Wetboek, artikel 2:7 van het Besluit tenuitvoerlegging strafrechtelijke beslissingen, artikel 3.1 van de Jeugdwet en artikel 5, eerste lid, van de Wet opneming buitenlandse kinderen ter adoptie.

Bij complexe casuïstiek zoals toegelicht in paragraaf 4.4 kunnen ook jeugdigen betrokken zijn. Soms zijn zij zelf betrokken bij criminele activiteiten, overlast, of veiligheidsproblematiek. De persoonsgerichte aanpak is dan op hen gericht. Echter vaak zal de oorzaak mede gelegen zijn in de thuissituatie. Vaak is de Raad dan al betrokken vanuit haar wettelijke taken, of is het van belang de mogelijkheden die de Raad heeft om bij te dragen aan de persoonsgerichte aanpak mee te nemen. Ook kan het zijn dat de casus betrekking heeft op leden van een gezin, waarbij in het belang van de veiligheid van jeugdigen in het gezin, de betrokkenheid van de Raad noodzakelijk is. Er is dan afstemming noodzakelijk met partijen op het gebied van strafrecht, bestuursrecht, begeleiding en zorg- of hulpverlening. De WGS biedt een wettelijk kader om die samenwerking en afstemming in het Zorg- en Veiligheidshuis te kunnen organiseren. Dit wetsvoorstel wijst de Raad voor de Kinderbescherming daarom aan als deelnemer.

De Dienst Justitiële Inrichtingen (onderdeel b)

De Dienst Justitiële Inrichtingen, neemt deel voor de uitvoering van de wettelijke taken en bevoegdheden bij of krachtens artikel 2 van de Beginselenwet justitiële jeugdinrichtingen, artikel 2 van de de Beginselenwet verpleging ter beschikking gestelden, artikel 2 van de Penitentiaire beginselenwet en artikel 2.2, eerste en tweede lid, van de Wet forensische zorg en de daaruit voortvloeiende bevoegdheden.

Deelname van de Dienst Justitiële Instellingen is noodzakelijk omdat bij complexe casuïstiek zoals toegelicht in paragraaf 4.4 ook sprake kan zijn van detentie. Het komt regelmatig voor dat een persoon waarop een persoonsgerichte aanpak in het Zorg- en Veiligheidshuis van toepassing is, in detentie gaat. Dat wil echter geenszins zeggen dat de omstandigheden die hebben geleid tot de persoonsgerichte aanpak in het Zorg- en Veiligheidshuis veranderd zijn als betrokkene vrij komt. Ook kan het zijn dat het wenselijk is dat bepaalde elementen van de persoonsgerichte aanpak doorlopen tijdens de detentie. De WGS biedt een wettelijk kader om die samenwerking en afstemming in het Zorg- en Veiligheidshuis te kunnen organiseren. Dit wetsvoorstel wijst de DJI daarom aan als deelnemer.

De politie (onderdeel c)

De politie neemt deel voor de taak bedoeld artikel 3 van de Politiewet 2012 en de daaruit voortvloeiende bevoegdheden, de artikelen 5:3, 7:3, 8:1, 8:2, 8:10, 8:29, 8:31 en 13:3 van de Wet verplichte geestelijke gezondheidszorg en de artikelen 28b, tweede lid, en 33 van de Wet zorg en dwang psychogeriatrische en verstandelijk gehandicapte cliënten.
Personen waarbij sprake is van complexe problematiek zoals toegelicht in paragraaf 4.4 komen veelal als eerste in beeld bij de politie, bijvoorbeeld als veroorzakers van criminaliteit, overlast of veiligheidsproblematiek. Vaak is er dan sprake van achterliggende problematiek, die niet door de politie of een louter strafrechtelijke aanpak kan worden opgelost. Het Zorg- en Veiligheidshuis is dan het aangewezen samenwerkingsverband om tot een persoonsgerichte aanpak te kunnen komen, waarbij interventies uit het strafrecht, bestuursrecht, begeleiding, zorg en hulpverlening op elkaar zijn afgestemd. De WGS biedt een wettelijk kader om die samenwerking en afstemming in het Zorg- en Veiligheidshuis te kunnen organiseren. Dit wetsvoorstel wijst de politie daarom aan als deelnemer.

Het openbaar ministerie (onderdeel d)

Het openbaar ministerie neemt deel, voor de in artikel 124 van de Wet op de rechterlijke organisatie opgedragen taak en de daaruit voortvloeiende bevoegdheden, artikel 1:7, de hoofdstukken 5, 7 en 8 en artikel 13:3a van de Wet verplichte geestelijke gezondheidszorg, de artikelen 18c, 28a, 28b, 28c van de Wet zorg en dwang

psychogeriatrische en verstandelijk gehandicapte cliënten, de artikelen 2.3, 5.1, 5.2 en 6.2 van de Wet forensische zorg.

Bij complexe casuïstiek zoals toegelicht in paragraaf 4.4, zal in de meeste gevallen ook sprake zijn van strafrechtelijke maatregelen. Een persoonsgerichte aanpak vraagt dan om een goede afstemming tussen strafrechtelijke maatregelen, bestuursrechtelijke maatregelen, begeleiding, ondersteuning en zorg. Ook kan het zijn dat het openbaar ministerie tot de conclusie komt dat een louter strafrechtelijke aanpak niet tot duurzame verbetering zal leiden als er niet ook andere maatregelen of trajecten ingezet worden, bijvoorbeeld op het gebied van begeleiding, zorg- of hulpverlening. De WGS biedt een wettelijk kader om die samenwerking en afstemming in het Zorg- en Veiligheidshuis te kunnen organiseren. Dit wetsvoorstel wijst het openbaar ministerie daarom aan als deelnemer.

De burgemeester (onderdeel e)

De burgemeester neemt deel voor de uitvoering van zijn wettelijke taken en bevoegdheden op het terrein van de handhaving van de openbare orde bij of krachtens de artikelen 151d en 172 van de Gemeentewet, de Opiumwet of een gemeentelijke verordening en voor de uitvoering van zijn wettelijke taken en bevoegdheden bij of krachtens de Wet tijdelijk huisverbod en de artikelen 7:1, 7:2, 7:4, 8:1, 8:28, 8:29 en 8:32 van de Wet verplichte geestelijke gezondheidszorg, de artikelen 18a, 18c, 29 tot en met 36 van de Wet zorg en dwang psychogeriatrische en verstandelijk gehandicapte cliënten.

De burgemeester is verantwoordelijk voor de handhaving van de openbare orde en veiligheid in de gemeente. In die hoedanigheid heeft de burgemeester o.a. bevoegdheden om bestuurlijke maatregelen in te zetten onder andere op grond van de bovengenoemde wetten. Bij complexe casuïstiek zoals toegelicht in paragraaf 4.4, is sprake van criminaliteit, overlast of veiligheidsproblematiek. De inzet van bestuurlijke maatregelen in aanvulling op andere interventies en trajecten op het gebied van begeleiding of zorg- of hulpverlening kan dan noodzakelijk zijn, onder andere om de veiligheid van betrokkene en zijn omgeving op korte termijn te waarborgen. De WGS biedt een wettelijk kader om die samenwerking en afstemming in het Zorg- en Veiligheidshuis te kunnen organiseren. Dit wetsvoorstel wijst de burgemeester daarom aan als deelnemer.

Het college van burgemeester en wethouders (onderdeel f)

Het college van burgemeester en wethouders neemt deel voor de uitvoering van zijn wettelijke taken en bevoegdheden bij of krachtens artikel 2.1.1, eerste lid, artikel 2.1.7, 2.3.1 tot en met 2.3.6, de artikelen 2.3.9, 2.3.10 en 2.4.1 van de Wet maatschappelijke ondersteuning 2015, de artikelen 2.3 en 2.4 van de Jeugdwet, artikel 7.1 van de Participatiewet, artikel 3 van de Wet gemeentelijke schuldhulpverlening, artikel 16 van de Leerplichtwet en de taken, bedoeld in de artikelen 5:1, 5:2, 5:16, 8:31 van de Wet verplichte geestelijke gezondheidszorg en artikel 28c van de Wet zorg en dwangpsychogeriatrische en verstandelijk gehandicapte cliënten.
Bij complexe casuïstiek zoals toegelicht in paragraaf 4.4, is er veelal sprake van achterliggende problematiek in het zorg- en sociaal domein. Verbetering van de situatie vraagt dan onder andere inzet van voorzieningen uit die domeinen, in aanvulling op de inzet van interventies uit strafrecht of bestuursrecht. Veelal zullen er ook al voorzieningen uit het gebied van zorg en of sociaal domein zijn ingezet, maar is de afstemming met andere domeinen onvoldoende. Het college van burgemeester en wethouders is in de gemeente verantwoordelijk voor wettelijke taken in het sociaal domein, onder andere op het gebied van de Jeugdwet, Participatiewet, Wet maatschappelijke ondersteuning 2015 en de Wet gemeentelijke schuldhulpverlening. Onder de collegetaken op grond van de Wet maatschappelijke ondersteuning 2015, valt onder andere de inzet van bemoeizorg. Ook heeft het college een taak in het kader van de Wet verplichte geestelijke gezondheidszorg en de Leerplichtwet, en heeft zij een rol bij de re-integratie van ex-gedetineerden. Met de decentralisaties in het sociaal domein van 2015 heeft het college

bovendien een coördinerende rol toegekend gekregen in het sociaal domein. Het college is vanuit deze veelheid aan taken en haar coördinerende rol, in de meeste gevallen een onmisbare partij in de totstandkoming van een persoonsgerichte aanpak. Dit wetsvoorstel biedt een wettelijk kader om de samenwerking en afstemming met andere partijen in het Zorg- en Veiligheidshuis te kunnen organiseren. Dit wetsvoorstel wijst het college van burgemeester en wethouders daarom aan als deelnemer.

Een instelling voor gemeentelijke gezondheidsdienst (GGD, onderdeel g)

Een instelling voor gemeentelijke gezondheidsdienst neemt deel voor het in opdracht van het college van burgemeester en wethouders uitoefenen van de wettelijke taken bij of krachtens de Wet publieke gezondheid en de artikelen 1.1.1 en 2.1.1, eerste lid, van de Wet maatschappelijke ondersteuning 2015. Met deze laatste taken wordt gedoeld op de taken die een GGD uitvoert in opdracht van het college van burgemeester en wethouders bij het ondersteunen van de zelfredzaamheid en de participatie van personen met een beperking of met chronische psychische of psychosociale problemen. Het betreft hier o.a. taken in het kader van bemoeizorg.

Bij complexe casuïstiek zoals toegelicht in paragraaf 4.4, is er veelal sprake van achterliggende problematiek in het zorg- en sociaal domein. Verbetering van de situatie vraagt dan onder andere inzet van voorzieningen uit die domeinen, in aanvulling op de inzet van interventies uit strafrecht en of bestuursrecht. Bij complexe casuïstiek is er relatief vaak sprake van personen die zorg mijden. Vaak zijn deze mensen al bij de GGD in beeld, of is het noodzakelijk dat de bemoeizorg wordt ingezet in aanvulling op andere interventies om iemand te bewegen hulp te aanvaarden, en zo te werken aan een duurzame oplossing. De WGS biedt een wettelijk kader om de samenwerking en afstemming met andere partijen in het Zorg- en Veiligheidshuis te kunnen organiseren. Dit wetsvoorstel wijst de gemeentelijke gezondheidsdienst daarom aan als deelnemer.

Tweede lid

Een reclasseringsinstelling (onderdeel a)

Een door de Minister voor Rechtsbescherming op grond van artikel 4, eerste lid, van de Reclasseringsregeling erkende reclasseringsinstelling neemt deel voor de taken bedoeld in hoofdstuk 3 van de Reclasseringsregeling 1995.

Bij complexe casuïstiek zoals toegelicht in paragraaf 4.4 is er in de meeste gevallen ook sprake van strafbare feiten. Reclassering is dan betrokken op basis van haar publiekrechtelijke taken. Vaak is er al sprake van een persoonsgerichte aanpak in het Zorg- en Veiligheidshuis is, bijvoorbeeld bij veelplegers, of is het van belang dat zo'n aanpak tot stand komt om tot een duurzame verbetering te komen van de situatie. Afstemming tussen reclassering en andere partijen in het domein van strafrecht, bestuursrecht, begeleiding, zorg- en hulpverlening is dan noodzakelijk. De WGS biedt een wettelijk kader om die samenwerking en afstemming in het Zorg- en Veiligheidshuis te kunnen organiseren. Dit wetsvoorstel wijst de reclasseringsinstelling aan als deelnemer.

Een advies- en meldpunt huiselijk geweld en kindermishandeling (onderdeel b)

De door het college van burgemeester en wethouders op grond van artikel 4.1.1., eerste lid, van de Wet maatschappelijke ondersteuning 2015 aangewezen organisatie van een advies- en meldpunt huiselijk geweld en kindermishandeling (AMHK) neemt deel voor de taken bedoeld in artikel 4.1.1, tweede lid, van de Wet maatschappelijke ondersteuning 2015. De AMHK's opereren onder de naam Veilig Thuis.

Bij complexe casuïstiek zoals toegelicht in paragraaf 4.4 kan er ook sprake zijn van huiselijk geweld, misbruik van jeugdigen, of kindermishandeling. Soms is er sprake van daderschap, dat plaatsvindt onder dwang van huisgenoten of familieleden. Veilig Thuis heeft wettelijke taken en bevoegdheden om in dergelijke situaties de noodzakelijke

stappen te ondernemen. Als er in dergelijke situaties sprake is van problematiek of lopende interventies en trajecten op het gebied van strafrecht, bestuursrecht, begeleiding of zorg- of hulpverlening, is het van belang dat stappen in afstemming hiermee genomen worden. De WGS biedt een wettelijk kader om die samenwerking en afstemming in het Zorg- en Veiligheidshuis te kunnen organiseren. Dit wetsvoorstel wijst de reclasseringsinstelling aan als deelnemer.

Een gecertificeerde instelling o.g.v. de Jeugdwet (onderdeel c)

Een gecertificeerde instelling die in het bezit is van een certificaat of voorlopig certificaat als bedoeld in artikel 3.4 van de Jeugdwet neemt deel voor zover die een kinderbeschermingsmaatregel of jeugdreclassering als bedoeld in artikel 1.1 van de Jeugdwet uitvoert.

Bij complexe casuïstiek zoals toegelicht in paragraaf 4.4 kunnen ook jeugdigen betrokken zijn. Soms zijn zij zelf betrokken bij criminele activiteiten, overlast, of veiligheidsproblematiek. De persoonsgerichte aanpak is dan op hen gericht. Vaak zal de oorzaak echter mede gelegen zijn in de thuissituatie. In veel gevallen zal er sprake zijn van jeugdbeschermingsmaatregelen uitgevoerd door een gecertificeerde instelling zoals bedoeld in de Jeugdwet, terwijl er ook sprake is van een persoonsgerichte aanpak gericht, of is er een noodzaak om tot een persoonsgerichte aanpak te komen, waarbij jeugdbeschermingsmaatregelen afgestemd moeten worden met interventies en trajecten uit strafrecht, bestuursrecht, begeleiding of zorg- of hulpverlening. Dit wetsvoorstel biedt een wettelijk kader om die samenwerking en afstemming in het Zorg- en Veiligheidshuis te kunnen organiseren. Dit wetsvoorstel wijst de gecertificeerde instellingen zoals bedoeld in de Jeugdwet daarom aan als deelnemer.

Een instelling voor geestelijke gezondheidszorg (onderdeel d)

Een instelling voor geestelijke gezondheidszorg die taken uitvoert, of zorg verleent krachtens artikel 1.1 jo. 2.1 van de Wet verplichte geestelijke gezondheidszorg, artikel 1.1.1 van de Wet langdurig zorg, artikel 1.1 van de Wet forensische zorg, de artikelen 1 en 9 van de Wet zorg en dwang psychogeriatrische en verstandelijk gehandicapte cliënten, of jeugdhulp verleent op grond van artikel 1.1 van de Jeugdwet, of een behandeling uitvoert op grond van een behandelovereenkomst krachtens artikel 446 van Boek 7 van het Burgerlijk Wetboek, of maatschappelijke ondersteuning biedt op grond van de artikelen 1.1.1 en 2.1.1 van de Wet maatschappelijke ondersteuning 2015.
Specifiek met het oog op instellingen voor geestelijke gezondheidszorg regelt het tweede lid, onderdeel d, de mogelijkheid om ook deelnemer te zijn op grond van hun activiteiten die plaatsvinden in het kader van een behandelovereenkomst op grond van de Wet geneeskundige behandelovereenkomst, jeugdhulp die zij verlenen op grond van de Jeugdwet, of het bieden van maatschappelijke ondersteuning zoals bedoeld in artikel 1.1.1 van de Wet maatschappelijke ondersteuning 2015 aan personen die kampen met chronische psychische of psychosociale problemen, waaronder bemoeizorg.
De mogelijkheid voor de GGZ om ook op grond van deze taken deelnemer te kunnen zijn wordt noodzakelijk geacht, omdat bij de complexe casuïstiek zoals die aan de orde is in het Zorg- en Veiligheidshuis, relatief vaak sprake is van psychiatrische en of psychosociale problematiek, die mede ten grondslag ligt aan de strafbare feiten of openbare orde problemen. In dat kader zal er ook vaak sprake zijn van vrijwillige psychische zorg, zonder dat er direct sprake hoeft te zijn van zorg in het gedwongen kader. De betrokkenheid van de GGZ-instelling of behandelaar is in dergelijke situaties noodzakelijk om tot een goede afweging te komen omtrent de persoonsgerichte aanpak, de effectiviteit of juist contraproductiviteit van beoogde maatregelen, en de bijdrage die vanuit de zorg geleverd kan worden aan het voorkomen van strafbare feiten, recidive of veiligheidsproblemen. Medewerkers van een GGZ-instelling die betrokken zijn bij de behandeling van patiënten zijn op grond van hun beroep gehouden aan zeer stringente geheimhoudingsverplichtingen zoals vastgelegd in de Wgbo, de Wet BIG en de Jeugdwet. Dat betekent dat gegevens die zij in het kader van bijvoorbeeld een casus in het ZVH ontvangen uitsluitend gebruikt mogen worden voor zover dat in het kader van de

1912034 02691

behandeling van betrokkene noodzakelijk is en voor zover er geen andere geheimhoudingsverplichtingen op deze gegevens rusten. Het is bijvoorbeeld niet toegestaan dat de behandelaar of de GGZ-instelling waar deze werkzaam is deze gegevens gebruikt voor andere doeleinden, of verstrekt aan derden. Dat is alleen mogelijk met toestemming van de betrokkene, of als er sprake is van een van de andere uitzonderingsgronden in de Wgbo, Wet BIG of de Jeugdwet. Deze vertrouwelijkheid wordt gewaarborgd door tuchtrecht dat rust op de behandelaar. Omwille van de inhoudelijke noodzaak, en de reeds aanwezig zijnde wettelijke waarborgen voor de vertrouwelijkheid van de gegevens in het kader van het beroepsgeheim, acht de regering het aanvaardbaar een GGZ-instelling de mogelijkheid te geven om deel te kunnen nemen op basis van haar civielrechtelijke betrokkenheid bij een patiënt. Dit wetsvoorstel creëert een wettelijk kader om voorkomende gevallen samenwerking en afstemming tussen de GGZ en partijen op het gebied van strafrecht, bestuursrecht, begeleiding of zorg- of hulpverlening in het Zorg- en Veiligheidshuis te kunnen organiseren. Dit wetsvoorstel wijst instellingen voor geestelijke gezondheidszorg daarom aan als deelnemer.

Een instelling voor maatschappelijke dienstverlening (onderdeel e)

Onderdeel e wijst als deelnemer aan een instelling die in opdracht van het college van burgemeester en wethouders taken verricht neemt deel ter uitvoering van de artikelen 2.3.1 tot en met 2.3.5 van de Wet maatschappelijke ondersteuning 2015, de artikelen 2.3 en 2.4 van de Jeugdwet, de Participatiewet en artikel 3 van de Wet gemeentelijke schuldhulpverlening. Het gaat hier om de taken van het college van burgemeester en wethouders in het kader van de toeleiding naar voorzieningen op grond van de genoemde sociaal domeinwetten. Deze worden in de praktijk veelal worden uitgevoerd door sociale wijkteams als onderdeel van een private stichting of samenwerkingsverband. Voor zover deze instellingen uitvoering geven aan taken van het college van burgemeester en wethouders in het sociaal domein zijn de redenen om de mogelijkheid te creëren een dergelijke organisatie deel te kunnen laten nemen aan de Zorg- en Veiligheidshuizen dezelfde als voor het college van burgemeester en wethouders, zoals toegelicht bij het eerste lid, onderdeel f.

Het is gelet op de hoeveelheid deelnemers die onder onderdeel e kunnen vallen binnen het territoriale werkgebied van een Zorg- en Veiligheidshuis alsook het verschil in betrokkenheid bij casussen aan het college van burgemeester en wethouders te bepalen welke daarvan als vaste deelnemer worden aangewezen of als derden incidenteel worden uitgenodigd op grond van artikel 52, negende lid.

Taken van deelnemers met betrekking tot de Wet verplichte geestelijke gezondheidszorg, Wet zorg en dwang psychogeriatrische en verstandelijk gehandicapte cliënten

Instellingen voor geestelijke gezondheidszorg en gehandicaptenzorg hebben ingevolge de Wet verplichte geestelijke gezondheidzorg en de Wet zorg en dwang psychogeriatrische en verstandelijk gehandicapte cliënten de bevoegdheid om verplichte of onvrijwillige zorg in te zetten. In het traject naar verplichte of onvrijwillige zorg hebben deze wetten ook taken toegewezen aan de burgemeester, het college van burgemeester en wethouders, het OM en de politie. Om die reden zijn ook bij deze deelnemers hun taken in het kader van deze wetten benoemd. Het uitgangspunt van de Wet verplichte geestelijke gezondheidzorg en de Wet zorg en dwang psychogeriatrische en verstandelijk gehandicapte cliënten is dat verplichte of onvrijwillige zorg wordt ingezet als ultimum remedium. In gevallen waar de burger in aanraking is gekomen met het strafrecht en tevens zorg noodzakelijk is, kan het van belang zijn om niet alleen te bekijken wat er in een vrijwillig kader mogelijk is, maar ook welke mogelijkheden een onvrijwillig kader zouden bieden. Het kan ook blijken dat reeds ingezette verplichte of onvrijwillige zorg onvoldoende is en wellicht het strafrecht een (aanvullende) oplossing kan bieden. Dan kan overleg in een Zorg- en Veiligheidshuis een mogelijkheid bieden om gezamenlijk te zoeken naar de meest passende oplossing. Voor de besluitvorming over toepassing van verplichte of onvrijwillige zorg worden de bepalingen van de Wet verplichte geestelijke gezondheidszorg en de Wet zorg en dwang psychogeriatrische en verstandelijk

gehandicapte cliënten gevolgd. Het Zorg- en Veiligheidshuis treedt niet in de besluitvorming van de afzonderlijke deelnemers.

Derde lid

Zoals hiervoor aangegeven wordt in afwijking van artikel 4, eerste lid, geregeld dat uitsluitend de deelnemers, bedoeld in het eerste lid, gezamenlijke verwerkingsverantwoordelijken zijn als bedoeld in artikel 26, eerste lid, van de Algemene verordening gegevensbescherming voor de verwerking van gegevens door de Zorg- en Veiligheidshuizen. De reden voor de tweedeling tussen publiekrechtelijke deelnemers of overheidsinstanties enerzijds en privaatrechtelijke deelnemers anderzijds, is gelegen in de toekenning van de gezamenlijke verwerkingsverantwoordelijkheid als bedoeld in artikel 26 van de AVG alsmede in de verduidelijking van de positie van private partijen die deelnemen aan een samenwerkingsverband, zoals een Zorg- en Veiligheidshuis. Artikel 4, tweede tot en met vierde lid, zijn van overeenkomstige toepassing.

Vierde lid

Het vierde lid schrijft voor dat bij of krachtens algemene maatregel nadere regels kunnen worden gesteld over de wettelijke taken en bevoegdheden van de deelnemers waarvoor gegevens kunnen worden verwerkt binnen de Zorg- en Veiligheidshuizen. In de lagere regelgeving wordt omwille van de afbakening van de reikwijdte van het wetsvoorstel – voor zover dat niet reeds volgt uit dit artikel – bepaald voor welke wettelijke taken en bevoegdheden persoonsgegevens kunnen worden verwerkt binnen het Zorg- en Veiligheidshuis. Ook biedt het vierde lid de mogelijkheid om rekening te houden met wijziging of verschuiving van wettelijke taken en bevoegdheden waarvoor de deelnemers persoonsgegevens moeten kunnen verwerken met het oog op het doel, bedoeld in artikel 47.

Vijfde lid

Het vijfde lid regelt dat bij of krachtens algemene maatregel van bestuur andere overheidsorganen of overheidsinstanties en private partijen kunnen worden aangewezen als deelnemer voor zover dat noodzakelijk is voor het doel als bedoeld in artikel 47. Gelet op de opgave van de Zorg- en Veiligheidshuizen kan het nodig zijn in de toekomst op structurele basis andere of nieuwe partijen te betrekken. Het vijfde lid beoogt de praktijk hierin enige flexibiliteit te bieden doordat in een dergelijk geval niet eerst een wetswijziging nodig is. Uiteraard zal bij de toevoeging van deelnemers worden getoetst of structurele deelname noodzakelijk is met het oog op het doel dat Zorg- en Veiligheidshuizen nastreven en zullen alle rechten en plichten die uit dit wetsvoorstel voortvloeien onverkort op nieuwe deelnemers van toepassing zijn. Bij de toevoeging van publiekrechtelijke deelnemers of overheidsinstanties enerzijds en private deelnemers anderzijds, geldt onverkort de systematiek van het eerste en tweede lid.

Artikel 49 (onderlinge gegevensuitwisseling)

Artikel 49 maakt het mogelijk dat Zorg- en Veiligheidshuizen onderling gegevens kunnen uitwisselen voor zover dat noodzakelijk is voor het doel, bedoeld in artikel 47. Dit kan bijvoorbeeld noodzakelijk zijn omdat een betrokkene verhuist naar een andere regio, terwijl de redenen om zijn casus te behandelen in het Zorg- en Veiligheidshuis nog steeds aanwezig zijn. Ook komt het voor dat een betrokkene feitelijk in meerdere regio's tegelijk woont, bijvoorbeeld als er sprake is van gebroken gezinnen, of als betrokkene geen vaste woon- of verblijfplaats heeft. In dergelijke situaties kan het voorkomen dat een betrokkene in beeld komt bij meerdere Zorg- en Veiligheidshuizen, of dat het voor een goed aanpak van de problematiek noodzakelijk is dat er samenwerking tot stand komt tussen deelnemers van meerdere Zorg- en Veiligheidshuizen. Gelet op het overkoepelende doel van artikel 47 moet de gegevensuitwisseling tussen Zorg- en Veiligheidshuizen in dergelijke situaties mogelijk zijn en beschouwd worden als vallend binnen het doel van artikel 47.

Daarbij wordt onderscheid gemaakt tussen twee vormen van gegevensuitwisseling. De eerste vorm is de check op bekendheid. Dit betekent dat indien iemand in beeld komt bij een Zorg en Veiligheidshuis, het Zorg- en Veiligheidshuis kan checken of deze persoon ook al bekend is bij een ander Zorg- en Veiligheidshuis. De tweede vorm van gegevensuitwisseling betreft de uitwisseling van inhoudelijke casusinformatie.

Eerste lid
Het eerste lid regelt de mogelijkheid voor de deelnemers, bedoeld in artikel 48, eerste lid, van een Zorg- en Veiligheidshuis dat persoonsgegevens verwerkt ter uitvoering van de activiteiten, bedoeld in artikel 47a, om ter vaststelling of een betrokkene bekend is bij een ander Zorg- en Veiligheidshuis, identificerende en contactgegevens van die betrokkene uit te wisselen met de deelnemers, bedoeld in artikel 48, eerste lid, van een ander Zorg- en Veiligheidshuis voor zover dat noodzakelijk is voor het doel, als bedoeld in artikel 47.
De check op bekendheid bij een ander Zorg- en Veiligheidshuis kan bijvoorbeeld plaatsvinden zodra een persoon wordt aangemeld volgens artikel 52, eerste lid. Deze check is noodzakelijk om te voorkomen dat meerdere Zorg- en Veiligheidshuizen onafhankelijk van elkaar een persoonsgerichte aanpak ontwikkelen, met het risico van stapeling van trajecten en interventies, en elkaar tegenwerkende aanpakken. Daarnaast is het feit dat iemand wordt aangemeld bij een Zorg- en Veiligheidshuis, terwijl er ook al een persoonsgerichte aanpak loopt of recent heeft gelopen bij een ander Zorg- en Veiligheidshuis een uitermate relevant gegeven in de beoordeling van de casus.
De check op bekendheid kan ook plaats vinden in het kader van de beoordeling of iemand op de lijst van geprioriteerde casussen geplaatst dient te worden volgens artikel 53, tweede lid.

Voor de check op bekendheid hoeven slechts zeer beperkt persoonsgegevens verwerkt worden. Het gaat dan om identificerende en contactgegevens enhet burgerservicenummer, de antwoordinformatie 'bekend of niet bekend', en indien 'bekend', de gegevens van het Zorg- en Veiligheidshuis waar betrokkene bekend is.

Tweede lid
Het tweede lid regelt de mogelijkheid om na het uitwisselen van identificerende en contactgegevens alsmede het burgerservicenummer inhoudelijke casusinformatie, namelijk andere gegevens, bedoeld in artikel 51, eerste lid, uit te wisselen tussen Zorg- en Veiligheidshuizen, indien de check op bekendheid daar aanleiding toe geeft. Indien uit de bekendheidscheck blijkt dat een betrokkene inderdaad reeds bekend is bij een ander Zorg- en Veiligheidshuis kan dit aanleiding zijn om contact op te nemen om tever kennen of het in het licht van de doelstelling van artikel 47 noodzakelijk is om tot nadere afstemming te komen tussen de Zorg- en Veiligheidshuizen.

Hierbij dient echter altijd een zorgvuldige afweging gemaakt te worden of en zo ja welke gegevens daarbij noodzakelijk zijn om uit te wisselen. Voorkomen moet namelijk worden dat er een *free flow van information* ontstaat tussen Zorg- en Veiligheidshuizen, waarbij de betrokkene, maar ook de bij een casus betrokken deelnemers geen zicht meer hebben op de verdere verwerking van hun gegevens bij een ander Zorg- en Veiligheidshuis. Uitwisseling van inhoudelijke casusinformatie tussen Zorg- en Veiligheidshuizen kan daarom uitsluitend na consultatie van de bij een casus betrokken deelnemers en met inachtneming van het gestelde in artikel 7, artikel 49, vierde lid, en artikel 50, derde lid. Artikel 7 bepaalt dat verstrekking van resultaten vanuit het samenwerkingsverband mogelijk is aan deelnemers of derden tenzij zwaarwegende belangen zich daar tegen verzetten onderscheidenlijk een deelnemer daartegen bezwaar heeft. Artikel 49, vierde lid, bepaalt dat het verstrekken van bijzondere persoonsgegevens en persoonsgegevens van strafrechtelijke aard van een Zorg- en Veiligheidshuis aan een ander Zorg- en Veiligheidshuis alleen mogelijk is als de deelnemer die de gegevens heeft ingebracht daarmee instemt. Artikel 50, derde lid, bepaalt dat deelnemers die gegevens inbrengen ten behoeve van de behandeling van een casus voorwaarden en beperkingen kunnen stellen aan de verdere verwerking van deze gegevens door andere deelnemers of derden.

Het is aan elk Zorg- en Veiligheidshuis zelf om een zorgvuldige procedure in te richten voor het uitwisselen van gegevens met een ander Zorg- en Veiligheidshuis, waarmee invulling gegevens wordt aan de beginselen van noodzaak, proportionaliteit en subsidiariteit uit de AVG, en om invulling te geven aan de voorwaarden van de artikelen 7, 49, vierde lid, en 50, derde lid.

Derde lid
Het derde lid regelt de mogelijkheid om inhoudelijke casusinformatie, namelijk gegevens als bedoeld in artikel 51, eerste lid, aan de deelnemers van een ander Zorg- en Veiligheidshuis te verstrekken tijdens de uitvoering van de activiteiten, bedoeld in artikel 47a, indien uit feiten en omstandigheden blijkt dat de verstrekking noodzakelijk is voor het doel als bedoeld in artikel 47. Hier kan bijvoorbeeld sprake van zijn in voorbeelden genoemd aan het begin van de toelichting op dit artikel. In formele zin gebeurt uitwisseling van gegevens tussen Zorg- en Veiligheidshuizen door uitwisseling tussen de deelnemers uit artikel 48, eerste lid, aangezien zij de gezamenlijke verwerkingsverantwoordelijken zijn. In praktische zin kan het gaan om uitwisseling van gegevens tussen deelnemers die bij een casus zijn betrokken.

Het Zorg- en Veiligheidshuis kan dan gericht contact opnemen met het Zorg- en Veiligheidshuis waarmee wordt samengewerkt, of waarheen overgedragen moet worden, om afspraken te maken over de over te dragen gegevens. Daarbij moet dezelfde zorgvuldigheid in acht genomen worden als hierboven toegelicht bij het tweede lid: uitwisseling van inhoudelijke casusinformatie tussen Zorg- en Veiligheidshuizen kan uitsluitend na consultatie van de bij een casus betrokken deelnemers en met inachtneming van het gestelde in artikel 7, artikel 49, vierde lid, en artikel 50, derde lid. Elk Zorg- en Veiligheidshuis zal een zorgvuldige procedure in moeten richten voor het uitwisselen van gegevens met een ander Zorg- en Veiligheidshuis, om te voldoen aan de hier boven genoemde voorwaarden van de AVG en deze wet.

Vierde lid
Indien toepassing wordt gegeven aan het tweede of derde lid, geldt daarbij als waarborg voor de fundamentele belangen van betrokkene dat de verstrekking van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard aan een ander Zorg- en Veiligheidshuis uitsluitend plaatsvindt nadat de partij of de partijen die deze persoonsgegevens aan het Zorg- en Veiligheidshuis heeft of hebben verstrekt, hiermee heeft of hebben ingestemd. Deze waarborg doet tevens recht aan de verantwoordelijkheid die elke deelnemer afzonderlijk heeft voor de rechtmatige verwerking van persoonsgegevens in het kader van de uitoefening van de taken en bevoegdheden van de deelnemer die deze gegevens verstrekt.

Artikel 50 (grondslag verwerking gegevens over gezondheid en het burgerservicenummer)

Eerste lid

Gelet op het doel, bedoeld in artikel 47, met het oog waarop Zorg- en Veiligheidshuizen gezamenlijk gegevens verwerken, is het noodzakelijk gegevens over gezondheid en het burgerservicenummer te verwerken. Zorg- en Veiligheidshuizen richten immers zich op complexe casuïstiek welke niet door één deelnemer of keten alleen kan worden opgelost. De aard van complexe casuïstiek, en het zwaarwegend maatschappelijk belang om tot een duurzame verbetering van de situatie te komen bij personen waarbij deze casuïstiek speelt, is toegelicht in paragraaf 4.4 van deze memorie. Het betreft casuïstiek waarbij problemen op het gebied van criminaliteit, overlastgevend gedrag en veiligheidsrisico's, mede hun oorzaak vinden in zorgproblematiek en sociale problematiek, zoals bijvoorbeeld psychische problemen, schulden, en of verslaving. Om bij dergelijke problematiek tot een goed inzicht van de situatie te komen, de achterliggende problematiek en persoonsgerichte aanpak die tot duurzame verbetering van de situatie kan leiden, moeten de verschillende ketens (strafrecht, bestuursrecht, zorg en sociaal) samen kunnen werken en hun interventies en trajecten kunnen afstemmen. De mogelijkheid tot de

gezamenlijke verwerking van persoonsgegevens, waaronder bijzondere persoonsgegevens, gegevens betreffende de gezondheid en strafrechtelijke gegevens is dan essentieel.
Artikel 50 heeft geen betrekking op persoonsgegevens van strafrechtelijke aard omdat reeds in de artikelen 5, 6 en 7 voor alle samenwerkingsverbanden is geregeld dat deze mogen worden verwerkt, zowel in de fase van verstrekking aan het samenwerkingsverband, verwerking binnen het samenwerkingsverband en verstrekking van de resultaten door het samenwerkingsverband.
De deelnemers mogen met het oog op het doel van artikel 47 gebruikmaken van het burgerservicenummer, bedoeld in artikel 1 van de Wet algemene bepalingen burgerservicenummer. Verstrekking van het burgerservicenummer aan het samenwerkingsverband is van belang om te kunnen waarborgen dat de te verwerken persoonsgegevens van de verschillende deelnemers betrekking hebben op dezelfde persoon. De deelnemers zoals benoemd in artikel 48 zijn allen reeds gehouden om het burgerservicenummer te verwerken op grond van hun eigen wettelijke taken en de wettelijke taken die zij uitoefenen namens een bestuursorgaan. Ook een GGZ-instelling is gehouden aan het gebruik van het burgerservicenummer op grond van het Besluit gebruik burgerservicenummer in de zorg.

Tweede lid
Het tweede lid stelt vast dat voor deelnemers waarop het wettelijk medisch beroepsgeheim van toepassing is op grond van de Wet geneeskundige behandelovereenkomst, de Wet op de beroepen in de individuele gezondheidszorg of de Jeugdwet bij het beoordelen van de verstrekking op grond van artikel 5, eerste lid, van gegevens over onder andere gezondheid, het medisch beroepsgeheim onverkort blijft gelden. Dat betekent dat zij gegevens over een betrokkene die zij in het kader van een behandeling hebben verkregen, uitsluitend aan een Zorg- en Veiligheidshuis verstrekken indien zij daarvoor uitdrukkelijke toestemming hebben verkregen van de betrokkene, behoudens de gevallen waarin enig wettelijk voorschrift een deelnemer verplicht gegevens te verstrekken of enig wettelijk voorschrift toestaat deze gegevens zonder uitdrukkelijke toestemming van betrokkene te verstrekken of deze verstrekking noodzakelijk is uit het oogpunt van goed hulpverlenerschap. Dit laatste verwijst naar het conflict van plichten zoals dat nader is uitgewerkt in beroepscodes, in het bijzonder in de richtlijn van de Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskunst (KNMG)[33]. Wettelijke beroepsgeheimen strekken zich uit tot gegevens die een hulpverlener in het kader van een behandeling ontvangt. Naast gegevens over gezondheid, beschikken hulpverleners over gegevens met betrekking tot de gezinssituatie, of de schoolsituatie. Het tweede lid van dit artikel heeft daarom betrekking op alle gegevens waarover een beroepsbeoefenaar beschikt op wie het wettelijk medisch beroepsgeheim van de Wet geneeskundige behandelovereenkomst, de Wet op de beroepen in de individuele gezondheidszorg of de Jeugdwet van toepassing is.

Derde lid
In het derde lid, is geregeld dat een deelnemer die op grond van de artikelen 5, eerste lid, de in artikel 5, tweede lid, genoemde bepalingen, of overeenkomstig artikel 50, tweede lid, gegevens verstrekt aan het Zorg- en Veiligheidshuis voorwaarden en beperkingen kan stellen aan het verstrekken van de resultaten aan deelnemers of derden op grond van artikel 7, eerste en tweede lid. Het komt de kwaliteit van het casusoverleg en de resultaten die daaruit voortvloeien ten goede als alle deelnemers de ruimte voelen om informatie in te brengen in de zekerheid dat zij te allen tijde grip kunnen houden op de verstrekking van resultaten aan andere deelnemers en aan derden. Die grip moet zich niet beperken tot alleen de bijzondere en strafrechtelijke gegevens, maar moet, mede gelet op de gegevens die overeenkomstig het tweede lid worden verstrekt, mogelijk zijn voor alle gegevens die deelnemers inbrengen. Het derde lid heeft daarmee een ruimer toepassingsbereik dan artikel 7, derde lid.

Artikel 51 (verstrekking van gegevens aan het samenwerkingsverband)

[33] KNMG-richtlijn "Omgaan met medische gegevens", KNMG 2020.

Eerste lid
Artikel 51, eerste lid, bepaalt welke categorieën gegevens, de deelnemers verstrekken aan het samenwerkingsverband met het oog op de activiteiten, bedoeld in artikel 47a.

Onderdeel a

Onderdeel a bepaalt dat over de betrokkene of betrokkenen waarop een melding als bedoeld in artikel 52 betrekking heeft dan wel die voldoet of voldoen aan de criteria voor plaatsing op de lijst met geprioriteerde casussen, bedoeld in artikel 53, eerste lid de volgende categorieën gegevens worden verstrekt.

- identificerende en contactgegevens;
- het burgerservicenummer;
- gegevens omtrent woonsituatie;
- financiële gegevens;
- inkomensgegevens;
- persoonsgegevens over gezondheid;
- persoonsgegevens van strafrechtelijke aard als bedoeld in artikel 8 en 13 van de Wet politiegegevens;
- persoonsgegevens van strafrechtelijke aard als bedoeld in de artikelen 8b, 39fa, en 51ca van de Wet justitiële en strafvorderlijke gegevens;
- gegevens betreffende relaties met gezinsleden en andere directe sociale contacten;
- gegevens inzake toezicht en handhaving alsmede getroffen bestuurlijke maatregelen of opgelegde beperkingen;
- gegevens over geïndiceerde en toegekende zorg of voorzieningen in het sociaal domein;
- gegevens over begeleiding, zorg en hulpverlening;

De Zorg- en Veiligheidshuizen behandelen met name casussen waarbij problemen op het gebied van criminaliteit, overlastgevend gedrag en veiligheidsrisico's mede hun oorzaak vinden in sociale en of zorgproblematiek. Welke problemen in een specifieke casus relevant zijn om mee te nemen in de analyse van de casus en de daarop gebaseerde persoonsgerichte aanpak, zal per casus verschillen. De behandeling van casussen in de Zorg- en Veiligheidhuizen is daarom altijd maatwerk, waarbij de aard van de problematiek van de persoon, en de aard van de problemen die daar het gevolg van zijn, leidend dienen te zijn bij de persoonsgerichte aanpak en de te verwerken gegevens. Dit betekent dat de categorieën van persoonsgegevens die potentieel aan de orde kunnen zijn in het Zorg- en Veiligheidshuis noodgedwongen vrijwel alle leefdomeinen van een persoon kunnen omvatten. Inperking van deze categorieën gegevens kan ertoe leiden dat onbedoeld aspecten buiten beeld blijven die achteraf wel noodzakelijk blijken te zijn voor een succesvolle persoonsgerichte aanpak. Hierdoor bestaat het risico dat problemen onnodig lang voort duren, of verergeren met alle gevolgen en risico's voor de persoon en de mensen in de omgeving waar hij woont, werkt en leeft die daarmee gepaard kunnen gaan. De waarborgen tegen een onnodige en onwenselijke inmenging in de levenssfeer van de betrokkene zullen daarom gevonden moeten worden in een zorgvuldige inrichting van het proces van casusbehandeling waarbij invulling gegeven dient te worden aan de beginselen van noodzaak, subsidiariteit en proportionaliteit van de AVG. Dit betekent onder andere dat per casus steeds op basis van de aard van de problematiek bekeken zal moeten worden welke gegevens noodzakelijk zijn om te verstrekken aan het Zorg- en Veiligheidshuis in het kader van de activiteiten van de artikelen 47a, 52 en 53, met het oog op het doel van artikel 47 van dit wetsvoorstel. In artikel 52 van dit wetsvoorstel wordt reeds invulling gegeven aan zo'n zorgvuldige inrichting. Zo dient er, indien een casus door een deelnemer wordt aangemeld, altijd een beoordeling plaats te vinden of de aanmelding in overeenstemming is met het doel van artikel 47. Alleen als dat zo is, kan een casus in behandeling worden genomen en kan verdere informatieverzameling plaats vinden. Daarnaast zullen de deelnemers in het Zorg- en Veiligheidshuis afspraken moeten maken hoe zij bij de uitvoering van de activiteiten in artikel 52 verder invulling geven aan de beginselen van noodzaak, subsidiariteit en proportionaliteit van de AVG, om zo de persoonlijke levenssfeer van de betrokkene te beschermen.

Met betrekking tot het opstellen van lijsten zoals bedoeld in artikel 47a, onder b, worden de te verwerken gegevens steeds beperkt door de objectieve criteria die door de deelnemers worden opgesteld voor plaatsing op de lijst.

Categorieën gegevens
Zoals hiervoor aangegeven is verstrekking van het burgerservicenummer aan het samenwerkingsverband van belang om te kunnen borgen dat de te verwerken persoonsgegevens van de verschillende deelnemers betrekking hebben op dezelfde persoon. De deelnemers zoals benoemd in artikel 48 zijn allen reeds gehouden om het burgerservicenummer te verwerken op grond van hun eigen wettelijke taken en de wettelijke taken die zij uitoefenen namens een bestuursorgaan. Ook een GGZ-instelling is gehouden aan het gebruik van het burgerservicenummer op grond van het Besluit gebruik burgerservicenummer in de zorg.
Onder persoonsgegevens van strafrechtelijke aard als bedoeld in de artikelen 8 en 13 van de Wet politiegegevens wordt onder meer verstaan het gebruik van een politiefoto en informatie over voertuigen.

Onder financiële gegevens en inkomenssituatie wordt onder meer verstaan de mogelijkheid om schulden van een persoon vast te stellen. Deze staan vaak centraal in de aanpak van een casus. Juist het ontbreken van zicht op de precieze financiële situatie is in de praktijk de reden dat een casus niet verder komt, moeizaam loopt, lang duurt.

Met gegevens omtrent geïndiceerde dan wel toegekende zorg, of voorzieningen in het sociaal domein wordt geduid op zorg of ondersteuning die een betrokkene ontvangt in de zin van de Wet langdurige zorg, of de Zorgverzekeringswet, respectievelijk de Wet maatschappelijke ondersteuning 2015, Jeugdwet, Participatiewet en de Wet gemeentelijke schuldhulpverlening. Met lopende trajecten op het gebied van zorg, hulp of ondersteuning wordt o.a. geduid op re-integratie-trajecten in het kader van de Participatiewet, of de Wet re-integratie ex-gedetineerden, of lopende schuldsaneringstrajecten. Het kan daarbij ook gaan om lopende trajecten in het kader van bemoeizorg.

Met gegevens inzake toezicht en handhaving alsmede getroffen bestuurlijke maatregelen of opgelegde beperkingen, worden onder andere bedoeld gegevens over maatregelen die getroffen zijn in het kader van de Wet verplichte geestelijke gezondheidszorg, of de Wet zorg en dwang psychogeriatrische en verstandelijk gehandicapte cliënten, maatregelen in het kader van de jeugdbescherming als bedoeld in de Jeugdwet, of tijdelijke huis- en/of gebiedsverboden. Ook maatregelen op het gebied van leerplicht kunnen hieronder vallen.

Onderdeel b

Onderdeel b bepaalt dat ter zake van natuurlijke personen uit de directe kring van betrokkene de volgende categorieën gegevens kunnen worden verstrekt

- identificerende en contactgegevens;
- gegevens omtrent woonsituatie;
- financiële gegevens;
- inkomensgegevens;
- persoonsgegevens over gezondheid;
- gegevens inzake toezicht en handhaving alsmede getroffen bestuurlijke maatregelen of opgelegde beperkingen;
- gegevens over geïndiceerde en toegekende zorg of voorzieningen in het sociaal domein;
- gegevens over begeleiding, zorg en hulpverlening.

Bij complexe casuïstiek zoals toegelicht in paragraaf 4.4 speelt ook vaak de omgeving van de betrokkene een rol. Vaak zal de oorzaak voor crimineel of overlastgevend gedrag of veiligheidsrisico's bijvoorbeeld mede gelegen zijn in de thuissituatie, of in het gedrag van een groep waarin een belangrijk deel van het leven van betrokkene zich afspeelt.

Voor een succesvolle persoonsgerichte aanpak is het dan belang om ook naar deze omgevingsfactoren te kunnen kijken en gegevens over deze personen uit de directe kring van betrokkene te kunnen verwerken. Zeker bij jeugdigen is het dan van belang om ook inzicht te hebben in strafrechtelijke en bestuursrechtelijke maatregelen en lopende trajecten op het gebied van begeleiding, zorg- en of hulpverlening bij de ouders of leden van het huishouden.

Bij de directe kring van betrokkene mogen alleen gegevens worden verwerkt van personen die in relatie staan tot de problematiek van de betrokkene. Dat kan gaan om leden van het huishouden die problemen hebben die bijdragen aan de problemen van de betrokkene. Het kan ook gaan om contacten bij criminele activiteiten zoals het netwerk op straat, mededaders, medeleden van een mogelijke jeugdgroep of fluïde crimineel netwerk. Hiernaast kan het ook gaan om broertjes of zusjes uit huishoudens die risico lopen om door betrokkene in de criminaliteit te worden betrokken. Indien na het casusoverleg geen betrokkenheid of ernstige risico's daarop vastgesteld kunnen worden dienen alle persoonsgegevens te worden vernietigd.

Onderdeel c

Ter zake van medewerkers van deelnemers en medewerkers van andere instanties, overheidsorganen of instellingen die betrokken zijn bij de begeleiding, zorg- en hulpverlening van betrokkene is het noodzakelijk om binnen het samenwerkingsverband hun identificerende en contactgegevens te kunnen verwerken.

Tweede lid

Het tweede lid, bepaalt dat bij of krachtens algemene maatregel van bestuur nadere regels worden gesteld over de categorieën van gegevens, bedoeld in het eerste lid en de bronnen van waaruit die gegevens afkomstig zijn. In deze bepaling is een gelaagdheid beoogd van de beschrijving van de categorieën gegevens die de Zorg- en Veiligheidshuizen op grond van deze paragraaf verwerken. De regering kiest ervoor de categorieën gegevens in het wetsvoorstel te benoemen en om de nadere concretisering daarvan en de bronnen van waaruit de gegevens afkomstig te zijn bij lagere regelgeving vast te stellen. Op deze manier wordt recht gedaan aan het uitgangspunt dat bij wet in formele zin moet worden vastgelegd ter zake van welke gegevens betrokkene kan verwachten dat die ten aanzien van zijn persoon worden verwerkt in het kader van het samenwerkingsverband.

Artikel 52 (Activiteit casusoverleg)

Eerste tot en met zesde lid
In artikel 52, eerste tot en met zesde lid, wordt de grondslag gecreëerd voor de verwerking van gegevens in het kader van de activiteit casusoverleg zoals beschreven in de toelichting bij artikel 47a, onderdeel a.
In deze bepaling wordt het stapsgewijze proces voor de verwerking van persoonsgegevens en andere relevante gegevens in aanloop naar, tijdens en de afsluiting van het casusoverleg vastgelegd. Zoals gesteld in de toelichting op artikel 48, betekent het feit dat een organisatie is aangewezen als deelnemer niet dat deze ook standaard betrokken zal zijn bij elke casus die in het kader van dit artikel wordt behandeld. Dat zou immers in strijd is met de beginselen van noodzaak, subsidiariteit en proportionaliteit. De behandeling van casussen, de betrokkenheid van deelnemers of derden, en de te verwerken gegevens zijn altijd maatwerk. De deelnemers aan het Zorg- en Veiligheidshuis zullen daarom afspraken moeten maken hoe zij bij de uitvoering van de in dit artikel geschetste stappen invulling geven aan dat maatwerk, en aan de beginselen van noodzaak, subsidiariteit en proportionaliteit van de AVG, om zo de betrokkene te beschermen tegen onnodige verwerking en verspreiding van zijn gegevens. Het eerste tot en met zesde lid beschrijven de afzonderlijke stappen in het proces:

1) een deelnemer kan een casus aanmelden wanneer deze naar zijn oordeel verband houdt met het doel, bedoeld in artikel 47 (eerste lid).

2) Daarna maken de deelnemers, bedoeld in artikel 48, eerste lid, een zorgvuldige beoordeling of deze melding inderdaad in overeenstemming is met het doel als bedoeld in artikel 47 (tweede lid).
3) Pas wanneer de melding naar oordeel van de deelnemers, bedoeld in artikel 48, eerste lid, in overeenstemming is met het doel, bedoeld in artikel 47, kunnen de deelnemers, overgaan tot verzameling en uitwisseling van en samenvoeging met andere relevante gegevens die beschikbaar zijn bij andere deelnemers (derde lid). De formele bevoegdheid om over te gaan tot deze stap ligt bij de deelnemers zoals bedoeld in artikel 48, eerste lid, aangezien zij optreden als gezamenlijke verwerkingsverantwoordelijken voor de Zorg- en Veiligheidshuizen. Dit laat echter onverlet dat in deze stap ook deelnemers, zoals bedoeld in artikel 48, tweede lid, bij de gegevensuitwisseling kunnen worden betrokken. Gegevensuitwisseling met deze deelnemers is in deze stap van het proces noodzakelijk, bijvoorbeeld om zicht te krijgen of er sprake is van actuele of recentelijke betrokkenheid bij de persoon op wie de casus betrekking heeft, en de aard van die betrokkenheid. Die informatie is cruciaal om tot een goede beoordeling te komen welke van de deelnemers zoals bedoeld in artikel 48, tweede lid, betrokken moet worden bij de verdere behandeling van de casus. Dit derde lid beoogt nadrukkelijk ook een grondslag te creëren voor de gegevensuitwisseling met deze deelnemers. Om diezelfde reden is het mogelijk dat in deze stap derden bevraagd worden om te kunnen bepalen of het noodzakelijk is hen te betrekken bij de verdere behandeling van de casus. Bij het bevragen en de verdere verwerking van persoonsgegevens zullen daarbij de beginselen van noodzaak, subsidiariteit en proportionaliteit in acht genomen moeten worden.
4) De deelnemers, bedoeld in artikel 48, eerste lid, beoordelen vervolgens welke deelnemers met het oog op het doel van artikel 47 moeten worden betrokken bij de behandeling van de casus en daarbij gegevens mogen verwerken (vierde lid). Ook beoordelen zij of, en zo ja welke derden incidenteel bij de casus betrokken moeten worden. De mogelijkheid tot het betrekken van incidentele derden is expliciet geregeld in het negende lid van dit artikel. Niet alle deelnemers worden automatisch betrokken: er wordt een zorgvuldige afweging gemaakt welke deelnemers moeten worden betrokken gelet op hun onderscheidenlijke taken en bevoegdheden. Hierdoor wordt de gezamenlijke verwerking beperkt tot die deelnemers wier deelname gelet op het doel van artikel 47 daadwerkelijk noodzakelijk is. In formele zin zijn het de deelnemers zoals bedoeld in artikel 48, eerste lid, die beoordelen welke deelnemers en eventueel derden bij de casus moeten worden betrokken, aangezien zij optreden als gezamenlijke verwerkingsverantwoordelijken voor de Zorg- en Veiligheidshuizen. Dit laat echter onverlet dat zij in deze beoordeling ook het oordeel of advies van de deelnemers zoals bedoeld in artikel 48, tweede lid kunnen betrekken.
5) Wanneer het casusoverleg plaatsvindt kunnen de betrokken deelnemers overgaan tot het bespreken van de reeds verzamelde informatie en voor zover noodzakelijk verder verzamelen en uitwisselen van en samenvoegen met andere relevante gegevens. Indien dat naar het oordeel van de deelnemers noodzakelijk is met het oog op het doel van artikel 47, kunnen zij afspraken maken over de interventies, begeleiding, hulp of zorg die ten aanzien van een betrokkene kunnen of moeten worden ingezet (vijfde lid). Tijdens het overleg bepalen deelnemers zelf of, en zo ja welke gegevens zij nader noodzakelijk achten om in te brengen met het oog op de doelstelling van artikel 47.
6) Indien de deelnemers afspraken hebben gemaakt over interventies die ten aanzien van een betrokkene worden ingezet, kunnen de betrokken deelnemers gegevens verwerken die met het oog op het doel van artikel 47 noodzakelijk zijn voor de uitvoering van hun eigen aandeel, de evaluatie en zo nodig het bijstellen van die afspraken alsmede voor het overleggen over afsluiting van de casus (zesde lid). Bij deze stap zal een zorgvuldige afweging plaats moeten vinden over de gegevens die elke deelnemer nodig heeft voor het uitvoeren van zijn aandeel in de afspraken. Daarnaast zal bij deze stap rekening moeten worden gehouden met artikel 7, derde lid, en artikel 50, derde lid. Artikel 7, derde lid, bepaalt dat bijzondere persoonsgegevens, en persoonsgegevens van strafrechtelijke aard

slechts vanuit het samenwerkingsverband aan derden kunnen worden verstrekt nadat de deelnemer die deze gegevens aan het samenwerkingsverband heeft verstrekt daarmee instemt. Artikel 50, derde lid, bepaalt dat elke deelnemer die gegevens aan het Zorg- en Veiligheidshuis verstrekt voorwaarden en beperkingen kan stellen aan de verdere verwerking van deze gegevens door andere deelnemers of derden.

Zevende lid
In het zevende lid is bepaald dat bij de verwerking van gegevens, bedoeld in het eerste tot en met zesde lid, de deelnemers ten aanzien van betrokkene en natuurlijke personen uit de directe kring van betrokkene de categorieën gegevens verwerken, bedoeld in artikel 51, eerste lid, onderdelen a en b.

Achtste lid
In het achtste lid is als aanvullende waarborg op de waarborgen uit artikel 8 bepaald dat de persoonsgegevens die in de casus zijn opgenomen, worden afgeschermd totdat de persoonsgegevens worden vernietigd, geanonimiseerd of verwijderd zoals bedoeld in artikel 8, zevende lid, eerste volzin. Met deze bepaling wordt veiliggesteld dat bij afsluiting van een casus de daarin opgenomen persoonsgegevens binnen zes maanden na afsluiting van de casus niet meer kunnen worden geraadpleegd of gebruikt in afwachting van vernietiging, anonimisering of verwijdering. Het is dan nog wel zichtbaar dat de casus in het Zorg- en Veiligheidshuis in behandeling is geweest, maar deelnemers kunnen niet meer bij de overige gegevens. Indien zich vóór de datum van vernietiging, anonimisering of verwijdering, omstandigheden voordoen die het noodzakelijk maken om de casus te heropenen, dan kan de afscherming worden opgeheven, in overeenstemming met artikel 8, zevende lid, tweede volzin. In overleg met de deelnemers die gegevens hebben verstrekt ten behoeve van de oorspronkelijke casus, kunnen gegevens die noodzakelijk zijn voor de hernieuwde casus opnieuw gebruikt worden.

In praktijk zal dit leiden tot twee mogelijkheden. De eerste is dat de oorspronkelijke casus wordt heropend, waarbij alle beschikbare gegevens nog steeds relevant blijken te zijn. Indien alle deelnemers daarmee instemmen komen de gegevens weer beschikbaar voor de heropende casusbehandeling (hernieuwde verwerking, in de zin van artikel 8, zevende lid, tweede volzin). De termijn van maximaal vijf jaar uit artikel, zevende lid,eerste volzin, begint dan opnieuw te lopen vanaf de datum van heropening. Indien een deelnemer aangeeft zijn eerder verstrekte gegevens niet noodzakelijk te achten voor de heropende casus, dan worden deze verwijderd.
De tweede mogelijkheid is dat er weliswaar sprake is van een casus rondom eenzelfde persoon, maar feiten en omstandigheden rond de persoon dusdanig gewijzigd zijn, dat er feitelijk sprake is van een nieuwe casus, waarbij geen, of slechts een klein deel van de beschikbare gegevens nog relevant lijkt te zijn. In dat geval ligt het voor de hand dat er een nieuwe casus wordt aangemaakt en slechts het kleine deel van de nog relevante gegevens wordt hergebruikt voor de nieuwe casus voor zover de deelnemers die deze gegevens hebben verstrekt daarmee instemmen. Op de gegevens die zijn verstrekt ten behoeve van de 'oude' casus blijft de termijn van maximaal vijf jaar uit artikel 8, zevende lid, eerste volzin van kracht, gerekend vanaf de datum van eerste verwerking ten behoeve van de oude casus. Voor de gegevens ten behoeve van de nieuwe casus wordt de termijn van maximaal vijf jaar gerekend vanaf de eerste datum van verwerking ten behoeve van de nieuwe casus.

De kern van deze werkwijze is dat er steeds een afweging plaatsvindt omtrent de gegevens die noodzakelijk zijn in het geval van een heropende of nieuwe casus rond dezelfde persoon. Alleen op die manier kan invulling worden gegeven aan de beginselen van noodzaak, subsidiariteit en proportionaliteit van de AVG, en aan de bescherming van de persoonlijke levenssfeer van de betrokkene. Het is aan de deelnemers in de Zorg- en Veiligheidshuizen om afspraken te maken hoe zij hier in de praktijk vorm aan geven.

Afgeschermde gegevens in relatie tot de uitwisseling met andere Zorg- en Veiligheidshuizen

In artikel 49 zijn regels gesteld ten aanzien van de mogelijkheid om gegevens uit te wisselen tussen Zorg- en Veiligheidshuizen. Indien gegevens op basis van artikel 52, achtstezijn afgeschermd, maar nog wel zichtbaar is dat een persoon in een Zorg- en Veiligheidshuis is behandeld, betekent dit dat deze gegevens ook beschikbaar zijn in het kader van een zogeheten 'check op bekendheid' door een ander Zorg- en Veiligheidshuis. Een ander Zorg- en Veiligheidshuis kan dus zien of een persoon bij een ander Zorg- en Veiligheidshuis in behandeling is geweest, tot het moment dat de gegevens daadwerkelijk zijn vernietigd, geanonimiseerd of verwijderd op basis van artikel 8, zevende lid,eerste volzin.

Of het feit dat een persoon in beeld komt bij een ander Zorg- en Veiligheidshuis ook leidt tot het beschikbaar stellen van overige gegevens uit de casus ten behoeve van casusbehandeling in het andere Zorg- en Veiligheidshuis, is ter beoordeling aan de bij de casus betrokken deelnemers en met name de de deelnemers die de gegevens oorspronkelijk hebben verstrekt. De deelnemers aan de Zorg- en Veiligheidshuizen zullen afspraken moeten maken hoe zij hier in de praktijk vorm aan geven.

Langlopende casussen
In principe is de betrokkenheid van een Zorg en Veiligheidshuis bij een persoon tijdelijk van aard, totdat de situatie voldoende is verbeterd, of totdat partners zonder tussenkomst van het Zorg- en Veiligheidshuis verder kunnen met de casus. Desalniettemin blijkt dat er soms gevallen zijn waarbij langdurige betrokkenheid van het Zorg- en Veiligheidshuis noodzakelijk is. Dit speelt bijvoorbeeld bij personen met een hoog veiligheidsrisico als gevolg van chronisch ernstig psychiatrische aandoeningen. Het Zorg- en Veiligheidshuis vervult dan een cruciale rol bij het duurzaam verbinden van de ketens van strafrecht, openbare orde en veiligheid, zorg en sociaal domein. In dergelijke situaties kan de termijn voor vernietiging, anonimisering of verwijdering van artikel 8, zevende lid,eerste volzin te kort blijken. De casus loopt dan misschien nog, of is pas vrij recent afgesloten. In dergelijke gevallen biedt artikel 8, zevende lid, tweede volzin, de mogelijkheid om met instemming van de deelnemers die gegevens ter beschikking hebben gesteld, de casus te verlengen. Uitgangspunt is wel dat er dan een nieuwe beoordeling plaats vindt door de deelnemers, welke gegevens nog noodzakelijk zijn om te hergebruiken. Uitgangspunt zal dan kunnen zijn dat de nieuwe termijn van maximaal vijf jaar na eerste verwerking, gerekend wordt vanaf het besluit tot verlenging.

Afsluiten van de casus
In formele zin zijn het de deelnemers zoals bedoeld in artikel 48, eerste lid die de casus afsluiten, aangezien zij optreden als gezamenlijke verwerkingsverantwoordelijke voor de Zorg- en veiligheidshuizen. Dit laat echter onverlet dat zij hierbij het oordeel van de overige betrokken deelnemers zullen betrekken.

Negende en tiende lid
In het negende lid is geregeld dat de deelnemers, bedoeld in artikel 48, eerste lid, derden op incidentele basis kunnen laten deelnemen aan het casusoverleg indien dat noodzakelijk is voor het doel van artikel 47. Deze derden krijgen uitsluitend toegang tot de persoonsgegevens die in het Zorg- en Veiligheidshuis worden verwerkt, voor zover dat noodzakelijk is voor het doel, bedoeld in artikel 47. Artikel 7, tweede lid, is van overeenkomstige toepassing. Voor de verstrekking van de resultaten van de gezamenlijke gegevensverwerking aan deze derden, gelden de regels die daarover zijn gesteld in artikel 7, tweede lid.

Indien naar het oordeel van de betrokken deelnemers voor een goede behandeling van complexe persoonsgebonden casuïstiek noodzakelijk kunnen derden worden betrokken op uiteenlopende gebieden zoals huisvesting, zorg, maatschappelijke opvang, jeugdhulp, crisisopvang, woonbegeleiding, beschermd wonen, begeleiding geestelijke of licht verstandelijke beperking problematiek, maatschappelijk werk, slachtofferzorg, bewindvoerders, huisartsenzorg, curatoren, bewindvoerders of mentoren.
Hiernaast kunnen indien dat naar het oordeel van de betrokken deelnemers voor een goede beoordeling van een individuele casus noodzakelijk is ook expertisecentra,

onderzoeksinstellingen of wetenschappelijke instellingen als derden deelnemen aan het overleg over een individuele casus. In formele zin zijn het de deelnemers zoals bedoeld in artikel 48, eerste lid die beoordelen of, en zo ja welke incidentele derden zij bij de casus willen betrekken, aangezien zij optreden als gezamenlijke verwerkingsverantwoordelijke voor de Zorg- en veiligheidshuizen. Dit laat echter onverlet dat zij hierbij ook het oordeel van overige betrokken deelnemers zullen betrekken.

Bij toepassing van het negende lid, zijn de artikelen die bij of krachtens deze wet van toepassing zijn op de deelnemers, bedoeld in artikel 48, tweede lid, van overeenkomstige toepassing en zien de deelnemers, bedoeld in artikel 48, eerste lid, erop toe dat derden die op incidentele basis deelnemen aan het casusoverleg voldoen aan de Algemene verordening gegevensbescherming en het bepaalde bij of krachtens deze wet. Dat betekent in de eerste plaats dat deze incidentele derden gelijk worden gesteld met de deelnemers, bedoeld in artikel 48, tweede lid. Op de verstrekking van de resultaten van de gezamenlijke verwerking aan deze derden, is artikel 7, tweede lid en vierde lid, van overeenkomstige toepassing.
Deze bepaling geeft in de tweede plaats mede uitvoering aan artikel 48, derde lid, waaruit volgt dat de publiekrechtelijke deelnemers, bedoeld in artikel 48, eerste lid, gezamenlijk verwerkingsverantwoordelijke zijn voor de gezamenlijke gegevensverwerking in het samenwerkingsverband. Wanneer deze deelnemers het noodzakelijk achten om derden op incidentele basis te laten deelnemen aan een casusoverleg, zijn zij er ook verantwoordelijk voor dat deze derden zich aan de AVG en aan het bepaalde bij of krachtens dit wetsvoorstel houden.
Voor derden die incidenteel deelnemen geldt bijvoorbeeld de geheimhoudingsbepaling op grond van artikel 9 van dit wetsvoorstel.
Op grond van het twaalfde lid, kunnen bij of krachtens algemene maatregel van bestuur nadere regels worden gesteld over incidentele deelname van derden alsmede die criteria die daarvoor gelden en werkwijze die daarbij wordt gevolgd.

Elfde lid
Het elfde lid, biedt de grondslag voor de deelnemers, bedoeld in artikel 48, eerste lid, om, overeenkomstig artikel 7, tweede lid, de resultaten van de verwerking op grond van dit artikel aan een derde te verstrekken.
Het gaat hier om een derde die niet bij de casus is betrokken op grond artikel 52, negende lid. Deelnemers kunnen afspraken maken hoe zij met dergelijke situaties omgaan. Daarbij dienen altijd de voorwaarden van artikel 7 tweede lid onderdeel a en b, artikel 7, derde lid en artikel 50, derde lid in acht genomen te worden.
Een derde die op grond van artikel 52, negende lid, betrokken wordt bij de casus dient op dat moment beschouwd te worden als een deelnemer voor de duur van de casus.

In formele zin zijn het de deelnemers zoals bedoeld in artikel 48, eerste lid die beslissen of zij resultaten uit het Zorg- en Veiligheidshuis aan een niet betrokken derde willen verstrekken, aangezien zij optreden als gezamenlijke verwerkingsverantwoordelijke voor de Zorg- en veiligheidshuizen. Dit laat onverlet dat zij bij deze beslissing zich rekenschap zullen moeten geven van het oordeel van de overige bij de casus betrokken deelnemers. Ook zullen zij hierbij de voorwaarden van artikel 7, eerste en tweede lid, onderdelen a en b, artikel 7, derde lid en artikel 50, derde lid, in acht dienen te nemen. Artikel 7, eerste en tweede lid, bepaalt onder andere dat verstrekking achterwege blijft indien een deelnemer aangeeft dat zwaarwegende belangen zich tegen de verstrekking verzetten. Artikel 7, derde lid, geeft aan dat verstrekking van bijzondere en strafrechtelijke gegevens aan derden slechts mogelijk is indien de deelnemer die de gegevens aan het samenwerkingsverband heeft verstrekt daarmee instemt. Artikel 50, derde lid, bepaalt voorts dat deelnemers die gegevens verstrekken aan het Zorg- en Veiligheidshuis voorwaarden en beperkingen kunnen stellen aan de verdere verwerking van gegevens, waaronder ook de verstrekking van gegevens aan derden. Waar hier gesproken wordt van deelnemers worden ook de incidentele derden bedoeld die op grond van het negende lid van dit artikel bij de casus zijn betrokken.

Twaalfde lid

In het twaalfde lid is geregeld dat bij of krachtens algemene maatregel van bestuur nadere regels kunnen worden gesteld over de gegevensverwerking bij het casusoverleg, waaronder over de criteria waaraan een casus moet voldoen om te kunnen worden behandeld in het Zorg- en Veiligheidshuis, de eisen van kwaliteit en betrouwbaarheid waaraan aan de casus moet voldoen, incidentele deelname van derden alsmede de criteria die daarvoor gelden en werkwijze die daarbij wordt gevolgd. Daarbij kunnen ook beperkingen worden gesteld aan de categorieën van persoonsgegevens waartoe derden toegang kunnen krijgen.

Artikel 53 (activiteit lijst geprioriteerde casussen)

Artikel 53 biedt de grondslag voor het verwerken van gegevens in het kader van de activiteit het maken en gebruiken van een lijst met geprioriteerde casussen. Zoals bij artikel 47a, onderdeel b, is toegelicht is het nodig om extra aandacht te schenken aan personen die het meest bijdragen aan de criminaliteit of onveiligheid dan wel een hoog veiligheidsrisico hebben. Met het vaststellen van een lijst van casussen, ook wel 'Top X' aanpak genoemd, worden de beschikbare middelen bij voorrang ingezet op de aldus geselecteerde casussen. Het prioriteren van casussen aan de hand van het opstellen en gebruiken van de lijst met geprioriteerde casussen draagt bij aan het bepalen en uitvoeren van een gezamenlijke strategie voor de uitoefening van de taken en bevoegdheden waarmee de deelnemers zijn belast. Deelnemers aan het Zorg- en Veiligheidshuis zullen voor de activiteiten in het kader van dit artikel afspraken moeten maken over de wijze waarop zij invulling geven aan de beginselen van van noodzaak, subsidiariteit en proportionaliteit van de AVG, om zo de betrokkene te beschermen tegen onnodige verwerking en verspreiding van zijn gegevens.

Eerste lid
In het eerste lid, is bepaald dat de deelnemers, bedoeld in artikel 48, eerste lid, objectieve criteria vaststellen op grond waarvan een persoon op de lijst met geprioriteerde casussen wordt geplaatst en dat zij deze criteria openbaar maken. Deze bepaling dient als waarborg voor betrokkenen om van tevoren een inschatting te kunnen maken wanneer hun persoonsgegevens door de Zorg- en Veiligheidshuizen in dit verband kunnen worden verwerkt.

Tweede lid
Het tweede lid bepaalt dat de deelnemers bedoeld in artikel 48, eerste lid, gegevens, bedoeld in artikel 51, eerste lid, onderdelen a en b kunnen verwerken om vast te stellen welke personen voldoen aan de vastgestelde criteria en op de lijst geplaatst dienen te worden voor zover dat noodzakelijk is voor het doel van artikel 47.
Het Zorg- en Veiligheidshuis draagt zorg voor een zorgvuldige totstandkoming van een lijst met daarop alle personen die voldoen aan de onder het eerste lid gestelde objectieve criteria. Het Zorg- en Veiligheidshuis zal op grond van informatie die deelnemers daarbij verstrekken beoordelen of personen inderdaad aan de criteria voldoen. Slechts in een enkel geval zal één deelnemer over alle gegevens beschikken waarmee uitsluitsel kan worden gegeven of een persoon aan alle vastgestelde criteria voldoet. In de regel zal de informatie die nodig is om aan alle criteria te kunnen toetsen, verspreid liggen over meerdere deelnemers. In die gevallen zal het nodig zijn om bij verschillende deelnemers gegevens over personen op te halen voor zover die betrekking hebben op een of meerdere criteria, om daarna door vergelijking vast te stellen welke personen aan alle gestelde criteria voldoen. Alleen de personen die aan alle criteria voldoen worden op de lijst geplaatst. Het selecteren op een of meer criteria en het matchen op alle criteria betreft geen geautomatiseerde gegevensanalyse zoals bedoeld in artikel 8a. Met geautomatiseerde analyse wordt gedoeld op verwerkingsprocessen waarbij wiskundige en statistische procedures worden gehanteerd. Daarvan is hierbij geen sprake.

Er worden persoonsgegevens verwerkt van alle personen die voldoen aan ten minste een deel van de criteria als tussenstap naar de selectie van personen die aan alle criteria voldoen. De persoonsgegevens van de betrokkene die worden vastgelegd zijn onder andere identificerende gegevens en de gegevens waaruit blijkt of de persoon voldoet aan

een of meerdere criteria voor plaatsing op de lijst. Als een persoon op de lijst wordt geplaatst, wordt deze daarover geïnformeerd conform de AVG. Als de persoon niet op de lijst wordt geplaatst dan vernietigt het Zorg- en Veiligheidshuis de bij haar geregistreerde informatie. Als een persoon op de lijst is geplaatst betekent dit dat deze met voorrang behandeld wordt conform de stappen zoals beschreven in artikel 52. Tijdens de casusbehandeling zoals beschreven in artikel 52, vindt periodiek een beoordeling plaats of plaatsing op de lijst nog aangewezen is op grond van de criteria.

Indien plaatsing op de lijst niet meer is nodig is, wordt de persoon van de lijst gehaald. De door het Zorg- en Veiligheidshuis geregistreerde informatie wordt dan na de in artikel 8, zevende lid, genoemde bewaartermijn vernietigd. De betrokkene wordt hierover geïnformeerd conform de AVG.

Derde lid

Het derde lid bepaalt dat indien een betrokkene op de lijst wordt geplaatst, zijn casus behandeld wordt als een melding aan het Zorg- en Veiligheidshuis die in overeenstemming is met het doel, bedoeld in artikel 47, en dat artikel 52, derde tot en met twaalfde lid dan van overeenkomstige toepassing is.

Vierde lid

Het vierde lid bepaalt dat indien opname op de lijst niet of niet langer noodzakelijk is voor het doel, bedoeld in artikel 47, eerste lid, de persoon en alle op hem betrekking hebbende gegevens onverwijld van de lijst worden verwijderd. Voor zover er andere persoonsgegevens over betrokkene zijn verwerkt in het kader de activiteiten zoals bedoeld onder artikel 47a, onder a, worden deze gegevens behandeld conform het gestelde in artikel 8, zevende lid en artikel 52, achtste lid.

Vijfde lid
Het vijfde lid regelt dat bij of krachtens algemene maatregel van bestuur nadere regels kunnen worden gesteld over dit artikel.

HOOFDSTUK 3. OVERIGE SAMENWERKINGSVERBANDEN

Om voldoende flexibiliteit te houden voor het oprichten van nieuwe samenwerkingsverbanden nadat de WGS in werking is getreden, wordt met hoofdstuk 3 een delegatiegrondslag voorgesteld, op basis waarvan een nieuw samenwerkingsverband bij amvb kan worden aangewezen. Daarbij wordt een bijzondere nahangprocedure voorgesteld om het parlement ook bij de aanwijzing en regeling van dit nieuwe verband te betrekken. Deze procedure houdt in dat na publicatie van de amvb de Staten-Generaal een periode van vier weken krijgen waarin één van beide Kamers met een absolute meerderheid kan verzoeken om het in de amvb geregelde onderwerp bij wet te regelen. In dat geval wordt de amvb onverwijld ingetrokken en wordt een daartoe strekkend wetsvoorstel zo spoedig mogelijk ingediend. In vier bestaande wetten is deze procedure overigens geregeld in deze vorm.

Aanwijzing van een samenwerkingsverband bij amvb is uitsluitend mogelijk als bij amvb doeleinden worden omschreven die passen binnen het raamwerk van het voorgestelde hoofdstuk 3:

a. het voorkomen en bestrijden van ernstige vormen van criminaliteit;
b. het voorkomen van grootschalig of systematisch onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen; of
c. het voorkomen van grootschalige of systematische ontduiking van wettelijke verplichtingen tot betaling van belastingen, retributies en rechten bij in- en uitvoer.

HOOFDSTUK 4. WIJZIGING VAN ANDERE WETTEN

De verplichting tot gegevenslevering uit het voorgestelde artikel 5 laat onverlet de geheimhoudingsplichten uit sectorale wetgeving die geen afwijking bij wettelijk voorschrift toelaten. Voor een aantal van deze geheimhoudingsplichten is het wenselijk en noodzakelijk dat uitzonderingen op die geheimhoudingsplichten worden opgenomen. Hiertoe dient hoofdstuk 4 van de WGS. Door de voorgestelde wijzigingen van die sectorale wetten worden geheimhoudingsplichten uit de volgende wetten doorbroken:

- Wet politiegegevens;
- Wet justitiële en strafvorderlijke gegevens;
- Wet op het financieel toezicht;
- Wet toezicht accountantsorganisaties;
- Wet toezicht trustkantoren 2018;
- Wet ter voorkoming van witwassen en financieren van terrorisme.

Artikel 70 (wijziging Wet politiegegevens)

Met dit voorgestelde artikel wordt in de Wpg een grondslag opgenomen voor verstrekking van politiegegevens door verwerkingsverantwoordelijken aan een samenwerkingsverband in de zin van de WGS, wanneer de politie of de Koninklijke marechaussee daaraan deelnemen. De voorgestelde wijziging is ook relevant voor bijzondere opsporingsdiensten, indien zij als deelnemer van een samenwerkingsverband in de zin van de WGS zijn aangewezen. Op basis van artikel 46, eerste lid, van de Wpg juncto artikel 2 van het Besluit politiegegevens bijzondere opsporingsdiensten en artikel 2 van het Besluit politiegegevens buitengewoon opsporingsambtenaren zullen de nieuwe bepalingen en de daarop te baseren bepalingen van het Besluit politiegegevens van overeenkomstige toepassing zijn op bijzondere opsporingsdiensten en buitengewoon opsporingsambtenaren.

De huidige Wpg (artikel 20, eerste lid) biedt bevoegde autoriteiten (zoals de politie en de Koninklijke marechaussee) de mogelijkheid om politiegegevens te verstrekken aan samenwerkingsverbanden waaraan zij deelnemen teneinde strafbare feiten te voorkomen en op te sporen, de openbare orde te handhaven, hulp te verlenen aan hen die deze behoeven of voor het uitoefenen van toezicht op de naleving van regelgeving. Zij mogen gegevens verstrekken voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang.

Op grond van de huidige bepaling verstrekt de politie als bevoegde autoriteit op lokaal, regionaal en landelijk niveau gegevens aan deelnemers van diverse soorten samenwerkingsverbanden. Hierbij valt te denken aan samenwerkingsverbanden met bijvoorbeeld gemeenten, jeugdzorg, de belastingdienst, scholen, uitkeringsinstanties en zorgorganisaties. Het kan gaan om tijdelijke samenwerking om een lokaal veiligheidsprobleem in een wijk aan te pakken maar bijvoorbeeld ook om een structurele samenwerking ter bestrijding van bepaalde criminaliteitsfenomenen op landelijk niveau. In de praktijk gaat het in veel gevallen om samenwerkingsverbanden waarvoor de verdergaande verwerkingsmogelijkheden die de WGS biedt, niet nodig zijn.

Voor de verstrekking van politiegegevens aan samenwerkingsverbanden die onder de WGS vallen, wordt voorgesteld aan artikel 20 Wpg een derde lid toe te voegen. Hiermee wordt benadrukt dat het gaat om een verstrekking aan een ander soort samenwerkingsverband dan bedoeld in het eerste lid. De doeleinden van de verwerking van de politiegegevens door een samenwerkingsverband dat onder de WGS valt, zijn in de eerste plaats opgesomd in hoofdstuk 2, de artikelen 11, 21, 31 en 47. Het gaat in dat hoofdstuk om vier samenwerkingsverbanden waaraan tenminste steeds de politie en in bepaalde gevallen ook de Koninklijke marechaussee deelnemen. Als de politie of de Koninklijke marechaussee aan een bij amvb aangewezen samenwerkingsverband als bedoeld in hoofdstuk 3, artikel 64, deelneemt, geldt de doelstelling die in dat artikel wordt bedoeld.

Volgens artikel 9, eerste lid, van de richtlijn gegevensbescherming opsporing en vervolging mogen persoonsgegevens die door verwerkingsverantwoordelijken worden verzameld voor opsporing en vervolging, niet worden verwerkt voor andere doeleinden, tenzij die verwerking krachtens het Unierecht of lidstatelijke recht is toegestaan. Het voorgestelde artikel 20, derde lid, is te beschouwen als een dergelijke bepaling van lidstatelijk recht.

Als de verwerkingsverantwoordelijke deelneemt aan een samenwerkingsverband onder de WGS dan verstrekt hij politiegegevens aan het samenwerkingsverband voor zover dat noodzakelijk is voor het bereiken van het doel van het samenwerkingsverband en met inachtneming van hetgeen bij artikel 21 Wpg is gesteld.

De voorgestelde bepaling bevat een uitzondering op de verstrekkingsplicht ingeval "zwaarwegende redenen zich daartegen verzetten". Bij zwaarwegende redenen moet in het geval van de opsporingsdiensten in ieder geval wordt gedacht aan redenen die verband houden met opsporingsbelangen. Over de vraag of sprake is van zwaarwegende redenen hebben *andere* deelnemers in het samenwerkingsverband dan de deelnemer die de gegevens zou verstrekken, geen zeggenschap.

Artikel 71 (wijziging Wet justitiële en strafvorderlijke gegevens)

Artikel 71 bevat wijzigingen van de Wjsg om een grondslag te regelen voor verstrekking van justitiële en strafvorderlijke gegevens door verwerkingsverantwoordelijken aan een samenwerkingsverband in de zin van de WGS, wanneer zij daaraan deelnemen.

In de verplichtingen tot verstrekking is telkens als uitzondering opgenomen "tenzij naar het oordeel van de verwerkingsverantwoordelijke zwaarwegende redenen zich daartegen verzetten". Een voorbeeld van deze uitzondering doet zich voor wanneer het OM besluit om geen gegevens te verstrekken omdat met verstrekking het opsporingsbelang zou worden geschaad. Een ander zwaarwegende reden zou kunnen zij dat het OM besluit om niet tot verstrekking over te gaan omdat zij besluit niet tot vervolging over te gaan wegens gebrek aan bewijs.

Met het oog op de deelname van politiële of justitiële autoriteiten aan samenwerkingsverbanden wordt voorgesteld in de Wjsg een artikel 8b en artikel 39fa op te nemen die de verstrekking van respectievelijk justitiële en strafvorderlijke gegevens aan samenwerkingsverbanden als bedoeld in de WGS regelen. Met betrekking tot deze bepalingen geldt mutatis mutandis grotendeels hetzelfde als wat in de toelichting op artikel 70 is vermeld.

Daarnaast wordt voorgesteld om in de Wjsg een artikel 51ca op te nemen die de verstrekking regelt van tenuitvoerleggingsgegevens. Zowel de minister van Justitie en Veiligheid als het College van procureurs generaal zijn in de Wjsg aangewezen als verwerkingsverantwoordelijken.

Artikel 72 (wijziging Wet op het financieel toezicht)

Dit artikel en de volgende artikelen wijzigen een aantal wetten op het gebied van de financiële markten. Voor deze wetgeving wordt een algemene uitzonderingsbepaling op de geheimhoudingsplicht voorgesteld voor verstrekking aan een samenwerkingsverband in de zin van de WGS. Dit maakt mogelijk dat de Autoriteit Financiële Markten (AFM) en De Nederlandsche Bank (DNB) kunnen deelnemen aan samenwerkingsverbanden en dat zij informatie die zij op grond van de gewijzigde wetten verkrijgen, kunnen delen. Het gaat om de Wet op het financieel toezicht (Wft), de Wet ter voorkomen van witwassen en het financieren van terrorisme (Wwft), de Wet toezicht trustkantoren 2018 (Wtt 2018) en de Wet toezicht accountantsorganisaties (Wta).

Het onderhavige artikel wijzigt de Wft. Op grond van artikel 1:89 Wft rust op de AFM en DNB een geheimhoudingsplicht, waarop alleen uitzonderingen in de Wft mogelijk zijn. In

de artikelen 1:90 tot en met 1:93f Wft zijn uitzonderingen opgenomen, die mogelijk maken dat de AFM en DNB aan bepaalde partijen, onder bepaalde voorwaarden gegevens verstrekken. Het voorgestelde artikel 1:93g Wft maakt mogelijk dat de AFM en DNB informatie die zij verkrijgen in het kader van het toezicht op de Wft en op Europese verordeningen delen met partijen in een samenwerkingsverband dat onder de WGS valt, als zij aan dat samenwerkingsverband deelnemen.

Het verstrekken van gegevens of inlichtingen door de AFM en DNB op grond van de Wft is telkens aan voorwaarden verbonden. Deze voorwaarden zijn per soort en per ontvangende partij verstrekking geregeld in de artikelen 1:90 tot en met 1:93f Wft. Zij komen veelal voort uit dwingende Europese voorschriften over de geheimhoudingsplicht waaraan de AFM en DNB gehouden zijn. Deze voorschriften verschillen per richtlijn of verordening. Veel richtlijnen of verordeningen bevatten een gesloten stelsel: een uitputtende opsomming van mogelijke uitzonderingen op de geheimhoudingsplicht. Andere laten de nationale wetgever vrijer. Binnen een samenwerkingsverband gelden de voorwaarden van de artikelen 1:90 tot en met 1:93f onverkort, voor zover de deelnemers aan het samenwerkingsverband partijen zijn waarmee de uitwisseling in deze artikelen is geregeld. Dit is geregeld in het tweede lid.

Ook bij verstrekking aan andere partijen, waarvoor op dit moment nog geen zelfstandige, bilaterale verstrekking in de Wft is geregeld, zullen de AFM en DNB altijd aan de Europese voorschriften over geheimhouding en gebruik van gegevens moeten voldoen. Veel voorkomende voorwaarden voor verstrekking zijn opgenomen in artikel 1:90, eerste lid, en 1:93, tweede lid, Wft. Deze bepalingen verbieden verstrekking indien:

a. het doel waarvoor de vertrouwelijke gegevens of inlichtingen zullen worden gebruikt onvoldoende bepaald is;
b. het beoogde gebruik van de vertrouwelijke gegevens of inlichtingen niet past in het kader van het toezicht op financiële markten of op personen die op die markten werkzaam zijn;
c. de verstrekking van de vertrouwelijke gegevens of inlichtingen zich niet zou verdragen met de Nederlandse wet of de openbare orde;
d. de geheimhouding van de vertrouwelijke gegevens of inlichtingen niet in voldoende mate is gewaarborgd;
e. de verstrekking van de vertrouwelijke gegevens of inlichtingen redelijkerwijs in strijd is of zou kunnen komen met de belangen die deze wet beoogt te beschermen; of
f. onvoldoende is gewaarborgd dat de vertrouwelijke gegevens of inlichtingen niet zullen worden gebruikt voor een ander doel dan waarvoor deze worden verstrekt.

In het geval van een samenwerkingsverband dat onder de WGS valt, worden deze voorwaarden ondervangen door het systeem van de WGS. Zo is het doel van het samenwerkingsverband per definitie voldoende bepaald (a), zal op het moment van het aanwijzen van de AFM of DNB als deelnemer worden beoordeeld of het doel van het samenwerkingsverband voldoende bij hun taken aansluit (b), zal verstrekking niet in strijd met de Nederlandse wet of openbare orde zijn (c), is de geheimhouding geregeld (d), is er de mogelijkheid om verstrekking te weigeren als dat in strijd komt met de belangen die de Wft beoogt te beschermen (zwaarwegende redenen) (e) en is de doelbinding geregeld (f).

Een andere voorwaarde die op grond van Europees recht veelal geldt voor verstrekking door de AFM en DNB is dat zij extra zorgvuldig omgaan met informatie die zij van andere toezichthouders hebben ontvangen. Zij kunnen deze informatie alleen verder verstrekken als de toezichthouder van wie zij die hebben ontvangen daar toestemming voor heeft gegeven (artikelen 1:90, tweede lid, 1:91, tweede lid, onderdeel b, 1:93, derde lid, 1:93b, tweede lid, 1:93c, tweede lid, 1:93e, eerste lid, en 1:93f, eerste lid Wft). Ook voor verstrekking aan samenwerkingsverbanden waarop de WGS van toepassing is, zal deze voorwaarde op grond van Europese voorschriften in de meeste gevallen moeten gelden en zal zij worden opgenomen in de amvb. Het systeem van de WGS met de toevoeging van deze voorwaarde biedt daarmee dezelfde waarborgen bij verstrekking van gegevens als de overige gegevensverstrekkingen die in de Wft zijn geregeld.

Per samenwerkingsverband zal bekeken worden of het wenselijk en mogelijk is dat de AFM en DNB als deelnemers worden aangewezen. Als dit het geval is en de AFM of DNB toetreedt tot een samenwerkingsverband, kan het zijn dat bij bepaalde gegevens het Europees recht beperkingen stelt aan de verstrekking van deze gegevens. In dat geval zullen bij algemene maatregel van bestuur nadere voorwaarden worden gesteld waaronder de verstrekking door de AFM en DNB kan plaatsvinden aan een samenwerkingsverband. Per samenwerkingsverband en per soort informatie zal telkens bekeken worden welke voorwaarden gelden op Europees niveau. Deze zullen vervolgens ook worden opgenomen in de amvb waarmee het samenwerkingsverband wordt opgericht. Daarmee is dan ook voor alle andere deelnemers in het samenwerkingsverband duidelijk onder welke voorwaarden de AFM en DNB gegevens kunnen verstrekken. Door deze werkwijze te hanteren past de verstrekking door de AFM en DNB in het kader van een samenwerkingsverband binnen het Europese stelsel van geheimhouding en gegevensverstrekking.

Artikel 73 (wijziging Wet toezicht accountantsorganisaties)

Op grond van artikel 63a Wta rust op de AFM een geheimhoudingsplicht, waarop alleen uitzonderingen in de Wta mogelijk zijn. In de artikelen 63b tot en met 63f, 63j en 63m zijn uitzonderingen opgenomen, die mogelijk maken dat de AFM aan bepaalde partijen, onder bepaalde voorwaarden gegevens verstrekt. Artikel 63ea maakt mogelijk dat de AFM informatie die zij verkrijgt in het kader van het toezicht op de Wta kan delen met partijen in een samenwerkingsverband dat onder de WGS valt, als zij als deelnemer aan dat samenwerkingsverband is aangewezen.

Het verstrekken van gegevens of inlichtingen door de AFM op grond van de Wta is aan voorwaarden verbonden. Deze voorwaarden zijn per soort verstrekking en per ontvangende partij geregeld. Voor verstrekking aan een samenwerkingsverband zullen deze voorwaarden onverkort gelden. Dat is opgenomen in het voorgestelde artikel 63ea, tweede lid, Wta. Zoals in de toelichting op artikel 72 is beschreven wordt aan veel van deze voorwaarden voldaan via het systeem van de WGS. Voor andere voorwaarden, die niet worden ondervangen door het systeem van de WGS, bepaalt het voorgestelde artikel 63ea, tweede lid, Wta dat zij onverkort gelden, voor zover de deelnemers aan het samenwerkingsverband partijen zijn waarvoor de verstrekking in de artikelen 63b, 63c, 63cc en 63e is geregeld. Voor andere partijen, waarvoor in die artikelen geen zelfstandige bilaterale verstrekking is geregeld, kan per geval worden bepaald welke voorwaarden in de amvb worden opgenomen.

In aanvulling op de voorwaarden die ook in de Wft voorkomen, bepaalt artikel 63cc, tweede lid, nog dat de gegevens die worden verstrekt niet herleidbaar mogen zijn tot andere personen dan accountantsorganisaties of externe accountants. Als de AFM voornemens is toe te treden tot een samenwerkingsverband zal moeten worden afgewogen of het verstrekken van deze gegevens aan (een deel van de) deelnemende partijen noodzakelijk en proportioneel is. Zo nodig zal voor bepaalde gegevens in de amvb waarmee het samenwerkingsverband wordt aangewezen worden geregeld dat zij niet worden verstrekt.

Het voorgestelde artikel 63ea, derde lid, Wta bevat een grondslag om in de amvb nadere voorwaarden en beperkingen te stellen. Dit kan nodig zijn om aan Europese voorschriften te voldoen. Op dit moment biedt artikel 36 van de richtlijn wettelijke controles jaarrekeningen[34] lidstaten de ruimte om in hun nationale wetgeving uitzonderingen op de geheimhoudingsplicht van de toezichthouders te maken. Ook artikel 22 van de verordening wettelijke controles jaarrekeningen[35] staat hier niet aan in de weg. Mochten

[34] Richtlijn 2006/43/EG van het Europees Parlement en de Raad van 17 mei 2006 betreffende de wettelijke controles van jaarrekeningen en geconsolideerde jaarrekeningen, tot wijziging van de Richtlijnen 78/660/EEG en 83/349/EEG van de Raad en houdende intrekking van Richtlijn 84/253/EEG van de Raad (PbEU 2006, L 157, p. 87)

[35] Verordening (EU) nr. 537/2014 van 16 april 2014 betreffende specifieke eisen voor de wettelijke controles van financiële overzichten van organisaties van openbaar belang en tot intrekking van Besluit 2005/909/EG van de Commissie (PbEU 2014, L158, p. 77).

op enig moment wel Europese voorschriften gaan gelden voor de verstrekking aan samenwerkingsverbanden waarvoor de WGS geldt, dan kunnen die voorschriften per samenwerkingsverband in de amvb worden vastgelegd.

Artikel 74 (wijziging Wet toezicht trustkantoren 2018)

Op grond van artikel 55 Wtt 2018 rust op DNB een geheimhoudingsplicht, waarop alleen uitzonderingen in die wet mogelijk zijn. In de artikelen 56 tot en met 58 Wtt 2018 zijn uitzonderingen opgenomen, die mogelijk maken dat DNB aan bepaalde partijen, onder bepaalde voorwaarden gegevens verstrekt. Artikel 56a maakt mogelijk dat DNB informatie die zij verkrijgt in het kader van het toezicht op de Wtt kan delen met partijen in een samenwerkingsverband dat onder de WGS valt, als zij als deelnemer aan dat samenwerkingsverband is aangewezen.

Het verstrekken van gegevens of inlichtingen door DNB op grond van de Wtt 2018 is aan voorwaarden verbonden. Deze voorwaarden zijn per soort verstrekking en per ontvangende partij geregeld in de artikelen 56 tot en met 58. Voor verstrekking aan een samenwerkingsverband zullen deze voorwaarden onverkort gelden. Dat is opgenomen in het voorgestelde artikel 56, tweede lid, Wtt 2018. Zoals in de toelichting op artikel 72 is beschreven wordt aan veel van deze voorwaarden voldaan via het systeem van de WGS. Voor andere voorwaarden, die niet worden ondervangen door het systeem van de WGS, bepaalt het voorgestelde artikel 56, tweede lid, Wtt 2018 dat zij gelden, voor zover de deelnemers aan het samenwerkingsverband partijen zijn waarvoor de verstrekking in de artikelen 56, 57 en 58 is geregeld. Voor andere partijen, waarvoor in die artikelen geen zelfstandige, bilaterale verstrekking is geregeld, kan per geval worden bepaald welke voorwaarden in de amvb worden opgenomen.

In aanvulling op de voorwaarden die ook in de Wft voorkomen, bevat artikel 56, eerste lid, nog het verbod om gegevens te verstrekken die betrekking hebben op cliënten van trustkantoren. Als DNB voornemens is toe te treden tot een samenwerkingsverband zal moeten worden afgewogen of het verstrekken van deze gegevens aan (een deel van de) deelnemende partijen noodzakelijk en proportioneel is. Zo nodig zal voor bepaalde gegevens in de amvb waarmee het samenwerkingsverband wordt aangewezen worden geregeld dat zij niet worden verstrekt.

Het voorgestelde artikel 56a, derde lid, Wtt 2018 bevat een grondslag om in de amvb nadere voorwaarden en beperkingen te stellen. Dit kan nodig zijn om aan Europese voorschriften te voldoen. In het geval van de Wtt 2018 gaat het om voorschriften uit de vierde anti-witwasrichtlijn[36], die in de Wtt 2018 zijn geïmplementeerd, voor zover het verplichtingen voor trustkantoren betreft. Op 30 mei 2018 is een richtlijn tot wijziging van de vierde anti-witwasrichtlijn[37] in werking getreden, die voor toezichthouders op de verplichtingen uit deze richtlijn een geheimhoudingsplicht voorschrijft.[38] Op die geheimhoudingsplicht zijn maar beperkte uitzonderingen mogelijk. Indien DNB deelneemt aan een samenwerkingsverband zal met deze beperking rekening gehouden moeten worden en zullen aan de verstrekking van gegevens op grond van de Wtt 2018 in de amvb eventueel aanvullende voorwaarden worden gesteld.

Artikel 75 (wijziging Wet ter voorkoming van witwassen en financieren van terrorisme)

[36] Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie (PbEU 2015, L 141)
[37] Richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU (PbEU 2018, L 156)
[38] Artikel 57bis van de richtlijn

Het artikel maakt mogelijk dat zowel Wwft toezichthoudende autoriteiten als instellingen die verplichtingen hebben op grond van de Wwft gegevens verstrekken aan een samenwerkingsverband waarop de WGS van toepassing is, als zij als deelnemer daaraan zijn aangewezen.

A

Artikel 22, eerste lid juncto zesde lid, bevat de geheimhoudingsplicht van toezichthoudende autoriteiten als bedoeld in de Wwft (DNB, AFM, Bureau Financieel Toezicht, de deken, de Minister van Financiën en de kansspelautoriteit). Het geldt voor al het Wwft toezicht, met uitzondering van het toezicht op advocaten en het toezicht op notarissen. De geheimhoudingsplicht van de toezichthoudende autoriteiten voor die beroepsgroepen is geregeld in specifieke wetgeving voor die beroepsgroepen. Het voorgestelde artikel bevat slechts een uitzondering op de geheimhoudingsplicht van de toezichthoudende instellingen dat in artikel 22, eerste lid, Wwft is geregeld en is niet van toepassing voor de toezichthoudende autoriteiten voor die beroepsgroepen. Om mogelijk te maken dat toezichthoudende autoriteiten gegevens verstrekken aan een samenwerkingsverband waarop de WGS van toepassing is, bevat het voorgestelde artikel 22d een uitzondering op de geheimhoudingsplicht.

Het bilateraal verstrekken van gegevens of inlichtingen door een toezichthoudende autoriteit op grond van de Wwft is aan voorwaarden verbonden. Deze voorwaarden zijn per soort verstrekking en per ontvangende partij geregeld in artikel 22 tot en met 22c. Voor verstrekking aan een samenwerkingsverband zullen deze voorwaarden onverkort gelden. Dat is opgenomen in het voorgestelde artikel 22d, tweede lid, Wwft. Zoals in de toelichting op artikel 72 is beschreven wordt aan veel van deze voorwaarden voldaan via het systeem van de WGS. Voor andere voorwaarden, die niet worden ondervangen door het systeem van de WGS, bepaalt het voorgestelde artikel 22d, tweede lid, Wwft dat zij gelden, voor zover de deelnemers aan het samenwerkingsverband partijen zijn waarvoor de verstrekking in de artikelen 22 tot en met 22c is geregeld. Voor andere partijen, waarvoor in die artikelen geen zelfstandige, bilaterale verstrekking is geregeld, kan per geval worden bepaald welke voorwaarden in de amvb worden opgenomen.

Het voorgestelde artikel 22d, derde lid, Wwft bevat een grondslag om in de amvb nadere voorwaarden en beperkingen te stellen. Dit kan nodig zijn om aan Europese voorschriften te voldoen. In het geval van de Wwft gaat het, net als bij de Wtt 2018, om voorschriften uit de vierde anti-witwasrichtlijn[39], die in de Wwft zijn geïmplementeerd. Op 30 mei 2018 is een richtlijn tot wijziging van de vierde anti-witwasrichtlijn[40] in werking getreden, die voor toezichthoudende autoriteiten een geheimhoudingsplicht voorschrijft.[41] Op die geheimhoudingsplicht zijn maar beperkte uitzonderingen mogelijk. Indien toezichthoudende autoriteiten deelnemen aan een samenwerkingsverband zal met deze beperking rekening gehouden moeten worden en zullen aan de verstrekking van gegevens op grond van de Wwft in de amvb eventueel aanvullende voorwaarden worden gesteld.

B

De Wwft kent naast een geheimhoudingsplicht voor toezichthoudende autoriteiten in artikel 23 ook een geheimhoudingsplicht (mededelingsverbod) voor instellingen die de beschikking hebben over bepaalde Wwft-informatie. Dit mededelingsverbod wordt

[39] Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie (PbEU 2015, L 141)
[40] Richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU (PbEU 2018, L 156)
[41] Artikel 57bis van de richtlijn

voorgeschreven in de vierde anti-witwasrichtlijn, die in de Wwft is geïmplementeerd.[42] In bepaalde gevallen kan de informatie waar het om gaat van nut zijn voor een samenwerkingsverband. Om die reden wordt voorgesteld om in artikel 23aa een uitzondering op het mededelingsverbod op te nemen, die het mogelijk maakt dat instellingen gegevens verstrekken aan een samenwerkingsverband dat valt onder de WGS.

Op grond van artikel 39, tweede lid, vierde anti-witwasrichtlijn, kan die verstrekking alleen plaatsvinden aan bevoegde autoriteiten of voor rechtshandhavingsdoeleinden. Verstrekking door een instelling aan een samenwerkingsverband dat valt onder de WGS zal daaraan dan ook telkens moeten voldoen. Dit wordt in het systeem van de WGS ondervangen doordat in het kader van de vraag of een instelling kan toetreden wordt nagegaan wat de mogelijkheden en voorwaarden zijn voor verstrekking. Als op grond van de richtlijn geen uitwisselingsmogelijkheden bestaan, zal een instelling de informatie die valt onder de geheimhoudingsplicht van artikel 23 niet in het samenwerkingsverband kunnen delen.

Artikel 75d (wijziging Wet Bibob)
Dit betreft een wetstechnische actualisering om op de juiste wijze te verwijzen naar de RIEC's.

Deze toelichting wordt ondertekend mede namens de Minister voor Rechtsbescherming.

De Minister van Justitie en Veiligheid,

[42] Artikel 39, eerste lid, van de richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie (PbEU 2015, L 141)