

NOTA VAN TOELICHTING

Inhoud

HOOFDSTUK 1. ALGEMENE BEPALINGEN	3
Artikel 1.1 Aanwijzing contactpunt.....	3
Artikel 1.2 Verantwoordelijkheid voor nakoming verzoeken AVG.....	5
Artikel 1.3 Verantwoordelijkheid voor nakoming informatieplicht	7
Artikel 1.4 Verantwoordelijkheid voor nakoming meldplicht datalekken	8
Artikel 1.5 Rechtmatig verwerkte gegevens	9
Artikel 1.6 Kwaliteit van een aangemeld signaal, verzoek of casus.....	9
Artikel 1.7 Correctie van onjuistheden tijdens gezamenlijke gegevensverwerking	10
Artikel 1.8 Kwaliteit van de resultaten.....	10
Artikel 1.9 Nationaliteit	12
Artikel 1.10 Nadere inkadering van gegevensuitwisseling tussen samenwerkingsverbanden..	12
Artikel 1.11 Betrouwbaarheid geautoriseerde personen	16
Artikel 1.12 Logging.....	17
Artikel 1.13 Werkwijze van de rechtmatigheidsadviescommissie.....	18
Artikel 1.14 Samenstelling van de rechtmatigheidsadviescommissie	21
Artikel 1.15 Rechtmatigheidsadviescommissie voor cluster van samenwerkingsverbanden....	22
Artikel 1.16 Precisering maximale bewaartermijn	22
Artikel 1.17 Opleiding en training ten aanzien van gegevensverwerking	24
Artikel 1.18 Uitwerking auditbepaling.....	25
HOOFDSTUK 2. BEPALINGEN INZAKE SPECIFIEKE SAMENWERKINGSVERBANDEN	26
PARAGRAAF 2.1 FINANCIËEL EXPERTISECENTRUM (FEC)	26
Artikel 2.1 Aanvullende deelnemers Programma Terrorismefinanciering	26
Artikel 2.2 Deelnemers aan publiek-private samenwerking	27
Artikel 2.3 Beperking gegevensverstrekking over kring van personen	29
Artikel 2.4 Criteria voor behandeling van een signaal of verzoek	30
Artikel 2.5 Nadere waarborgen signalenoverleg en gegevensanalyse.....	32
PARAGRAAF 2.2 INFOBOX CRIMINEEL EN ONVERKLAARBAAR VERMOGEN (iCOV)	33
Artikel 2.6 Aanvullende deelnemers	33
Artikel 2.7 Beperking gegevensverstrekking over kring van personen	35
Artikel 2.8 Criteria voor een rapportage over vermogen en inkomsten of financieel-zakelijke relaties .	35
Artikel 2.9 Vaststelling van thema voor een themarapportage.....	37
Artikel 2.10 Vaststelling van indicatoren voor een themarapportage	41
Artikel 2.11 Criteria voor behandeling van een verzoek om een themarapportage	41
Artikel 2.12 Uitvoering van de gegevensanalyse voor een themarapportage	43
PARAGRAAF 2.3 REGIONALE INFORMATIE- EN EXPERTISECENTRA (RIEC's)	44
Artikel 2.13 Territoriale werkgebieden.....	44
Artikel 2.14 Nadere regels over wettelijke taken en bevoegdheden van deelnemers.....	45
Artikel 2.15 Concretisering van te verstrekken gegevens.....	45
Artikel 2.16 Criteria voor behandeling van een signaal	46
PARAGRAAF 2.4 ZORG- EN VEILIGHEIDSHUIZEN (ZVH).....	48
Artikel 2.17 Definitiebepaling	48
Artikel 2.18 Territoriale werkgebieden.....	48
Artikel 2.19 Beperking gegevensverstrekking over kring van personen.....	48
Artikel 2.20 Criteria voor behandeling van een casus	49
Artikel 2.21 Nadere criteria voor incidentele deelname aan Zorg- en Veiligheidshuis	51
Artikel 2.22 Objectieve criteria voor plaatsing op een lijst van geprioriteerde casussen	53
HOOFDSTUK 3. WIJZIGING VAN ANDERE BESLUITEN	54
Artikel 3.1 Wijziging Besluit politiegegevens	54

ALGEMEEN

In het onderhavige Besluit gegevensverwerking door samenwerkingsverbanden (hierna: dit besluit) wordt uitvoering gegeven aan verplichtingen uit de Wet gegevensverwerking door samenwerkingsverbanden (hierna: WGS, of: de wet). Ook wordt nadere invulling gegeven aan de WGS ten aanzien van de gegevensverwerkingen en de waarborgen daarbij. Tevens worden in dit besluit zorgpunten geadresseerd van het parlement, de Afdeling advisering van de Raad van State en de Autoriteit Persoonsgegevens.

De WGS regelt gegevensdeling binnen het kader van samenwerkingsverbanden die zich richten op de aanpak van zware criminaliteit en ondermijning, namelijk de Infobox Crimineel en Onverklaarbaar Vermogen (iCOV), de Regionale Informatie- en Expertisecentra (RIEC's) en het Financieel Expertisecentrum (FEC). Ook regelt de WGS de gegevensdeling in Zorg- en Veiligheidshuizen. De Zorg- en Veiligheidshuizen richten zich op complexe gevallen, waarbij sprake is van een onveilige situatie die voortvloeit uit multi-problematiek en waarbij een ketenoverstijgende aanpak nodig is. De WGS creëert heldere juridische grondslagen waardoor deelnemers aan deze samenwerkingsverbanden gegevens met elkaar mogen delen en verwerken. Ter bescherming van de privacy bevat de WGS een aantal belangrijke waarborgen voor het gebruik van de gegevens, in aanvulling op en ter specificering van de waarborgen van de AVG.

Het onderhavige besluit regelt het volgende ter uitvoering van verplichtingen uit de WGS om bij amvb nadere regels te stellen:

1. Aanwijzing van een deelnemende overheidsinstantie als contactpunt voor betrokkenen;
2. Regels over werkwijze en de verantwoordelijkheidsverdeling van de deelnemers bij de uitoefening van AVG-rechten van betrokkene;
3. Nadere regels over de inhoud en wijze van uitvoering van audits;
4. Nadere waarborgen ten aanzien van de gegevensanalyse door FEC en iCOV, waaronder voorzieningen ter bevordering van de kwaliteit van de gehanteerde methodiek;
5. Nadere regels over de aan de RIEC's te verstrekken categorieën gegevens, de concretisering daarvan, en de bronnen van waaruit de gegevens afkomstig zijn.

Daarnaast vloeien de navolgende punten voort uit de brief van Minister van Justitie en Veiligheid van 17 december 2021 aan de Tweede en Eerste Kamer in reactie op de nadere adviezen van de Afdeling advisering van de Raad van State, de Autoriteit Persoonsgegevens en het College voor de Rechten van de Mens:¹

1. dat het startpunt van de gegevensverwerking zoveel mogelijk wordt geconcretiseerd (artikelen 2.4, 2.8, 2.11, 2.16 en 2.20) en daarbij te expliciteren dat deelnemers alleen rechtmatig verkregen informatie mogen inbrengen in het samenwerkingsverband (artikel 1.5);
2. dat iCOV voor haar doelstellingen gegevens alleen mag verwerken indien de gegevensverwerking ziet op onrechtmatig financieel gewin (artikelen 2.8, 2.10 en 2.11);²
3. dat bij iCOV een ondergrens geldt voor het aanvragen van rapportages over vermogen en inkomsten of relaties, met het oog op de proportionaliteit (artikel 2.8);
4. dat de doelstelling van het FEC wordt gepreciseerd waar het gaat om risico's met betrekking tot "andere ernstige vormen van criminaliteit" (artikel 2.4, derde lid);
5. dat bij de Zorg- en Veiligheidshuizen de gegevensverstrekking wordt beperkt tot de eerste schil rond een betrokkene, en dus niet de tweede en derde schil omvat (artikel 2.19);
6. dat uitdrukkelijke criteria zullen worden gesteld voor incidentele deelname aan de Zorg- en Veiligheidshuizen (artikel 2.21);

¹ Kamerstukken II 2021/22, 35447, nr. 21, §6 en 7 en de bijlage.

² Zie voor een nadere toelichting antwoord 23 uit de "Beantwoording vragen schriftelijk overleg over de reactie op nadere adviezen over het wetsvoorstel Wet gegevensverwerking door samenwerkingsverbanden".

Consultatieversie nota van toelichting concept-BGS

7. dat het delen van persoonsgegevens tussen samenwerkingsverbanden nader wordt geclausuleerd (artikel 1.10);
8. dat wordt beschreven wanneer persoonsgegevens in ieder geval eerder dan binnen vijf jaar moeten worden gewist en de verdere beperking van de mogelijkheid tot hernieuwde verwerking (artikel 1.16);
9. dat de positie van de rechtmatigheidsadviescommissies verder wordt versterkt bij de vaststelling van regels over de werkwijze, samenstelling en benoeming (artikel 1.13);
10. dat samenwerkingsverbanden bij de verstrekking van resultaten zoveel mogelijk moeten motiveren op basis van welke informatie de uitkomst tot stand is gekomen (artikel 1.8, tweede lid);
11. dat in de rechtmatigheidsadviescommissie ook aandacht is voor het tegengaan van risico's op ongelijke behandeling en discriminatie (artikel 1.14, vierde lid);
12. dat de medewerkers die worden ingezet in het samenwerkingsverband en de leden van de rechtmatigheidsadviescommissie passende opleidingen en trainingen krijgen (artikel 1.17);
13. dat de samenwerkingsverbanden geen persoonsgegevens over nationaliteit mogen verwerken, tenzij dit voor de identificatie van betrokkene onvermijdelijk is (artikel 1.9).

Het systeem van de WGS gaat uit van gezamenlijke verwerkingsverantwoordelijkheid van de deelnemers "voor de verwerking van persoonsgegevens door het samenwerkingsverband" (aldus artikel 1.4, eerste lid, van de wet). De gezamenlijke verwerkingsverantwoordelijkheid ontstaat na de verplichte gegevensverstrekking door de deelnemers aan het samenwerkingsverband op grond van artikel 1.5 van de WGS, of voor zover het gaat om de politie, de Koninklijke marechaussee en het openbaar ministerie – de artikelen 4.1 en 4.2 van de WGS, die enkele bepalingen toevoegen aan de Wet politiegegevens (hierna: Wpg) en de Wet justitiële en strafvorderlijke gegevens (hierna: Wjsg). De gegevensverstrekking van deelnemers aan het samenwerkingsverband valt onder de zelfstandige verantwoordelijkheid van de deelnemers. Vervolgens verwerkt het samenwerkingsverband de ontvangen gegevens gezamenlijk, bijvoorbeeld voor een signalenoverleg of gegevensanalyse (FEC), voor het opstellen van een rapportage (iCOV), een casusoverleg (RIEC's en Zorg- en Veiligheidshuizen) of een gebieds- of thematische scan (RIEC's). De gezamenlijke verwerkingsverantwoordelijkheid eindigt na ontvangst van een resultaat van de gezamenlijke gegevensverwerking door een deelnemer voor de eigen taak op grond van artikel 1.7 van de WGS. Dat is de fase waarin op basis van de gegevensanalyse daadwerkelijk gehandeld wordt door een deelnemer van een samenwerkingsverband. Die handeling kan bijvoorbeeld het overgaan tot daadwerkelijke interventies in concrete situaties betreffen. Deze fase valt onder de individuele verantwoordelijkheid van de betreffende deelnemer.

In hoeverre de invoering en naleving van de aanvullende waarborgen, zoals die worden uitgewerkt in dit besluit, een administratieve lastenverzwaring met zich meebrengen voor de deelnemers, en welke middelen daarvoor benodigd zijn, zal moeten blijken uit de uitvoeringstoetsen die worden uitgevoerd ten tijde van de consultatie inzake deze amvb. Deze zijn niet op voorhand te kwantificeren, maar bedacht moet worden dat de wet en dit besluit in substantiële mate een specificering of concretisering vormen van regels die samenwerkingsverbanden nu al op basis van de AVG moeten toepassen en dat de in de WGS opgenomen samenwerkingsverbanden bestendig zijn en kunnen bogen op ruime ervaring en expertise.

ARTIKELSGEWIJS

HOOFDSTUK 1. ALGEMENE BEPALINGEN

Artikel 1.1 Aanwijzing contactpunt

(grondslag: artikel 1.4, vierde lid, onder b, WGS)

Algemeen

Dit artikel is de uitwerking van artikel 1.4, vierde lid, onder b, WGS. Dit verplicht ertoe om bij amvb regels te stellen over de aanwijzing van een deelnemende overheidsinstantie als contactpunt

Consultatieversie nota van toelichting concept-BGS

voor een betrokkene voor de uitoefening van zijn rechten op grond van de Algemene verordening gegevensbescherming (AVG). Dit is een uitwerking van artikel 26, eerste lid, van de AVG, dat de mogelijkheid biedt om in een lidstaatrechtelijke bepaling een contactpunt voor betrokkenen aan te wijzen. De gedachte daarachter is dat burgers één duidelijk aanspreekpunt hebben waar zij terecht kunnen voor de uitoefening van hun rechten inzake de verwerking van hun persoonsgegevens door de deelnemers van het samenwerkingsverband (volgens artikel 1.4, eerste lid, WGS zijn zij de gezamenlijke verwerkingsverantwoordelijken). Hierdoor kunnen betrokkenen makkelijker hun rechten op grond van de AVG uitoefenen. De aanwijzing van het contactpunt voorkomt dat het voor een burger onduidelijk is wie hij kan benaderen wanneer hij bijvoorbeeld inzage of correctie wil van zijn persoonsgegevens. Het contactpunt zorgt er bovendien voor dat de deelnemers van het samenwerkingsverband hun communicatie met betrokkenen via het contactpunt op een efficiëntere manier kunnen coördineren. Ook stelt het contactpunt de deelnemers in staat om verzoeken van burgers om hun rechten op grond van de AVG uit te oefenen op een gecoördineerde, consistente wijze te beantwoorden.

De aanwijzing als contactpunt betekent dat die overheidsinstantie als vast contactpunt wordt aangewezen voor alle casussen.

Het contactpunt heeft de respectieve verantwoordelijkheid, in de zin van artikel 26, eerste lid, AVG voor:

- de nakoming van verzoeken van een betrokkene om zijn rechten op grond van de AVG uit te oefenen (zie artikel 1.2 van dit besluit);
- de nakoming van de informatieplicht jegens betrokkene op grond van artikel 14 van de AVG (zie artikel 1.3 van dit besluit);
- de nakoming van de meldplicht datalekken (zie artikel 1.4 van dit besluit).

Dit wil niet zeggen dat het contactpunt hierbij alleen opereert. Zoals blijkt uit de artikelen 1.2 tot en met 1.4 handelt het contactpunt in afstemming met de betrokken deelnemers. Het contactpunt krijgt een communicatieve, coördinerende taak en zorgt voor één centrale afhandeling van verzoeken tot uitoefening van rechten op grond van de AVG, informatieverstrekking aan betrokkenen en melding van datalekken.

De artikelen over het contactpunt doen dan ook niets af aan de gezamenlijke verwerkingsverantwoordelijkheid van de deelnemers voor de gezamenlijke gegevensverwerking.

Eerste lid

Op grond van de AVG oefent een betrokkene zijn rechten uit bij de verwerkingsverantwoordelijke. Bij de samenwerkingsverbanden zijn er meerdere gezamenlijke verwerkingsverantwoordelijken. In het eerste lid is bepaald dat de betrokkene een verzoek tot uitoefening van diens AVG-rechten (bijvoorbeeld een inzageverzoek) moet richten aan het contactpunt.

Mocht de betrokkene een verzoek tot uitoefening van zijn rechten op grond van de AVG indienen bij een ander overheidsorgaan dan het contactpunt, dan geldt de doorzendplicht, bedoeld in artikel 2:3, eerste lid, van de Algemene wet bestuursrecht: "Het bestuursorgaan zendt geschriften tot behandeling waarvan kennelijk een ander bestuursorgaan bevoegd is, onverwijld door naar dat orgaan, onder gelijktijdige mededeling daarvan aan de afzender." Immers, uit de artikelen 1.2 tot en met 1.4 van dit besluit volgt dat *alleen* het contactpunt verantwoordelijk is voor de behandeling van AVG-verzoeken, de nakoming van de informatieplicht en de nakoming van de meldplicht datalekken.

De slotzin van het eerste lid expliciteert dat een verzoek aan het contactpunt geldt als een verzoek aan alle gezamenlijke verwerkingsverantwoordelijken in het samenwerkingsverband.

Tweede lid

Dit lid voorziet in een vast contactpunt voor ieder samenwerkingsverband omwille van de transparantie en rechtszekerheid. Het is niet toegestaan om het contactpunt per casus te laten wisselen of per casus telkens opnieuw aan te wijzen. Weliswaar is het in de praktijk denkbaar dat het contactpunt niet betrokken is (geweest) bij de specifieke casuïstiek, maar ook in dergelijke gevallen heeft het contactpunt meerwaarde: enerzijds voor de burger die te maken heeft met één loket, anderzijds voor het samenwerkingsverband, omdat het contactpunt zorgdraagt voor een

Consultatieversie nota van toelichting concept-BGS

gecoördineerde afhandeling van AVG-verzoeken en een gecoördineerde toepassing van de informatieplicht.

Voor wat betreft het contactpunt is waar mogelijk gekozen voor de deelnemende overheidsinstantie waarvan het samenwerkingsverband operationele faciliteiten van die deelnemer gebruikt, zoals een gebouw of ICT, of die een grote inhoudelijke betrokkenheid bij de problematiek heeft. Bij de RIEC's en bij de Zorg- en Veiligheidshuizen is het niet altijd voorzienbaar welke gemeente het meest te maken heeft met de problematiek. Daarom moeten de deelnemers van een RIEC in onderling overleg bepalen welke burgemeester als contactpunt optreedt.³ Voor de Zorg- en Veiligheidshuizen moeten de gezamenlijke verwerkingsverantwoordelijken – dat wil zeggen de deelnemende overheidsinstanties, bedoeld in artikel 2.27, eerste lid, van de WGS – in onderling overleg bepalen van welke gemeente de burgemeester of het college als contactpunt optreedt. In het geval van RIEC's of de Zorg- en Veiligheidshuizen is het mogelijk dat na verloop van tijd de gezamenlijke verwerkingsverantwoordelijken overeenkomen dat een andere gemeente de rol van contactpunt overneemt. Dat moet worden gepubliceerd op grond van het derde lid.

Derde lid

Dit lid bevat een verplichting tot publicatie van de naam en contactgegevens van het contactpunt op de website van het samenwerkingsverband. Dit is nodig voor de transparantie.

Artikel 1.2 Verantwoordelijkheid voor nakoming verzoeken AVG

(grondslag: artikel 1.4, vierde lid, onder a, WGS)

Dit artikel vormt de uitwerking van artikel 1.4, vierde lid, onderdeel a, van de WGS, voor zover daaruit volgt dat bij amvb regels moeten worden gesteld over de werkwijze en de respectievelijke verantwoordelijkheden van de deelnemers met betrekking tot de uitoefening van de rechten van betrokkene.

Eerste lid

Dit lid regelt dat het contactpunt als enige van de deelnemers verantwoordelijk is voor de afhandeling van verzoeken van betrokkenen inzake de uitoefening van hun rechten op grond van hoofdstuk III van de AVG. In de praktijk gaat het dan om een verzoek op grond van de artikelen 15 tot en met 18, 21 en 22 van de AVG, die voorzien in het recht op inzage, rectificatie en wissing van gegevens, het recht op beperking van de verwerking, het recht om bezwaar te maken tegen de verwerking en het recht om niet te worden onderworpen aan geautomatiseerde besluitvorming. De overheidsinstantie die optreedt als contactpunt, neemt als enige de besluiten op verzoeken inzake de uitoefening van AVG-rechten. Dit draagt bij aan de eenduidige communicatie richting betrokkene: er wordt één besluit genomen jegens betrokkene. Ook is er hierdoor eenduidigheid naar betrokkenen: zowel in de fase van een AVG-verzoek als bij bezwaar en beroep is er één en hetzelfde aanspreekpunt voor betrokkenen. Vanuit de rechtszekerheid en duidelijkheid is het gewenst dat de betrokkene niet alleen voor de verzoeken op grond van de AVG naar het contactpunt kan, maar ook dat dit contactpunt vervolgens het besluit neemt op dat verzoek. Hiermee is tevens duidelijk dat er bij het contactpunt bezwaar kan worden gemaakt tegen het genomen besluit, dat er door het contactpunt op het bezwaar moet worden beslist en dat het contactpunt de verweerder is in een beroepsprocedure (wat onverlet laat dat naast het contactpunt ook een andere deelnemer als belanghebbende kan deelnemen aan een beroepsprocedure overeenkomstig artikel 8:26 Awb). Ten derde zorgt deze regeling ervoor dat het contactpunt het overzicht binnen het samenwerkingsverband behoudt, en weet of reeds is besloten

³ Voor de meeste RIEC's wordt tot op heden de postbus van de stad met het grootste inwoneraantal gebruikt als contactpunt. Uitzonderingen zijn RIEC Amsterdam Amstelland en RIEC Midden-Nederland, waar de postbus van de politie wordt gebruikt, RIEC West-Brabant/Zeeland en RIEC Oost-Brabant, waar de postbus van de gemeente Gilze-Rijen wordt gebruikt, en RIEC Noord, waar niet het adres van de stad met het grootste inwoneraantal (Groningen) wordt gebruikt maar dat van Leeuwarden.

Consultatieversie nota van toelichting concept-BGS

op een AVG-verzoek. Tot slot wordt met deze regeling voorkomen dat er mandaatregelingen nodig zijn tussen het contactpunt en de andere deelnemers.

Verzoeken van burgers om uitoefening van hun AVG-rechten moeten in beginsel binnen een maand worden afgehandeld, met dien verstande dat deze termijn indien nodig met nog eens twee maanden kan worden verlengd, afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken (artikel 12, derde lid, AVG). Het contactpunt moet deze termijn in acht nemen. Inhoudelijke betrokkenheid van meerdere deelnemers kan maken dat sprake is van een complex verzoek als bedoeld in voornoemde bepaling.

Indien een betrokkene het niet eens is met het besluit op zijn verzoek, dan staat voor hem bestuursrechtelijke rechtsbescherming open: bezwaar indienen bij het contactpunt en vervolgens (hoger) beroep bij de bestuursrechter. Immers, de schriftelijke beslissing van het contactpunt geldt als besluit in de zin van de Algemene wet bestuursrecht volgens artikel 34 van de Uitvoeringswet AVG. De in artikel 1.1 opgesomde deelnemers die optreden als contactpunt, zijn allemaal bestuursorganen in de zin van de Awb.

Als de betrokkene bezwaar indient, is het aan het contactpunt om een besluit op dat bezwaar te nemen. Ook dit doet het contactpunt in afstemming met de overige deelnemers.

Tweede lid

Op grond van dit lid wijst het contactpunt het verzoek af indien of voor zover naar het oordeel van één of meer van de deelnemers die betrokken waren bij de verwerking van de persoonsgegevens over de betrokkene, een uitzonderingsgrond van toepassing is. Hieruit volgt dat het contactpunt voorafgaand aan het nemen van een besluit moet overleggen, in ieder geval met de deelnemers die de persoonsgegevens hebben verstrekt of als resultaat hebben ontvangen. Zij kunnen immers een zwaarwegend belang hebben dat zich tegen inwilliging van het AVG-verzoek verzet, en kunnen aangeven of daarvan sprake is (bijvoorbeeld een toezichts-, opsporings- of vervolgingsbelang) en hoe zwaar dit zou moeten wegen voor eventuele beperking van de rechten van betrokkene overeenkomstig artikel 41 van de Uitvoeringswet AVG. Daarbij mag worden verwacht dat de benodigde motivering wordt verstrekt aan het contactpunt ten behoeve van de motivering van het besluit. Het artikel staat er niet aan in de weg dat op die manier de *feitelijke* voorbereiding van het besluit geschiedt door een andere deelnemer dan het contactpunt.

Dit artikellid laat door de zinsnede "of voor zover" de mogelijkheid open dat het contactpunt een AVG-verzoek gedeeltelijk inwilligt: als bijvoorbeeld een zwaarwegend belang van één deelnemer zich tegen inzage van de door deze deelnemer ingebrachte gegevens verzet, hoeft dat niet in de weg te staan aan inzage van door andere deelnemers ingebrachte gegevens. Gedeeltelijke inwilliging van het AVG-verzoek is daarentegen niet mogelijk indien een zwaarwegend belang ertoe noopt dat helemaal geen informatie wordt verstrekt. Dit kan bijvoorbeeld het geval zijn als een iCOV-aanvraag wordt gedaan in het kader van een embargo-onderzoek door de politie.

Uit dit lid volgt dat het AVG-verzoek wordt afgewezen indien naar het oordeel van één van de betreffende deelnemers een uitzonderingsgrond zich verzet tegen (gedeeltelijke) inwilliging van het verzoek. Aldus sluit het artikel uit dat meningsverschillen tussen deelnemers in de weg staan aan het kunnen nemen van een besluit door het contactpunt. Daarbij weegt zwaar dat het niet-honoreren van zwaarwegende belangen die nopen tot toepassing van een uitzonderingsgrond, onomkeerbare gevolgen kan hebben, zoals doorkruising van opsporings- of toezichtbelangen.

Overigens bevat artikel 17, derde lid, AVG andere (technische) uitzonderingsgronden die niet zien op de zwaarwegende belangen van deelnemers. Daarom is dit lid daarop niet van toepassing. Het contactpunt kan dan volstaan met overleg.

Derde lid

Consultatieversie nota van toelichting concept-BGS

Het is mogelijk dat de uitzonderingsgrond na verloop van tijd vervalt, bijvoorbeeld omdat toezichts- of opsporingsbelangen niet langer doorkruist zouden worden indien positief wordt besloten op het AVG-verzoek, zoals een inzageverzoek. Daarom regelt dit lid dat zodra naar het oordeel van de betreffende deelnemer de uitzonderingsgrond niet langer van toepassing is, de deelnemer dit zo spoedig mogelijk aan het contactpunt meldt. Hierdoor kan het contactpunt alsnog bijvoorbeeld inzage verlenen.

Artikel 1.3 Verantwoordelijkheid voor nakoming informatieplicht

(grondslag: artikel 1.4, vierde lid, onder a, WGS)

Eerste lid

Artikel 14 van de AVG verplicht elk van de deelnemers aan een samenwerkingsverband die de gezamenlijke verwerkingsverantwoordelijken zijn, om de betrokkene, behoudens uitzonderingen, te informeren over onder andere het feit dat gegevens over betrokkene worden verwerkt en voor welke doeleinden.⁴ Het onderhavige artikel bepaalt dat alleen de deelnemende overheidsinstantie die optreedt als het contactpunt, verantwoordelijk is voor de (coördinatie bij de) nakoming van deze informatieplicht, mits de deelnemers die betrokken waren bij de verwerking van persoonsgegevens over betrokkene, aan het contactpunt de nodige informatie verstrekken ter uitvoering van die plicht, met name over de vraag of een uitzonderingsgrond van toepassing is. Laten deelnemers dat na, dan zijn zij daarvoor zelf verantwoordelijk.

Met dit artikel wordt invulling gegeven aan artikel 1.4, vierde lid, onder a, WGS, dat bepaalt dat hierover bij amvb regels worden gesteld. Als beste praktijk beveelt het Europees Comité voor gegevensbescherming aan om een privacyverklaring op de website te plaatsen en de betrokkene daarnaar te verwijzen, bijvoorbeeld door een rechtstreekse link of QR-code.⁵

De informatieplicht en de rechten van betrokkene, zoals het recht op inzage en het recht op bezwaar, zijn nauw met elkaar verbonden. Daarom ligt het in de rede dat het contactpunt zowel verantwoordelijk is voor de (coördinatie bij de) informatieplicht als voor de nakoming van de rechten van betrokkene. Hierdoor kan een betrokkene, na te zijn geïnformeerd door het contactpunt, vervolgens bij datzelfde contactpunt terecht voor de uitoefening van zijn rechten op grond van de AVG. Ook zorgt deze regeling ervoor dat het contactpunt het overzicht binnen het samenwerkingsverband behoudt, en weet of betrokkene is geïnformeerd.

Tweede lid

In het tweede lid is de mogelijkheid opgenomen dat één of meer van de deelnemers die betrokken waren bij de verwerking van de persoonsgegevens over de betrokkene, zich kunnen verzetten tegen het feit dat een betrokkene geïnformeerd wordt, indien naar hun oordeel op grond van artikel 14, vijfde lid, onder b, van de AVG of artikel 41 van de Uitvoeringswet AVG een uitzonderingsgrond van toepassing is op de informatieplicht.

Op de informatieplicht gelden verschillende uitzonderingen, onder meer in geval van het doorkruisen van toezichts- en opsporingsbelangen (artikel 41, eerste lid, onder h en e, Uitvoeringswet AVG jo. artikel 23 AVG). Dit kan betekenen dat betrokkene niet of pas *na afronding* van een gezamenlijk project wordt geïnformeerd. Een relevante uitzondering doet zich verder voor als het verstrekken van de informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen of indien het verstrekken van de informatie de doeleinden van de gegevensverwerking zou doorkruisen (artikel 14, vijfde lid, onderdeel b, AVG).⁶ Bij de vraag of de rechtstreekse

⁴ Artikel 14 AVG ziet op gegevens die niet rechtstreeks van de betrokkene zijn verkregen. Dat is hier aan de orde, aangezien samenwerkingsverbanden de gegevens niet verkrijgen van betrokkenen, maar van de deelnemers. Daarom wordt artikel 13 van de AVG hier niet genoemd, waarin de informatieplicht is geregeld indien gegevens wel rechtstreeks van de betrokkene zijn verkregen.

⁵ Europees Comité voor gegevensbescherming, Richtsnoeren inzake transparantie overeenkomstig AVG, WP260 rev.01, punten 33 en 11.

⁶ Op de relevante excepties is nader ingegaan in paragraaf 3.4 van de memorie van toelichting bij de WGS (Kamerstukken II 2019/20, 35447, nr. 3).

Consultatieversie nota van toelichting concept-BGS

informatieverstrekking aan betrokkene onevenredig veel inspanningen zou kosten, mag in aanmerking worden genomen om hoeveel betrokkenen het gaat, hoe oud de gegevens zijn en welke passende waarborgen moeten worden ingebouwd.⁷ Eén passende maatregel, zoals gespecificeerd in artikel 14, vijfde lid, onder b, AVG die verwerkingsverantwoordelijken altijd moeten nemen is openbaar maken welke informatie wordt verwerkt. Een verwerkingsverantwoordelijke kan dit op verschillende manieren doen, bijvoorbeeld door de informatie op zijn of haar website te plaatsen of door proactief bekendheid te geven aan de informatie (privacy statement).⁸

Derde lid

Het is mogelijk dat de uitzonderingsgrond na verloop van tijd vervalt, bijvoorbeeld omdat toezichts- of opsporingsbelangen niet langer doorkruist zouden worden indien betrokkene wordt geïnformeerd. Daarom regelt dit lid dat zodra naar het oordeel van de betreffende deelnemer de uitzonderingsgrond niet langer van toepassing is, de deelnemer dit zo spoedig mogelijk aan het contactpunt meldt. Hierdoor kan het contactpunt de betrokkene alsnog informeren. Dat kan bijvoorbeeld het geval zijn indien later blijkt dat er geen risico's (meer) zijn, zoals in de situatie waarin de feitelijke uitvoering van de interventie inmiddels is gestart (tenzij er bijvoorbeeld nog een ander opsporingsonderzoek loopt) of de situatie waarin van een interventie wordt afgezien. Als de risico's zijn geweken, dient betrokkene alsnog te worden geïnformeerd over de eerdere gegevensverwerking door het samenwerkingsverband. Het kan echter voorkomen dat de belangen zodanig zijn dat ook op een later moment niet meer tot informeren kan worden overgegaan. Het contactpunt is verantwoordelijk voor de nakoming van de informatieplicht in de fase van gezamenlijke gegevensverwerking door het samenwerkingsverband.

Artikel 1.4 Verantwoordelijkheid voor nakoming meldplicht datalekken

(grondslag: artikel 1.4, vierde lid, onder a, WGS)

Eerste lid

Dit lid maakt duidelijk dat het contactpunt verantwoordelijk is voor de nakoming van de verplichting uit de artikelen 33 en 34 van de AVG om een inbreuk in verband met persoonsgegevens (een datalek) mede te delen aan de Autoriteit Persoonsgegevens en de betrokkene (de meldplicht datalekken), mits de deelnemers aan het contactpunt zo spoedig mogelijk de informatie verstrekken die het contactpunt nodig heeft voor de uitvoering van de voornoemde artikelen. Laten deelnemers dat na, dan zijn zij daarvoor zelf verantwoordelijk. De melding van een datalek gebeurt in afstemming met de gezamenlijke verwerkingsverantwoordelijken.

Dit lid sluit aan bij de verantwoordelijkheden van het contactpunt voor de nakoming van de informatieplicht jegens betrokkenen (artikel 14 AVG) en de nakoming van de rechten van betrokkenen op grond van hoofdstuk III van de AVG, zoals het inzagerecht. Het onderhavige artikel is alleen van toepassing op persoonsgegevens die worden verwerkt door het samenwerkingsverband.

Tweede lid

Dit lid regelt de mogelijkheid dat één of meer gezamenlijke verwerkingsverantwoordelijken zich verzetten tegen melding van een datalek indien dat naar hun oordeel noodzakelijk en evenredig is ter waarborging van een zwaarwegend belang als bedoeld in artikel 41 Uitvoeringswet AVG. Artikelen 33, eerste lid, en 34, derde lid, AVG en artikel 42 Uitvoeringswet AVG bevatten enkele andere meer technische uitzonderingsgronden. Daarvoor volstaat overleg met het contactpunt.

⁷ Europees Comité voor gegevensbescherming, Richtsnoeren inzake transparantie overeenkomstig AVG, WP260 rev.01, punt 61.

⁸ Europees Comité voor gegevensbescherming, Richtsnoeren inzake transparantie overeenkomstig AVG, WP260 rev.01, punt 64.

Artikel 1.5 Rechtmatig verwerkte gegevens

(grondslag: artikel 1.8, eerste lid, WGS)

Dit artikel expliciteert dat deelnemers alleen informatie mogen inbrengen in het samenwerkingsverband als zij die informatie rechtmatig verwerken. Dit is reeds beschreven in de brief van de Minister van Justitie en Veiligheid van 17 december 2021 aan de Tweede en Eerste Kamer.⁹ De rechtmatigheid behelst de vraag of de verstrekende instantie de gegevens zelf mag verwerken. Met rechtmatig verwerkte gegevens wordt bedoeld dat de deelnemer een grondslag heeft om deze te verwerken. Als het gaat om persoonsgegevens moet er een grondslag zijn in de zin van artikel 6 van de AVG of, als het gaat om politiegegevens of justitiële of strafvorderlijke gegevens of tenuitvoerleggingsgegevens, een grondslag in de zin van de Wpg of Wjsg. Dit is ter beoordeling van de verstrekende instantie. Als een deelnemer bijvoorbeeld een signaal bij het samenwerkingsverband aanmeldt, staat die deelnemer ervoor in dat hij de gegevens die hij daarbij aan het samenwerkingsverband verstrekt, zelf rechtmatig verwerkt.

Indien een deelnemer ten behoeve van de eigen taken en bevoegdheden gegevens verkrijgt of heeft verkregen *van een derde* en de deelnemer deze gegevens zelf mag verwerken, dan zijn dat ook rechtmatig verwerkte gegevens, zodat het onderhavige artikel zich niet verzet tegen verstrekking aan het samenwerkingsverband. Zoals opgemerkt in de memorie van toelichting bij de WGS valt te denken aan de data van het Kadaster of de Kamer van Koophandel waarvan een deelnemer voor zijn of haar taken rechtmatig gebruik mag maken¹⁰ of aan informatie uit publiek toegankelijke bronnen die door de inbrengende deelnemer rechtmatig mag worden verwerkt.¹¹ Het is aan de betreffende deelnemer om te beoordelen of deze gegevens conform artikel 1.5 WGS ingebracht moeten worden en of sprake is van zwaarwegende redenen die zich tegen verstrekking verzetten.

Het onderhavige artikel verzet zich er wel tegen dat een deelnemer op verzoek van (een deelnemer van) het samenwerkingsverband gegevens bij een derde vergaart om deze vervolgens in te brengen in het samenwerkingsverband. Een (deelnemer van een) samenwerkingsverband kan geen instructie of opdracht geven aan een deelnemer om bepaalde informatie bij een derde te verzamelen. De betreffende deelnemer moet deze gegevens initieel rechtmatig mogen verwerken vanuit eigen taken en bevoegdheden en zelf de afweging maken of deze gegevens dienen te worden ingebracht conform artikel 1.5 WGS.

Artikel 1.6 Kwaliteit van een aangemeld signaal, verzoek of casus

(grondslag: artikel 1.8, eerste lid, en artikel 1.4, vierde lid, onder a, WGS)

Eerste lid

Dit lid is een verbijzondering ten opzichte van het beginsel van juistheid, bedoeld in artikel 5, eerste lid, onder d, van de AVG. De juistheid en kwaliteit van de gegevens die bij een signaal, verzoek of casus worden verstrekt, moeten reeds vóór de aanmelding worden getoetst door de deelnemer die een signaal, verzoek of casus wil aanmelden. Hiermee wordt de verantwoordelijkheidsverdeling verduidelijkt inzake de nakoming van het beginsel van juistheid, bedoeld in artikel 5, eerste lid, onder d, AVG. Het artikel strekt zich ook uit tot andere gegevens dan persoonsgegevens, omdat ook onjuistheden in dergelijke gegevens ervoor kunnen zorgen dat ten onrechte of onjuiste persoonsgegevens worden verstrekt.

Deze uitdrukkelijke toets op juistheid en kwaliteit geldt in aanvulling op de startcriteria voor de gegevensverwerkingen, die zijn uitgewerkt in hoofdstuk 2. Uiteraard moeten de deelnemers ook bij de overige gegevensverstrekkingen zorgdragen dat zij voldoen aan het voornoemde beginsel van juistheid uit de AVG.

⁹ Kamerstukken II 2021/22, 35447, nr. 21, bijlage, punt 1.

¹⁰ In die zin: Kamerstukken II 2019/20, 35447, nr. 3, blz. 26.

¹¹ Kamerstukken II 2020/21, 35447, nr. 6, blz. 51-52 (antwoord 61).

Een concreet voorbeeld van hoe deze toets onder meer gestalte kan krijgen, is beschreven in de RIEC-procesbeschrijving integrale casusaanpak: "Alvorens persoonsgegevens door een of meer deelnemers aan het samenwerkingsverband ter bespreking worden ingebracht, hebben partijen de juistheid van de NAW-gegevens aan de hand van de vermelding in de Brp gecheckt."¹² Dat wil zeggen dat wordt gecontroleerd of de signalen betrekking hebben op een en dezelfde persoon. "Immers, persoonsverwisselingen dienen, mede gelet op de impact die deze registraties binnen het samenwerkingsverband RIEC op betrokkenen kunnen hebben, te worden voorkomen."¹³

Tweede lid

Bij inbreng in het samenwerkingsverband is het van belang dat de inbrenger de ingebrachte gegevens juist en actueel houdt, ook nadat een signaal vanuit het samenwerkingsverband aan een andere deelnemer is verstrekt. Dit is in dit lid geregeld. Voorop staat immers dat de deelnemer zelf verantwoordelijk is voor de juistheid van de persoonsgegevens die deze aan het samenwerkingsverband verstrekt bij de aanmelding van een signaal, verzoek of casus. Die deelnemer beschikt immers over de context op basis waarvan de juistheid en kwaliteit van de verstrekte gegevens kan worden getoetst.

Artikel 1.7 Correctie van onjuistheden tijdens gezamenlijke gegevensverwerking

(grondslag: art. 1.4, vierde lid, onder a, 1.8, eerste lid, 2.7, tweede lid, 2.14, tweede lid, WGS)

Eerste lid

Deze bepaling verduidelijkt dat de deelnemer die onjuiste gegevens heeft verstrekt ervoor verantwoordelijk is om onjuistheden te corrigeren die in de fase van gezamenlijke gegevensverwerking naar voren komen. Deze deelnemer dient er zorg voor te dragen dat alle redelijke maatregelen worden genomen om onjuiste gegevens onverwijld te wissen of rectificeren. Hiermee wordt de verantwoordelijkheidsverdeling verduidelijkt inzake de nakoming van het beginsel van juistheid, bedoeld in artikel 5, eerste lid, onder d, AVG. Verder is het van belang dat ook andere gegevens moeten worden gecorrigeerd als die niet juist blijken te zijn. Immers, ook onjuiste gegevens, niet zijnde persoonsgegevens, kunnen leiden tot een onnodige verwerking van persoonsgegevens of tot verwerking van persoonsgegevens die niet relevant zijn. De reikwijdte van dit lid is niet beperkt tot gegevens die bij de aanmelding zijn verstrekt, maar ziet ook op alle gegevens die zijn verstrekt in de fase van de gezamenlijke gegevensverwerking.

Tweede lid

Dit lid regelt een verplichting tot terugmelding van onjuistheden. Bij gebleken onjuistheden moet de deelnemer die de gegevens aan het samenwerkingsverband had verstrekt, dit – indien van toepassing – melden aan de organisatie waarvan die gegevens afkomstig zijn. Weliswaar regelt artikel 1.9, vierde lid, WGS een soortgelijke verplichting voor het specifieke geval van "geautomatiseerde gegevensanalyse", maar een dergelijke terugmeldingsplicht is ook van belang bij de reguliere vormen van gezamenlijke gegevensverwerking. Overigens geldt de verplichting tot terugmelding van onjuistheden aan *de bronhouder* in aanvulling op de verplichting uit de AVG om *de ontvanger* van persoonsgegevens in kennis te stellen van eventuele rectificaties (artikel 19 AVG).

Artikel 1.8 Kwaliteit van de resultaten

(grondslag: artikelen 1.8, eerste lid, 2.7, tweede lid, 2.14, tweede lid, WGS)

Eerste lid (toets op juistheid en kwaliteit voor verstrekking resultaat)

Dit lid waarborgt dat een samenwerkingsverband uitsluitend de resultaten van de gezamenlijke gegevensverwerking verstrekt aan een deelnemer of derde (overeenkomstig artikel 1.7 WGS) na

¹² Voor zover mogelijk binnen hun taken en bevoegdheden.

¹³ Werkproces integrale casusaanpak door het Regionaal Informatie en Expertise Centrum (RIEC), blz. 4.

Consultatieversie nota van toelichting concept-BGS

de feitelijke juistheid en de kwaliteit van de daarbij te verstrekken gegevens te hebben getoetst op aspecten die het samenwerkingsverband kan toetsen. Zo wordt voorkomen dat een niet op juistheid en objectiviteit geverifieerd resultaat wordt verstrekt, en dat ten onrechte een risico wordt gesignaleerd. Deze toets kan gestalte krijgen doordat binnen het samenwerkingsverband een conceptrapport of conceptproduct op kwaliteit en juistheid wordt gecontroleerd en wordt besproken voordat het definitief wordt. Het is afhankelijk van de complexiteit van het resultaat hoe intensief deze toets moet zijn. Bij een iCOV-rapportage die een feitelijk overzicht geeft van de inkomsten en het vermogen van een betrokkene op basis van feitelijke bronnen van meerdere overheidsorganisaties kan in beginsel steekproefsgewijs of marginaal worden getoetst, terwijl een resultaat dat bestaat uit een interventieadvies een intensieve toetsing behoeft.

Het samenwerkingsverband kan uitsluitend de aspecten toetsen op basis van de gegevens waarover het reeds beschikt van de deelnemers, want een samenwerkingsverband heeft geen bevoegdheden om eigenstandig nog allerlei gegevens te vergaren. Om die reden is opgenomen dat deze kwaliteits- en juistheidstoets alleen ziet op de aspecten die het samenwerkingsverband kan toetsen. Daarvoor is het aangewezen dat juist het samenwerkingsverband dit toetst. Dit is voornamelijk een basistest of het resultaat op de aan het samenwerkingsverband verstrekte gegevens gebaseerd kan worden. Na verstrekking van het resultaat blijft een check door de ontvanger nodig op de aspecten die de ontvanger kan toetsen. Indien een deelnemer een rapportage ontvangt met sturingsinformatie, moet die deelnemer eigenstandig vervolgonderzoek verrichten om deze sturingsinformatie te valideren.

Tweede lid (navolgbaarheid van de resultaten)

Dit lid waarborgt dat bij de verstrekking van sturingsinformatie of een interventieadvies wordt vermeld op basis van welke informatie het resultaat tot stand is gekomen. Het is van belang dat traceerbaar is op basis waarvan sturingsinformatie of een interventieadvies tot stand is gekomen. Het gaat dan onder meer om het antwoord op de vraag van welke partijen de informatie afkomstig is op basis waarvan de resultaten tot stand zijn gekomen. Deze informatie heeft de ontvanger nodig om de informatie te kunnen wegen: voor het vervolgonderzoek door de ontvanger van een resultaat, is vereist dat bekend is wat de input is geweest, zodat de ontvanger zich een beeld kan vormen van de betrouwbaarheid en volledigheid daarvan.

Met deze bepaling wordt gevolg gegeven aan de voorlichting van de Afdeling advisering van de Raad van State over de WGS, waarin werd gesteld dat mag worden verwacht dat het samenwerkingsverband bij de verstrekking van resultaten zoveel mogelijk motiveert op basis van welke informatie de signalering tot stand is gekomen.¹⁴ In reactie hierop is in de Kamerbrief van de toenmalige Minister van Justitie en Veiligheid van 17 december 2021 aangekondigd dat in de onderhavige amvb wordt geregeld dat samenwerkingsverbanden bij de verstrekking van resultaten aan deelnemers of derden, zoveel mogelijk moeten motiveren op basis van welke informatie de uitkomst tot stand is gekomen.¹⁵ Indien de ontvanger een bestuursorgaan is, wordt deze aldus in staat gesteld om gevolg te geven aan de motiveringsplicht uit de Algemene wet bestuursrecht en de daaruit voortvloeiende verplichting om te toetsen of de feiten juist zijn vastgesteld en of een voorgenomen besluit op deze feiten mag worden gebaseerd. Ook wanneer de interventie strafrechtelijk of van andere aard is, is het van belang dat navolgbaar is wat de aanleiding hiervoor is. Er zal altijd eigenstandig onderzoek verricht moeten worden naar aanleiding van ontvangen resultaten, conform wettelijke taken en bevoegdheden.

Bepaalde uitzonderingsgronden, zoals het opsporings- en vervolgingsbelang, kunnen zich verzetten tegen het verstrekken van (bepaalde aspecten van) de motivering. Om die reden is in het artikellid de zinsnede "voor zover mogelijk" opgenomen.

In de voornoemde Kamerbrief is tevens opgemerkt dat bij een dergelijke regeling rekening gehouden zal moeten worden met de verschillen in karakter van de werkzaamheden van de samenwerkingsverbanden. Het onderhavige artikellid is daarom alleen van toepassing op het motiveren van sturingsinformatie en interventieadviezen in de vorm van concrete producten. Het gaat dan om iCOV-rapportages, thematische of gebiedscans van RIEC's of gegevensanalyses van

¹⁴ Kamerstukken II 2021/22, 35447, H, blz. 16.

¹⁵ Kamerstukken II 2021/22, 35447, nr. 21, blz. 8 en 15.

het FEC. Dit lid is niet van toepassing op casuoverleggen (van een RIEC of Zorg- en Veiligheidshuis) of een signalenoverleg (van het FEC). Daarbij is geen sprake van een concreet product maar van mondelinge overleggen, waarin afstemming plaatsvindt over eventuele interventies. De benodigde deelnemers zitten steeds aan tafel. Gelet op deze afwijkende aard van de gegevensverwerking zou de voornoemde motiveringsplicht daarbij weinig zinvol zijn.

Artikel 1.9 Nationaliteit

(grondslag: artikel 1.8, eerste lid, WGS)

Zoals aangegeven in de Kamerbrief van 17 december 2021,¹⁶ en tijdens het wetgevingsoverleg in de Tweede Kamer over de WGS,¹⁷ mogen in de samenwerkingsverbanden op grond van de WGS geen persoonsgegevens worden verwerkt over nationaliteit, ras of etnische afkomst. Voor persoonsgegevens waaruit ras of etnische afkomst blijkt, volgt dit verbod uit artikel 9 van de AVG en artikel 22, eerste lid, van de Uitvoeringswet AVG. Een uitzondering geldt op grond van artikel 25, aanhef en onderdeel a, Uitvoeringswet AVG indien de verwerking geschiedt met het oog op de identificatie van de betrokkene, en slechts voor zover de verwerking voor dat doel onvermijdelijk is.

Met het onderhavige artikel wordt hetzelfde geregeld voor persoonsgegevens inzake nationaliteit. Dit betekent dat de samenwerkingsverbanden geen persoonsgegevens over nationaliteit mogen verwerken, tenzij dit voor de identificatie van betrokkene onvermijdelijk is. Dit is relevant voor de reikwijdte van de term "identificerende gegevens" in de artikelen 2.4, eerste lid, onder a, 2.12, eerste lid, onder a, 2.22, eerste lid, onder a, en 2.30, eerste lid, onder a, WGS. Voor andere doeleinden dan de identificatie van de betrokkene is de verwerking van persoonsgegevens over nationaliteit niet toegestaan.

Artikel 1.10 Nadere inkadering van gegevensuitwisseling tussen samenwerkingsverbanden

(grondslag: artikel 1.8, eerste lid, WGS)

Met het amendement-Yeşilgöz-Zegerius¹⁸ is artikel 1.7, achtste lid, aan de WGS toegevoegd. Dat bepaalt dat een samenwerkingsverband de resultaten van de gezamenlijke gegevensverwerking kan verstrekken aan een ander samenwerkingsverband in zin van de WGS voor zover de verstrekking noodzakelijk is voor het doel van het ontvangende samenwerkingsverband en uitsluitend voor zover de deelnemers die de betreffende persoonsgegevens aan het samenwerkingsverband hebben verstrekt, daarmee instemmen.

Gelet op deze voorwaarden is het geenszins beoogd dat een ongedefinieerde gegevensuitwisseling op gang kan komen tussen de samenwerkingsverbanden. De toelichting op het amendement noemt dat bij amvb nadere voorwaarden kunnen worden gesteld.¹⁹ Zoals is aangekondigd in de Kamerbrief van 17 december 2021 is het voornemen om bij amvb de gegevensverstrekking tussen de samenwerkingsverbanden nader te clausuleren.²⁰ Het eerste lid van het onderhavige artikel bevat deze nadere clausulering, en beperkt de gegevensuitwisseling tussen twee samenwerkingsverbanden tot vier relevante situaties:

- De situatie waarin twee samenwerkingsverbanden dezelfde betrokkene bespreken (eerste lid, onderdeel a).
- Een betrokkene wordt tegelijk in een RIEC en een Zorg- en Veiligheidshuis besproken (eerste lid, onderdeel b).
- Een betrokkene wordt tegelijk in een RIEC en het FEC besproken (eerste lid, onderdeel c).
- Degene die in een RIEC of het FEC wordt besproken, is onderwerp van een iCOV-rapportage (eerste lid, onderdeel d).

¹⁶ Kamerstukken 2021/22, 35447, nr. 21, paragraaf 7.1.

¹⁷ Kamerstukken 2020/21, 35447, nr. 20, blz. 37.

¹⁸ Kamerstukken 2020/21, 35447, nr. 14.

¹⁹ Namelijk op grond van artikel 1.8, eerste lid, van de wet.

²⁰ Kamerstukken 2021/22, 35447, nr. 21, bijlage, punt 7.

Consultatieversie nota van toelichting concept-BGS

Het onderhavige artikel heeft geen betrekking op onderlinge gegevensuitwisseling tussen meerdere RIEC's – dat is geregeld in artikel 2.20 WGS – en evenmin op onderlinge gegevensuitwisseling tussen meerdere Zorg- en Veiligheidshuizen – dat is geregeld in artikel 2.28 WGS.

Eerste lid, onderdeel a (twee samenwerkingsverbanden bevoegd)

Indien twee samenwerkingsverbanden in het concrete geval²¹ bevoegd zijn de casus te behandelen, mogen zij op grond van dit onderdeel uitsluitend gegevens uitwisselen over welke deelnemers in beide samenwerkingsverbanden betrokken zijn of zijn geweest bij de casus. Vervolgens kan de afstemming via de reguliere weg tot stand komen. Met onderdeel a, in samenhang gelezen met artikel 1.7, achtste lid, tweede volzin, van de wet wordt invulling gegeven aan de toezegging uit de Kamerbrief van 17 december 2021 om dit te regelen.²² Het kan ook voorkomen dat een deelnemer een casus aanmeldt bij een samenwerkingsverband dat tot de conclusie komt dat een van de andere samenwerkingsverbanden het meest aangewezen is om de casus te behandelen. Het ligt dan in de rede dat het samenwerkingsverband de deelnemer adviseert de casus zelf aan te melden bij dat andere samenwerkingsverband.²³

Eerste lid, onderdeel b (afstemming tussen RIEC en ZVH)

Met dit lid wordt gevolg gegeven aan de aankondiging uit de Kamerbrief van 17 december 2021 om voor gegevensuitwisseling tussen een RIEC en een Zorg- en Veiligheidshuis een alternatieve clausulering te onderzoeken, waarbij de gegevensuitwisseling wordt beperkt tot afstemming over geplande interventies in dezelfde casus.²⁴

Nadat een Zorg- en Veiligheidshuis en een Regionaal Informatie- en Expertisecentrum via de bekendheidscheck op grond van artikel 1.7, achtste lid, tweede volzin, vaststellen dat een betrokkene bekend is bij deze beide samenwerkingsverbanden, mogen zij uitsluitend gegevens uitwisselen die noodzakelijk zijn om het plan van aanpak van de deelnemers in het Zorg- en Veiligheidshuis af te stemmen op de afspraken van de deelnemers in het RIEC over interventies. Omdat de RIEC's tot doel hebben om georganiseerde criminaliteit te bestrijden, gaat het onder andere om situaties van mensenhandel en druggerelateerde activiteiten waarbij veelal misbruik wordt gemaakt van kwetsbare mensen. Zij worden dan bijvoorbeeld geëxploiteerd of ingezet voor criminele activiteiten. Afstemming tussen de deelnemers van een RIEC en van een Zorg- en Veiligheidshuis kan in dergelijke situaties van belang zijn. Een dergelijke samenwerking tussen Zorg- en Veiligheidshuizen met de overige WGS-samenwerkingsverbanden ligt veel minder voor de hand en valt daarom buiten de reikwijdte van deze bepaling. De analyses van financiële

²¹ Of beide samenwerkingsverbanden in het concrete geval dezelfde casus behandelen, kan blijken uit de bekendheidscheck op grond van artikel 1.7, achtste lid, tweede volzin, WGS waarmee een samenwerkingsverband kan vaststellen of een betrokkene bekend is bij een ander samenwerkingsverband. Het is hierbij wel van belang dat steeds per geval beoordeeld wordt of het noodzakelijk is om deze check uit te voeren. Het is niet toegestaan lijsten van betrokkenen uit te wisselen om te controleren of de betrokkenen op die lijst mogelijk ook besproken worden in dat andere verband. Er zou dan een ongedifferentieerde gegevensuitwisseling op gang kunnen komen tussen de verbanden. De zinsnede "ter vaststelling of de betrokkene bekend is" in artikel 1.7, achtste lid, bevestigt dat per geval een beoordeling plaatsvindt.

²² Kamerstukken 2021/22, 35447, nr. 21, bijlage, punt 7.

²³ Indien bijvoorbeeld het resultaat van bespreking in een RIEC is dat de besproken persoon kennelijk voldoet aan de criteria voor behandeling in het Zorg- en Veiligheidshuis, mag een deelnemer van het RIEC die ook deelneemt aan het Zorg- en Veiligheidshuis, deze persoon aldaar aanmelden en daartoe persoonsgegevens verstrekken op grond van artikel 2.31, eerste lid, van de wet. Concreet kan het bijvoorbeeld gaan om kwetsbare personen die onder druk van criminelen betrokken zijn geraakt bij het plegen van delicten en waar zorg en ondersteuning noodzakelijk zijn om iemand structureel op het rechte pad te krijgen. Het kan ook gaan om jeugdige familieleden in een netwerk waarin de familiebanden een belangrijke rol spelen bij het plegen en beramen van strafbare feiten en zorg en ondersteuning ingezet moeten worden om te voorkomen dat jeugdigen afglijden naar crimineel gedrag.

²⁴ Kamerstukken 2021/22, 35447, nr. 21, bijlage, punt 7.

Consultatieversie nota van toelichting concept-BGS

geldstromen of de integriteit van het financiële stelsel liggen daarvoor te ver af van het doel van het Zorg- en Veiligheidshuis.

De achtergrond voor de bevoegdheid tot informatie-uitwisseling tussen een RIEC en Zorg- en Veiligheidshuis is geweest dat VNG en Regioburgemeesters hebben aangegeven dat het uiterst omslachtig is om een bepaalde casus met dezelfde informatievraag zowel binnen een RIEC als binnen een Zorg- en Veiligheidshuis in te brengen, wanneer het bijvoorbeeld gaat om zorggegevens die nodig zijn in de aanpak van jeugdcriminaliteit en het voorkomen van jeugdige criminele aanwas.²⁵ In dat licht is artikel 1.7, achtste lid, WGS ingevoegd bij amendement.²⁶ De toelichting van het amendement wijst erop dat hiermee wordt bereikt dat bijvoorbeeld een RIEC de resultaten kan delen met een Zorg- en Veiligheidshuis wanneer criminele familieleden inwonen bij kinderen met jeugdzorgproblematiek teneinde de oorzaken beter te kunnen duiden en de kinderen beter te kunnen helpen. Door de voorwaarden uit artikel 1.7, achtste lid, van de wet aan te vullen met de voorwaarden uit het onderhavige artikel wordt voorkomen dat deze informatie-uitwisseling verder gaat dan noodzakelijk. Overigens gaat het louter om het uitwisselen van noodzakelijke informatie tussen samenwerkingsverbanden; de WGS geeft geen grondslag om over en weer aan te sluiten bij de besprekingen van de verschillende samenwerkingsverbanden.

Onderdeel b stelt een aanvullend vereiste voor de uitwisseling van gegevens tussen een RIEC en Zorg- en Veiligheidshuis. Eerst moet een bekendheidscheck hebben plaatsgevonden op grond van artikel 1.7, achtste lid, tweede volzin, van de wet. Vereist is immers dat betrokkene bekend is bij beide samenwerkingsverbanden. Als uit de bekendheidscheck blijkt dat betrokkene bekend is bij zowel een RIEC als Zorg- en Veiligheidshuis, mogen uitsluitend gegevens worden uitgewisseld tussen het RIEC en het Zorg- en Veiligheidshuis voor zover dat noodzakelijk is voor de afstemming van activiteiten van beide samenwerkingsverbanden. Het gaat dan bijvoorbeeld om situaties waarbij deelnemers in het RIEC voornemens zijn civielrechtelijke interventies te plegen jegens een persoon die tevens behandeld wordt in het Zorg- en Veiligheidshuis. Het is dan van belang dat het plan van aanpak in het Zorg- en Veiligheidshuis en de voorgenomen interventies door de deelnemers in het RIEC elkaar niet doorkruisen. Volgens dit onderdeel moet de gegevensuitwisseling worden beperkt tot dergelijke *afstemmingsinformatie*. Het is dus niet toegestaan dat onderliggende gegevens waarover een Zorg- en Veiligheidshuis beschikt, die een gedetailleerd beeld schetsen van de problematiek bij betrokkene, worden uitgewisseld met het RIEC, of dat bijvoorbeeld het Zorg- en Veiligheidshuis gegevens verstrekt aan het RIEC ten behoeve van het analyseren van signalen, casusoverleggen, thematische of gebiedscans. Met onderliggende informatie wordt onder meer bedoeld op het plan van aanpak en de notulen van de besprekingen.

Onderliggende informatie die van belang kan zijn, is in de meeste gevallen reeds bekend bij partijen die deelnemer zijn in beide samenwerkingsverbanden zoals de politie, het OM of een burgemeester. Zij kunnen gegevens waarover zij rechtmatig beschikken in het kader van hun eigen taakuitoefening, inbrengen bij het betreffende samenwerkingsverband zodat samenwerking plaatsvindt binnen de reguliere kaders van de samenwerkingsverbanden.

Eerste lid, onderdeel c (afstemming RIEC en FEC)

Het is mogelijk dat een betrokkene zowel in een FEC als in een RIEC wordt besproken, en dat het nodig is om af te stemmen over geplande interventies van deelnemers. Daarom regelt dit onderdeel dat indien het FEC en een RIEC via de bekendheidscheck op grond van artikel 1.7, achtste lid, tweede volzin, vaststellen dat een betrokkene bekend is bij deze beide samenwerkingsverbanden, zij gegevens mogen uitwisselen die noodzakelijk zijn om de interventies van deelnemers af te stemmen. In het RIEC zal doorgaans het accent meer liggen op het onderliggende delict, terwijl in het FEC meer de nadruk ligt op de financiële geldstroom.

²⁵ Brief aan Tweede Kamer van 25 november 2020, getiteld: 'Inbreng VNG en Regioburgemeesters voor WGO Wet Gegevensverwerking door Samenwerkingsverbanden 7 december'.

²⁶ Kamerstukken II 2020/21, 35447, nr. 14

Consultatieversie nota van toelichting concept-BGS

Voorbeelden van onderwerpen waar dit aan de orde kan zijn, zijn fraude met vastgoed, witwassen/ondermijning, en handel in cryptovaluta.

Eerste lid, onderdeel d (verstrekking iCOV-rapportage aan RIEC of FEC)

Indien iCOV een rapportage heeft verstrekt aan een deelnemer die ook deelneemt aan een RIEC of het FEC, moet de deelnemer deze rapportage kunnen inbrengen overeenkomstig de voorwaarden van artikel 1.7, achtste lid, eerste volzin, van de wet, indien in het RIEC of FEC een signaal wordt besproken over een persoon die onderwerp is van die rapportage. Dit is een bevoegdheid van de betreffende deelnemer; het RIEC of FEC kan geen opdracht geven om de iCOV-rapportage in te brengen. Verder is van belang dat wordt voldaan aan de voorwaarden van artikel 1.7, achtste lid, eerste volzin, van de wet. Dit betekent allereerst dat de iCOV-rapportage noodzakelijk moet zijn voor het doel van het andere samenwerkingsverband: daarvan kan sprake zijn als de iCOV-rapportage helpt om RIEC-deelnemers in staat te stellen om georganiseerde criminaliteit beter aan te pakken of als de FEC-deelnemers hierdoor risico's van inbreuken op de integriteit van het financiële stelsel beter kunnen aanpakken.²⁷ Tevens is vereist dat de deelnemers wier persoonsgegevens zijn gebruikt voor het opstellen van de iCOV-rapportage, instemmen met verstrekking aan een RIEC of het FEC.

Tweede lid (uitzondering beroepsgeheimen in de zorg)

Dit lid dient om gegevens die met doorbreking van de beroepsgeheimen op grond van de Wet inzake de geneeskundige behandelingsovereenkomst (WGBO), de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG) of de Jeugdwet zijn verstrekt bij de behandeling van een casus in het Zorg- en Veiligheidshuis, uit te sluiten van de verstrekking aan andere samenwerkingsverbanden. Indien deze gegevens onder de genoemde verstrekkingmogelijkheid zouden vallen, wordt het immers onmogelijk voor de betreffende professional om de gevolgen van zijn verstrekking te overzien, en om te beoordelen of deze nog passend is binnen zijn beroepsgeheim. De genoemde geheimhoudingsplichten dienen een maatschappelijk doel, namelijk het borgen van de onbelemmerde toegang tot zorg.

Hetzelfde geldt voor de gegevens die zijn verstrekt in het kader van procedures voor verplichte of gedwongen zorg. Ook deze zijn uitgesloten van de verstrekkingmogelijkheid op grond van artikel 1.7, achtste lid. De Wet verplichte geestelijke gezondheidszorg (Wvggz) en Wet zorg en dwang psychogeriatrische en verstandelijke gehandicapte cliënten (Wzd) beogen bescherming te bieden aan degenen die aan een procedure in het kader van verplichte of gedwongen zorg worden onderworpen en kennen een specifieke geheimhouding om die bescherming te borgen. Indien dergelijke gegevens na verstrekking in het Zorg- en Veiligheidshuis doorverstrekt kunnen worden aan andere samenwerkingsverbanden komt deze bescherming onder druk te staan.

Artikel 2.29, tweede lid, WGS kent al een specifieke inkadering voor de verstrekking aan het Zorg- en Veiligheidshuis die borgt dat deelnemers op basis van de specifieke omstandigheden in de casus de afweging maken of zij deze gegevens mogen verstrekken, en onder welke condities. Indien gegevens doorverstrekt mogen worden, kunnen de deelnemers hun geheimhoudingsplicht ten aanzien van de gegevens niet meer waarmaken. Daarnaast liggen de meer criminaliteitsgerichte doelen van de andere drie samenwerkingsverbanden dusdanig ver af van de doelen van het Zorg- en Veiligheidshuis dat verstrekking waarschijnlijk op gespannen voet staat met de in de bepalingen genoemde geheimhoudingen.

Derde lid (uitzondering verstrekking gegevens Rijksbelastingdienst)

De wet regelt in artikel 1.7, zesde lid, dat resultaten van samenwerkingsverbanden niet aan private deelnemers en private derden worden verstrekt ter behartiging van een gerechtvaardigd belang van die private deelnemer of private derde, voor zover zij mede gebaseerd zijn op

²⁷ Aangezien de iCOV-rapportages betrekking hebben op onrechtmatig financieel gewin en een casus in een RIEC of FEC daarop ook betrekking kan hebben, kan het voorkomen dat de verstrekking van een iCOV-rapportage noodzakelijk is om effectief te handelen in een RIEC of FEC. De iCOV-rapportage kan worden gebruikt om te bepalen in welke richting gezocht moet worden. Zo zijn deelnemers uit een RIEC of het FEC bijvoorbeeld beter in staat om te achterhalen hoe een netwerk om een subject eruit ziet, om een papieren constructie te weerleggen en om de juiste personen nader te onderzoeken.

gegevens van de rijksbelastingdienst, met uitzondering van de Fiscale Inlichtingen- en Opsporingsdienst. Het derde lid behelst een zelfde bepaling waar het gaat om de uitwisseling van gegevens tussen samenwerkingsverbanden, bedoeld in het eerste lid.

Artikel 1.11 Betrouwbaarheid geautoriseerde personen

(grondslag: artikel 1.8, derde lid, WGS)

Dit artikel regelt de autorisatie van personen die door hun deelnemende organisatie worden ingezet ten behoeve van het samenwerkingsverband voor de toegang tot de systemen waarin de deelnemers gezamenlijk persoonsgegevens verwerken. Zij moeten ten minste beschikken over een verklaring omtrent gedrag die voor indiensttreding bij de betreffende deelnemer vereist is, of ten minste zijn gescreend overeenkomstig de wettelijke bepalingen die van toepassing zijn op de respectievelijke deelnemers waar zij werkzaam zijn en van waaruit zij bij het samenwerkingsverband zijn betrokken.

In het geval van iCOV moet gelet op de aard van de toegang tot gevoelige informatie worden voldaan aan de eisen die gesteld worden aan het hoogste rubriceringsniveau van de gegevens waarmee wordt gewerkt (te denken valt aan de screening van politieambtenaren als politiegegevens worden behandeld). Bij de andere samenwerkingsverbanden is in belangrijke mate sprake van casusoverleggen of signalenoverleggen, waarin het kan voorkomen dat de inbreng van een deelnemer relatief beperkt of kortstondig is. Het zou dan praktisch niet werkbaar zijn om het screeningsniveau af te laten hangen van het hoogste rubriceringsniveau van de gegevens.

Dit artikel is grotendeels een codificatie van de screeningsvereisten die al zijn opgenomen in de toepasselijke protocollen en andere documenten. Zo is voor de Zorg- en Veiligheidshuizen reeds een VOG of een veiligheidsonderzoek vereist (artikel 13.3 template privacy protocol) en voor de RIEC's minimaal een VOG of screening overeenkomstig de bepalingen van de deelnemer (artikel 12.1, onder j, RIEC-privacyprotocol). Voor iCOV worden medewerkers die geautoriseerd worden voor de systemen waarin gezamenlijk gegevens verwerkt worden, door de AIVD gescreend als dit nog niet geregeld is vanuit de moederorganisatie.²⁸

Het gaat om functies van personen die toegang geven tot (gevoelige) informatie van de samenwerkingsverbanden die in belangrijke mate betrekking hebben op het veiligheidsdomein. Deze functies vereisen dat de betrokkene van onbesproken gedrag moet zijn. Een VOG is een verklaring waaruit blijkt dat iemands (justitiële) verleden geen bezwaar vormt voor het vervullen van een specifieke taak of functie in de samenleving. Voor zover sprake is van functies die "toegang [geven] tot gevoelige informatie bij de uitvoering van wettelijke taken op het terrein van openbare orde en veiligheid of handhaving van de rechtsorde", kan bij ministeriële regeling worden geregeld dat de VOG mede op grond van politiegegevens kan worden geweigerd. Het moet dan gaan om de functies waarin personen daadwerkelijk toegang hebben tot gevoelige informatie bij de uitvoering van voornoemde wettelijke taken. Met de Regeling aanwijzing functies VOG politiegegevens zijn limitatief functies aangewezen, die middels een verklaring omtrent het gedrag met politiegegevens (VOG politiegegevens) worden gescreend.²⁹ Dit is per 1 juli 2022 gebeurd voor onder meer functies die deelnemers van de RIEC's vervullen. Dit is geregeld in de Regeling aanwijzing functies VOG politiegegevens. In de toekomst zou in die ministeriële regeling bijvoorbeeld kunnen worden bepaald dat indien een VOG wordt aangevraagd voor geautoriseerde personen van andere samenwerkingsverbanden dan de RIEC's, zo'n VOG mede op grond van politiegegevens *kan* worden geweigerd (VOG politiegegevens). Het onderhavige artikel zorgt ervoor dat een VOG politiegegevens dan niet slechts *mogelijk* is, maar ook *verplicht* is voor deze personen, tenzij er is gescreend overeenkomstig de wettelijke bepalingen die van toepassing zijn op de betreffende deelnemer.

²⁸ BIO Handboek Informatiebeveiliging hoofdstuk 7 en iCOV Screeningsbeleid 2022.

²⁹ Ter uitvoering van artikel 35a Wjsg,

Consultatieversie nota van toelichting concept-BGS

Volledigheidshalve wordt opgemerkt dat indien een medewerker al een VOG heeft vanwege de indiensttreding bij de betreffende deelnemer in het kader van een soortgelijk beroep, er geen tweede VOG nodig is voor autorisatie in het samenwerkingsverband.

Het onderhavige artikel is eveneens van toepassing op de screening van de onafhankelijke auditors die de privacy audits verrichten op grond van artikel 1.10 van de wet. Zij zijn immers "geautoriseerde personen" in de zin van artikel 1.8, tweede lid, onder b, van de wet. ICT'ers vallen ook onder het onderhavige artikel, want zij zijn geautoriseerde personen op grond van artikel 1.8, tweede lid, aanhef en onder c, WGS: zij worden geautoriseerd vanwege het onderhoud of de ondersteuning van de systemen.

Het onderhavige artikel verzet zich geenszins tegen een strengere screening indien daartoe aanleiding is, mede gelet op de gevoeligheid van de data, bijvoorbeeld op grond van de Wet veiligheidsonderzoeken. In de Leidraad aanwijzing vertrouwensfuncties³⁰ staat beschreven op welke gronden een minister een vertrouwensfunctie kan aanwijzen. De Wet veiligheidsonderzoeken biedt de mogelijkheid om functies waarin de nationale veiligheid geschaad kan worden, aan te wijzen als zogeheten vertrouwensfunctie.

Alle uitgegeven toegangsrechten (autorisaties) moeten minimaal eenmaal per halfjaar worden beoordeeld conform de Baseline Informatiebeveiliging Overheid (BIO).³¹ Artikel 1.8, achtste lid, van de wet stelt naleving van de BIO wettelijk verplicht. Dit is een minimumeis; het meest in de rede ligt om wanneer personen geautoriseerd worden ten behoeve van een samenwerking gelijktijdig te controleren of bestaande autorisaties nog noodzakelijk zijn.

Artikel 1.12 Logging

(grondslag: artikel 1.8, vierde lid, WGS)

Artikel 1.8, vierde lid, van de wet verplicht de deelnemers om zorg te dragen voor de vastlegging langs elektronische weg (logging) van bij of krachtens algemene maatregel van bestuur te beschrijven verwerkingen van persoonsgegevens in geautomatiseerde systemen van het samenwerkingsverband. De vastgelegde gegevens mogen volgens artikel 1.8, vierde lid, WGS uitsluitend worden 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 gerechtelijke procedures". Vanuit audit-perspectief zijn goede logfiles zeer belangrijk; met de logfiles kunnen handelingen en acties worden herleid.

Als uitwerking van artikel 1.8, derde lid, van de wet verplicht dit artikel de deelnemers om de logging te laten plaatsvinden in lijn met de Baseline Informatiebeveiliging Overheid (BIO).³² Daarin is eveneens een loggingsplicht van de gegevensverwerkingen opgenomen. De BIO is door de ministerraad op 14 december 2018 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 die verplichten tot overheidsmaatregelen.

De BIO bevat ook regels over logging van de gegevensverwerking, die hierna worden toegelicht. Vanuit het oogpunt van eenvoud, consistentie en uitvoerbaarheid is het verkieslijk aan te sluiten bij dit bestaande kader. Met dit artikel wordt dit wettelijk verankerd. Concreet bevat de BIO de navolgende verplichtingen die ook relevant zijn voor samenwerkingsverbanden in de zin van de WGS.

Verplichting tot audit logging

Volgens de BIO dienen activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen te worden vastgelegd in audit-logbestanden. Deze

³⁰ <https://www.aivd.nl/actueel/nieuws/2014/09/08/nieuwe-leidraad-aanwijzing-vertrouwensfuncties>.

³¹ Zie punt 9.2.5.3 van de BIO. Staatscourant 2020 nr. 7857 en <https://www.bio-overheid.nl>.

³² Zie Staatscourant 2020 nr. 7857 en <https://www.bio-overheid.nl>.

Consultatieversie nota van toelichting concept-BGS

logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole. De BIO bepaalt onder meer het volgende (zie nader §12.4 van de BIO):

- *Over hetgeen moet worden gelogd:* maatregel 12.4.1 (gebeurtenissen registreren) schrijft voor dat logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren behoren te worden gemaakt en bewaard. De loggingsgegevens dienen periodiek te worden beoordeeld. Maatregel 12.4.1.1 vereist dat een logregel minimaal de volgende informatie moet bevatten: de gebeurtenis, de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon, het gebruikte apparaat, het resultaat van de handeling en de datum en het tijdstip van de gebeurtenis.
- *Over controles op de logs:* maatregel 12.4.1.3 vereist dat de informatieverwerkende omgeving wordt gemonitord door een Security Information & Event Management (SIEM) en/of Security Operations Center (SOC) middels detectievoorzieningen.³³ SOC en SIEM moeten volgens de BIO worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd. De Handreiking logging informatiebeveiligingsdienst³⁴ benadrukt dat het belangrijk is dat een organisatie actief controles uitvoert op de verzamelde logs. Alleen op die manier kan een organisatie misbruik van de omgeving en inbraakpogingen detecteren. Immers, als er wordt gelogd maar niemand ernaar kijkt, dan zou loggen zinloos zijn, aldus de Handreiking.
- *Over de bewaartermijn van de logs:* maatregel 12.4.2.2 schrijft voor dat ten behoeve van de loganalyse op basis van een expliciete risicoafweging de bewaarperiode van de logging wordt bepaald. Binnen deze periode moet de beschikbaarheid van de loginformatie worden gewaarborgd. Dit is uitgewerkt op blz. 11 van de Handreiking logging informatiebeveiligingsdienst, die uitgaat van een bewaartermijn van een half jaar, twee jaar of zeven jaar, afhankelijk van de mate van vertrouwelijkheid van de informatie.

Verplichting tot technische logging (controle van systeemgebruik)

Maatregel 9.4.4.2 van de BIO bepaalt dat het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen dient te worden gelogd. Een systeemhulpmiddel is een programma voor beheer en onderhoud van (informatie)systemen en ICT-infrastructuur. Deze logging moet een halfjaar beschikbaar zijn voor onderzoek. In de technische logging dienen gebeurtenissen te worden opgenomen zoals het gebruik van technische en functionele beheerfuncties, handelingen van beveiligingsbeheer, verstoringen in het productieproces en beveiligingsincidenten.

Artikel 1.13 Werkwijze van de rechtmatigheidsadviescommissie

(grondslag: artikel 1.8, zesde lid, WGS)

Algemeen

De artikelen 1.13 tot en met 1.15 bevatten de uitwerking van artikel 1.8, zesde lid, van de wet WGS door regels te stellen omtrent de werkwijze en de samenstelling van de rechtmatigheidsadviescommissie, de wijze van benoeming van haar leden en de instelling van één gezamenlijke rechtmatigheidsadviescommissie ten behoeve van een cluster van samenwerkingsverbanden. Artikel 1.13 bevat deze uitwerking voor de werkwijze van de rechtmatigheidsadviescommissie, artikel 1.14 voor de samenstelling van de

³³ Security Information & Event Management is software om de infrastructuur realtime te monitoren. Een Security Operations Center is verantwoordelijk voor het signaleren en opsporen van kwetsbaarheden in de operationele infrastructuur, het duiden van cyberdreigingen en het adviseren van tegenmaatregelen om bestaande risico's op te heffen.

³⁴ Zie de Handreiking Aanwijzing Logging BIO, <https://www.informatiebeveiligingsdienst.nl/product/aanwijzing-logging/>. De handreikingen bij de BIO bevatten – zoals het BIO het zelf omschrijft – “aanbevelingen in het kader van de bedrijfsvoering die geen verplichtend karakter hebben en niet essentieel zijn voor de werking van een stelsel”.

Consultatieversie nota van toelichting concept-BGS

rechtmatigheidsadviescommissie en artikel 1.15 voor de instelling van één gezamenlijke rechtmatigheidsadviescommissie voor een cluster van samenwerkingsverbanden.

Zoals aangekondigd in de brief van Minister van Justitie en Veiligheid van 17 december 2021 aan de Tweede en Eerste Kamer, moeten de rechtmatigheidsadviescommissies goed worden toegerust en wordt bij amvb de positie van de rechtmatigheidsadviescommissies verder versterkt. Daartoe strekt dit artikel.³⁵

Eerste lid

De taak van de rechtmatigheidsadviescommissies is reeds bepaald in artikel 1.8, zesde lid, van de wet: het structureel beoordelen van de rechtmatigheid van de verwerking van persoonsgegevens in het samenwerkingsverband bij nieuwe verwerkingen en wijziging in verwerkingen en het doen van voorstellen aan het samenwerkingsverband om onrechtmatigheden op te lossen. Dit lid voegt daaraan toe dat de commissie zowel gevraagd als ongevraagd kan adviseren ter uitoefening van haar wettelijke adviestaak.

De bepaling expliciteert bovendien dat de deelnemers ervoor moeten zorgen dat de rechtmatigheidsadviescommissie ten behoeve van haar wettelijke adviestaak naar behoren en tijdig in ieder geval wordt betrokken bij nieuwe verwerkingswijzen en wijzigingen daarvan. Om haar functie effectief te kunnen uitoefenen is het van belang dat de rechtmatigheidsadviescommissie voldoende en op tijd gevoed wordt met informatie over de plannen binnen een samenwerkingsverband. Gekozen is voor de formulering "verwerkingswijzen", want zoals beschreven in de memorie van toelichting op de wet ligt het in de rede dat bij verstrekkingen op casusniveau conform een in de WGS vastgelegde verwerkingswijze er in beginsel geen tussenkomst van de rechtmatigheidsadviescommissie nodig zal zijn; zij is nodig om uitspraken te doen over nieuwe verwerkingswijzen en over kwesties waarbij er twijfel bestaat over de rechtmatigheid van een verwerking.³⁶

Tweede lid

Zoals genoemd in de voornoemde Kamerbrief van 17 december 2021 zijn rechtmatigheidsadviescommissies bevoegd rechtstreeks aan het samenwerkingsverband te adviseren, zonder tussenkomst van leidinggevendenden, en worden zij geacht hierin onafhankelijk te opereren.³⁷ Dit is in dit lid geregeld. Het is noodzakelijk dat de leden van de rechtmatigheidsadviescommissie rechtstreeks kunnen adviseren aan de bestuurders van de deelnemende organisaties die het samenwerkingsverband aansturen, zonder afhankelijkheden of tussenkomst van management teams van de samenwerkingsverbanden. De adviezen zijn volgens artikel 1.8, zesde lid, van de wet immers bestemd voor het samenwerkingsverband, dus voor de deelnemers gezamenlijk. Daarbij behoort een duidelijke rolverdeling: de rechtmatigheidscommissie adviseert, de bestuurders van de deelnemers nemen de beslissingen. De adviezen zijn bestemd voor het leidinggevende niveau van de deelnemers die het samenwerkingsverband besturen, dat wil zeggen: de bestuurders van de deelnemers die het samenwerkingsverband aansturen. Het is belangrijk dat de adviezen daaraan worden verstrekt, gelet op de verwerkingsverantwoordelijkheid van de deelnemers.³⁸ Concreet gaat het om de leden van de bestuurlijke gremia van de deelnemers van waaruit de samenwerkingsverbanden worden aangestuurd. Te denken valt aan de FEC-Raad, het Opdrachtgeversoverleg iCOV, de stuurgroepen RIEC's en de stuurgroepen van de Zorg- en Veiligheidshuizen.

De functionarissen voor gegevensbescherming hebben op grond van artikel 38, tweede lid, van de AVG een recht op toegang tot de adviezen. Het ligt in de rede om hierop te anticiperen door de coördinerend functionaris voor gegevensbescherming voor het samenwerkingsverband, bedoeld in artikel 1.4, tweede lid, WGS een afschrift van (bepaalde) adviezen toe te zenden. Het is aan de

³⁵ Kamerstukken II 2021/22, 35447, nr. 21, bijlage, punt 9.

³⁶ Kamerstukken II 2019/20, 35447, nr. 3, blz. 60.

³⁷ Kamerstukken II 2021/22, 35447, nr. 21, bijlage, punt 9.

³⁸ Vergelijk artikel 38, derde lid, slotzin, AVG: "De functionaris voor gegevensbescherming brengt rechtstreeks verslag uit aan het hoogste leidinggevende niveau van de verwerkingsverantwoordelijke of de verwerker".

Consultatieversie nota van toelichting concept-BGS

rechtmatigheidsadviescommissie om te bepalen of zij het nodig vindt om een afschrift van het advies ook aan de coördinerend FG toe te sturen. Indien de verwerkingsverantwoordelijken besluiten af te wijken van het advies van de rechtmatigheidsadviescommissie, regelt het zesde lid dat zij verplicht zijn zowel aan de rechtmatigheidsadviescommissie als aan de coördinerend FG te rapporteren.

Derde lid

Volgens dit lid wordt over een advies besloten in overleg tussen de leden die afkomstig zijn van de deelnemers die het aangaat (ongeacht de vraag of de besluitvorming fysiek of in een andere vorm plaatsvindt). Het is daarbij niet noodzakelijk dat iedereen fysiek aanwezig is bij een overleg. Schriftelijke consultatie of schriftelijke goedkeuring van een voorgelegd advies is ook voldoende. Welke leden moeten worden betrokken, is afhankelijk van waar het zwaartepunt van het vraagstuk ligt. Gelet op de gezamenlijke verwerkingsverantwoordelijkheid zal een advies veelal alle leden in meer of mindere mate aangaan, zodat alle leden in de besluitvorming moeten worden betrokken. Het kan echter ook voorkomen dat een bepaald vraagstuk voornamelijk ziet op bepaalde deelnemers, bijvoorbeeld uit het opsporingsdomein. Het is dan gewenst dat de vertegenwoordigers van de opsporingsdiensten en/of het OM aan het overleg deelnemen. Zij zijn immers ingevoerd in de juridische ins- en outs van de Wpg en de Wjsg. Volgens deze bepaling kan niet zonder hen besloten worden over dat advies, ook al zijn de overige leden aanwezig. Er moet sprake zijn van besluitvorming die recht doet aan het type vraagstuk dat voorligt en waarin de concreet benodigde expertise wordt betrokken.

Voor het overige laat dit lid open op welke wijze de besluitvorming plaatsvindt. Het is goed mogelijk dat bepaalde vraagstukken ertoe nopen dat het belang van een bepaalde deelnemer zwaarder moet wegen dan dat van een andere deelnemer. Als in een bepaald rechtmatigheidsvraagstuk het medisch beroepsgeheim en de verwerking van gezondheidsgegevens een belangrijke rol speelt, dan zou het in die situaties voor de hand liggen dat aan de leden die voor de zorgpartijen deelnemen, een belangrijke rol wordt toebedeeld.

De wijze van besluitvorming wordt daarom verder overgelaten aan de rechtmatigheidsadviescommissie zelf. Zij heeft daarbij de bevoegdheid om nadere regels over de besluitvorming te stellen in het reglement van orde op grond van het vijfde lid.

Vierde lid

Dit lid maakt het mogelijk om bij een advies een individueel standpunt te voegen. Daarmee wordt tevens voorkomen dat in belangrijke vraagstukken principiële of fundamentele verschillen in opvatting tussen leden van de rechtmatigheidsadviescommissie dwingen tot het uitbrengen van compromis-adviezen. Deze bepaling moet niet zo worden uitgelegd dat een advies altijd schriftelijk moet zijn. Bij meningsverschillen tussen de leden ligt het echter wel in de rede dat het advies schriftelijk is.

Vijfde lid

De rechtmatigheidsadviescommissie kan een reglement van orde opstellen. Zo'n reglement zou bijvoorbeeld nuttig kunnen zijn voor de aanwijzing van de taken van de voorzitter, de wijze van overleg, en stemmingen.

Zesde lid

Ingevolge dit lid geldt een motiveringsplicht als wordt afgeweken van een advies. Dit betekent dat de bestuurders moeten motiveren waarom wordt afgeweken van het betreffende advies en welke risico-inschatting zij daaraan verbinden. Dit moet zorgen voor transparantie. De afwijking moet traceerbaar zijn en daartoe door de deelnemers worden gedocumenteerd, zodat later kan worden herleid waarom is afgeweken van een advies en zodat in een privacy audit kan worden onderzocht hoe het heeft uitgepakt. De afwijking van een advies wordt door de deelnemers gerapporteerd aan de rechtmatigheidsadviescommissie en de coördinerend functionaris voor gegevensbescherming voor het samenwerkingsverband.

Artikel 1.14 Samenstelling van de rechtmatigheidsadviescommissie

(grondslag: artikel 1.8, zesde lid, WGS)

Eerste lid (samenstelling)

Allereerst vereist dit artikellid dat elke deelnemer een of enkele personen benoemt tot lid van de rechtmatigheidsadviescommissie. De reden hiervoor is dat elke deelnemer een eigen wettelijk regime kent in de fasen voorafgaand aan gegevensverstrekking aan het samenwerkingsverband en volgend op de ontvangst van resultaten van de gegevensverwerking uit het samenwerkingsverband. Soms kennen verschillende diensten van een deelnemer op hun beurt elk een eigen wettelijke regime. De rijksbelastingdienst is een deelnemer waarvoor verschillende wettelijke regimes gelden, zoals de Algemene wet inzake rijksbelastingen, Algemene douanewet, Algemene wet inkomensafhankelijke regelingen en Invorderingswet 1990. Zie hiervoor de artikelen 2.3, eerste lid, onder d, 2.11, eerste lid, onder f, en 2.19, eerste lid, onderdeel b, WGS. De expertises die samengaan met de verschillende wettelijke regimes zijn niet te combineren in één persoon, waardoor meerdere personen vanuit de rijksbelastingdienst moeten kunnen deelnemen aan een rechtmatigheidsadviescommissie.

Verder stelt dit artikellid als eis dat de leden van de rechtmatigheidsadviescommissie beschikken over deskundigheid en ervaring op het gebied van de toepasselijke wetgeving inzake gegevensverwerking en de werking van het samenwerkingsverband. Bij de samenwerkingsverbanden gaat het om complexe vraagstukken en is goede expertise noodzakelijk. Het is immers van belang dat organisaties leden aanwijzen die in staat zijn adviezen uit te brengen die wellicht niet altijd in lijn liggen met de bestuurlijke wens, maar echt sec zien op de rechtmatigheid van hetgeen voorvalt.

Overigens verzet dit artikellid zich er niet tegen dat een rechtmatigheidsadviescommissie externe experts uitnodigt, indien het onderwerp waarover wordt geadviseerd daartoe aanleiding geeft. Het artikel biedt echter geen grondslag om met de externe experts persoonsgegevens te delen. Bij de vraag of externe experts worden uitgenodigd, ligt het voor de hand om eerst te kijken of intern – bij de deelnemers – voldoende expertise beschikbaar is.

Tweede lid (waarneming)

Voorkomen moet worden dat, als gevolg van de regel dat elke deelnemer ten minste één lid benoemt in de rechtmatigheidsadviescommissie, in geval van uitval of ontstentenis van één lid de werkzaamheden van de rechtmatigheidscommissie vertraging kunnen oplopen. Daarom is bepaald dat indien een lid voor een bepaalde deelnemer ontbreekt, die deelnemer aan het lid van een andere deelnemer kan verzoeken om waar te nemen. De waarneming vergt uiteraard dat de waarnemer zich bij de oordeelsvorming verplaatst in de context van de waargenomen organisatie.

Derde lid (private partijen)

In het kader van de praktische uitvoerbaarheid is toegevoegd dat deelnemende private partijen de mogelijkheid hebben om een of enkele leden te benoemen in de rechtmatigheidsadviescommissie, maar daartoe niet verplicht zijn. Deze mogelijkheid is met name van belang voor de Zorg- en Veiligheidshuizen, waar deelnemende private partijen uit de zorg een rol spelen vanwege onder meer het beroepsgeheim en tuchtrecht. Met deelnemende private partijen wordt bedoeld op deelnemers van het samenwerkingsverband die geen overheidsorgaan of overheidsinstantie zijn. Uit artikel 1.5, vierde lid, van de wet volgt overigens dat de private leden geen gegevens van de Belastingdienst mogen ontvangen.

Vierde lid

Dit lid vereist dat de deelnemers zorgdragen dat in de rechtmatigheidsadviescommissie ook aandacht is voor het tegengaan van risico's op ongelijke behandeling en discriminatie. Zoals bevestigd in de brief van Minister van Justitie en Veiligheid van 17 december 2021 aan de Tweede

en Eerste Kamer,³⁹ past dit binnen de taak van rechtmatigheidsadviescommissies op grond van artikel 1.8, zesde lid, van de wet om de rechtmatigheid van de verwerking van persoonsgegevens in het samenwerkingsverband structureel te beoordelen: deze taak ziet ook op het signaleren van mogelijke discriminatierisico's bij de gezamenlijke gegevensverwerking. De fase die volgt op de verstrekking van de resultaten aan de deelnemers – die naar aanleiding daarvan eventuele concrete interventies uitvoeren – valt buiten de reikwijdte van de WGS, zoals ook de Afdeling advisering opmerkt, net zoals de fase van verstrekking aan het samenwerkingsverband.⁴⁰ De deelnemers en de rechtmatigheidsadviescommissies moeten in de fase van gezamenlijke gegevensverwerking voor zover mogelijk anticiperen op mogelijke discriminatie of ongelijke behandeling die kan voortvloeien uit het verstrekken van resultaten.

Artikel 1.15 Rechtmatigheidsadviescommissie voor cluster van samenwerkingsverbanden

(grondslag: artikel 1.8, zesde lid, WGS)

Eerste lid

Dit lid regelt dat de RIEC's over één gezamenlijke rechtmatigheidsadviescommissie beschikken en de Zorg- en Veiligheidshuizen eveneens. Hiermee wordt de grondslag gebruikt uit artikel 1.8, zesde lid, WGS om dit te regelen. Voor de instelling van de gezamenlijke rechtmatigheidsadviescommissies wordt aanleiding gezien, omdat hierdoor uiteenlopende rechtmatigheidsadviezen tussen de verschillende regio's worden voorkomen. Dit is van belang voor de rechtszekerheid en voorspelbaarheid voor burgers. Bovendien worden met de instelling van één commissie de krachten gebundeld en de uitvoeringslasten beperkt. Gelet daarop ligt het niet in de rede dat de tien RIEC's en alle 33 Zorg- en Veiligheidshuizen ieder voor zich rechtmatigheidsadviescommissies zouden moeten instellen. Op de werkwijze van een gezamenlijke rechtmatigheidscommissie is artikel 1.13 van toepassing.

Tweede lid

Voor clusters van samenwerkingsverbanden, zoals de Zorg- en Veiligheidshuizen, is het wenselijk dat er voor lokale en regionale deelnemers de mogelijkheid is om personen uit vertegenwoordigende koepelorganisaties of brancheverenigingen van deelnemers te benoemen tot leden van de rechtmatigheidsadviescommissie. Gelet op de opsomming van de deelnemers van de Zorg- en Veiligheidshuizen in artikel 2.27 van de WGS valt hierbij te denken aan gemeenten (VNG), GGD (GGD-GHOR Nederland), reclasseringsinstellingen (Reclassering Nederland), regionale Veilig-Thuisorganisaties (Landelijk Netwerk Veilig Thuis), Jeugdbescherming (Jeugdzorg Nederland), GGZ (de Nederlandse GGZ), sociale wijkteams (Associatie Wijkteams). Om lid te worden van de rechtmatigheidsadviescommissie geldt het vereiste dat moet worden voldaan aan de algemene deskundigheidseisen die zijn verbonden aan het lidmaatschap van de rechtmatigheidsadviescommissie.

Artikel 1.16 Precisering maximale bewaartermijn

(grondslag: artikel 1.8, negende lid, WGS)

De hoofdregel van de maximale bewaartermijn is neergelegd in artikel 1.8, zevende lid, WGS: de persoonsgegevens die door het samenwerkingsverband gezamenlijk worden verwerkt, worden vernietigd of geanonimiseerd zodra zij niet langer noodzakelijk zijn voor het doel van het samenwerkingsverband, en worden in ieder geval uiterlijk vijf jaar na de datum van eerste verwerking verwijderd uit de systemen van het samenwerkingsverband of geanonimiseerd. Het onderhavige artikel bevat enkele preciseringen: enerzijds van gevallen waarin de gegevens in ieder geval eerder dan na vijf jaar dienen te worden gewist, anderzijds van de bijzondere gevallen

³⁹ Kamerstukken II 2021/22, 35447, nr. 21, paragraaf 7.2.

⁴⁰ In de fase voorafgaand aan de gezamenlijke gegevensverwerking zijn allerlei waarborgen en voorwaarden van toepassing op basis van het eigen wettelijke regime dat van toepassing is op een deelnemer (zoals de gezagsrol van de officier van justitie).

Consultatieversie nota van toelichting concept-BGS

waarin hernieuwde verwerking kan plaatsvinden volgens artikel 1.8, zevende lid, tweede volzin, WGS.

Eerste lid

In dit lid wordt geregeld dat de gezamenlijk verwerkte persoonsgegevens moeten worden gewist in het geval dat de analyse en bewerkingen door het samenwerkingsverband geen verdere aanwijzingen voor risico's met het oog op de doelen van het verband of sturingsinformatie hebben opgeleverd. Dit is aangekondigd in de brief van Minister van Justitie en Veiligheid van 17 december 2021 aan de Tweede en Eerste Kamer, in reactie op de aanbeveling van de Autoriteit Persoonsgegevens om dit te regelen.⁴¹ De gegevens dienen ook direct te worden gewist indien een aangemeld signaal, verzoek of casus niet in behandeling wordt genomen door het samenwerkingsverband. Dat kan voorkomen als niet is voldaan aan de vereisten voor gezamenlijke gegevensverwerking. Met het eerste lid is niet beoogd om uitputtend te regelen wanneer de persoonsgegevens moeten worden vernietigd of geanonimiseerd. Daarom is de zinsnede "onverminderd artikel 1.8, zevende lid, van de wet" opgenomen.

Tweede lid

Artikel 1.8, zevende lid, tweede volzin, van de wet geeft aan dat "in bijzondere gevallen" deelnemers persoonsgegevens ter beschikking kunnen stellen voor hernieuwde verwerking, mits dat noodzakelijk is voor het doel van het samenwerkingsverband. Zij moeten instemming hebben verkregen van de deelnemers die de betreffende persoonsgegevens hebben verstrekt. De onderhavige bepaling specificeert de bijzondere gevallen uit artikel 1.8, zevende lid, van de wet. Het moet gaan om een casus die in een Zorg- en Veiligheidshuis wordt behandeld en die voldoet aan onderdeel a of b van het onderhavige artikellid. Ook deze specificering van de bijzondere gevallen is aangekondigd in de voornoemde Kamerbrief van Minister van Justitie en Veiligheid van 17 december 2021.⁴²

De bepaling verduidelijkt allereerst dat de bevoegdheid tot hernieuwde verwerking alleen betrekking heeft op Zorg- en Veiligheidshuizen. Zoals aangegeven in de memorie van toelichting bij de WGS, is deze mogelijkheid opgenomen met het oog op de Zorg- en Veiligheidshuizen, omdat er soms gevallen zijn waarbij langdurige betrokkenheid van het Zorg- en Veiligheidshuis noodzakelijk is, namelijk bij langlopende casussen.⁴³ Anders dan bij de andere samenwerkingsverbanden in de WGS kan de uitvoering van een plan van aanpak in het Zorg- en Veiligheidshuis soms een langdurige periode van betrokkenheid vergen. Zoals aangegeven in de memorie van toelichting, speelt dit bijvoorbeeld bij personen met een hoog veiligheidsrisico als gevolg van chronische, ernstige psychische stoornissen. 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 1.8, zevende lid, eerste volzin, van de wet te kort blijken. Het gaat immers over complexe problematiek waarbij soms lange tijd ondersteuning nodig is om tot een duurzame oplossing te komen, of waarbij het risico bestaat op terugval. Bij de toepassing van het onderhavige artikel dient rekening te worden gehouden met bewaar- en vernietigingstermijnen uit bijzondere wetten. Zo kunnen op grond van de WGS vanuit het OM gegevens worden ingebracht (met beperking tot bepaalde artikelen) vanuit de Wvggz-taak van het OM. In de Wvggz zijn bewaar- en vernietigingstermijnen opgenomen met betrekking tot die gegevens. De mogelijkheden tot hernieuwde verwerking moeten er niet toe leiden dat Wvggz-gegevens langer bewaard worden in het Zorg- en Veiligheidshuis dan de bedoeling is op grond van de Wvggz, in het geval dat bijvoorbeeld ook Wvggz-gegevens opgenomen zijn in het plan van aanpak dat opgeslagen is in het systeem van het Zorg- en Veiligheidshuis.

Onderdeel a stelt dat het ter beschikking stellen voor hernieuwde verwerking mogelijk is als de casus nog niet is afgerond op het moment dat de wettelijke maximale bewaartermijn van vijf jaar

⁴¹ Kamerstukken II 2021/22, 35447, nr. 21, bijlage, punt 8.

⁴² Kamerstukken II 2021/22, 35447, nr. 21, bijlage, punt 8.

⁴³ Kamerstukken II 2019/20, 35447, nr. 3, blz. 128-129.

Consultatieversie nota van toelichting concept-BGS

na de eerste verwerking verstrijkt, omdat de problematiek dermate complex is dat de casus nog steeds voldoet aan de criteria voor behandeling in het Zorg- en Veiligheidshuis. De deelnemers dienen expliciet vast te stellen dat de casus nog steeds aan die criteria voldoet en moeten deze afweging vastleggen in het casusdossier (gelet op de verantwoordingsplicht uit artikel 5, tweede lid, AVG). Met de hernieuwde behandeling kan worden voorkomen dat alle gegevens worden vernietigd en vervolgens weer opnieuw moeten worden verzameld via een nieuwe aanmelding. De continuïteit wordt daarmee geborgd.

Te denken valt bij onderdeel a aan personen die voldoen aan de Ketenveldnorm en waarop de zogeheten levensloopbenadering wordt toegepast. Bij deze personen is sprake van chronische aandoeningen met een hoog veiligheidsrisico. Gezien de aard van de aandoening blijven de veiligheidsrisico's over een lange periode latent aanwezig. Langdurige en meerjarige samenwerking tussen partijen uit de verschillende ketens is dan noodzakelijk om het risico op nieuwe incidenten te voorkomen. De gezamenlijke strategie is dan vooral gericht op stabiliteit en het beheersbaar houden van de situatie, zowel voor de persoon zelf als voor de omgeving. De levenslooppaanpak kan soms jaren vergen, waarbij periodes dat het met de betrokkene beter gaat, afgewisseld worden met periodes waarin betrokken een hoog veiligheidsrisico vormt. Aaneengesloten dossierbeschikbaarheid en het aanhouden van de casus blijven dan nodig om de situatie snel in goede banen te leiden. De Zorg- en Veiligheidshuizen spelen een cruciale rol in de organisatie van de samenwerking tussen deelnemers uit het strafrechtelijke, bestuursrechtelijke, zorg- en sociaal domein rond deze doelgroep.

Het kan ook gaan om casuïstiek waarbij crimineel gedrag in combinatie met sociale problematiek van generatie op generatie wordt overgedragen. In dergelijke situaties is ook vaak een langdurige aanpak nodig om een betrokkene duurzaam uit deze vicieuze cirkel te trekken.

Onderdeel b maakt het mogelijk om de gegevens ter beschikking te stellen voor hernieuwde verwerking als de casus minder dan een jaar voor het verstrijken van de maximale bewaartermijn van vijf jaar is afgesloten. Daaraan is de voorwaarde verbonden dat dit alleen kan als de deelnemers, gezien de complexiteit van de problematiek, van oordeel zijn dat er een groot risico bestaat op terugval waardoor de casus binnen korte tijd opnieuw voldoet aan de criteria voor behandeling in het Zorg- en Veiligheidshuis. Dat betekent dat de gegevens nog enige tijd beschikbaar kunnen blijven voor het geval die terugval ook daadwerkelijk optreedt. Zo wordt voorkomen dat gegevens worden vernietigd en korte tijd later blijkt dat de casus weer opgestart moet worden en daarmee ook de gegevensverzameling weer opnieuw gestart moet worden.

Derde lid

Het derde lid beperkt de bewaartermijn bij hernieuwde beschikbaarstelling tot twee jaar. Indien nog steeds sprake is van een bijzonder geval als bedoeld in het tweede lid kan opnieuw hernieuwde beschikbaarstelling plaatsvinden. Dit vraagt steeds een specifieke en expliciete beoordeling en het vastleggen van de afweging in het dossier gelet op de verantwoordingsplicht uit artikel 5, tweede lid, AVG. Tevens dient betrokkene geïnformeerd te worden over de verlenging van de termijn.

De praktijk wijst uit dat het weinig voorkomt dat een casus na zeven jaar nog steeds voldoet aan de criteria, namelijk vrijwel uitsluitend als er tevens sprake is van chronische aandoeningen die een hoog veiligheidsrisico inhouden zoals hierboven beschreven in de toelichting op onderdeel a van het tweede lid. Terugval nadat een casus is afgesloten komt wel regelmatig voor. Maar als iemand pas na twee jaar weer in beeld komt voor behandeling bij het Zorg- en Veiligheidshuis, zijn de omstandigheden vaak dusdanig gewijzigd, dat deze beter opgepakt kan worden als een nieuwe casus.

Artikel 1.17 Opleiding en training ten aanzien van gegevensverwerking

(grondslag: artikel 1.8, negende lid, WGS)

Consultatieversie nota van toelichting concept-BGS

De Afdeling advisering van de Raad van State heeft in haar voorlichting over de WGS terecht benadrukt dat niet alles bij wet kan worden voorzien en dat de wetgever moet kunnen vertrouwen op een kwalitatief goede uitvoeringspraktijk. Volgens de Afdeling advisering is de adequate en zorgvuldige uitvoering en het investeren in professionaliteit en (juridische) deskundigheid op de werkvloer randvoorwaardelijk en daarmee urgent, ook voor wat betreft bijvoorbeeld de werking van algoritmen.⁴⁴ In reactie hierop is in de brief van de Minister van Justitie en Veiligheid aan de Eerste en Tweede Kamer van 17 december 2021 aangegeven dat de overheid vanzelfsprekend dient te waarborgen dat wordt geïnvesteerd in professionaliteit en (juridische) deskundigheid op de werkvloer, evenals in een cultuur waarin kan en mag worden afgeweken van algoritmische uitkomsten. Met het onderhavige artikel wordt beoogd daaraan bij te dragen door middel van een verplichting voor de deelnemers om ervoor te zorgen dat de medewerkers en de leden van de rechtmatigheidsadviescommissie passende opleidingen en trainingen krijgen op het gebied van een zorgvuldige omgang met persoonsgegevens, de regels die op het samenwerkingsverband van toepassing zijn, de werkprocessen van het samenwerkingsverband, methoden en technieken van informatieanalyse, informatiebeveiliging en data-ethiek.

Artikel 1.18 Uitwerking auditbepaling

(grondslag: artikel 1.10, vijfde lid, WGS)

Dit artikel is een uitwerking van artikel 1.10, vijfde lid, WGS, dat de verplichting bevat om nadere regels te stellen over de inhoud en wijze van controle door middel van periodieke privacy audits. Het onderhavige artikel zorgt ervoor dat de regels over audits uniform zijn voor alle samenwerkingsverbanden in de zin van de WGS.

De privacy audits zien volgens artikel 1.10, eerste lid, WGS op "de uitvoering van de bij of krachtens deze wet gegeven regels en de Algemene verordening gegevensbescherming".

Eerste lid

Met deze nadere regels over de frequentie van de audits is aangesloten bij artikel 6:5 van het Besluit politiegegevens, dat ertoe verplicht om audits op grond van de Wet politiegegevens twee jaren na inwerkingtreding van die wet te houden, en vervolgens eenmaal in de vier jaren.

Tweede lid

Volgens dit artikellid moet bij de privacy audit worden getoetst of, en in welke mate de maatregelen en procedures die in de adequate uitvoering van WGS, BGS en AVG moeten voorzien, in hun opzet, bestaan en werking bijdragen aan de naleving van die wettelijke voorschriften. Daarbij worden de gegevensverwerkingen beoordeeld op de naleving van de uit de wettelijke voorschriften voortvloeiende technische en juridische verplichtingen. De audit ziet bijvoorbeeld op de zorgvuldigheid van het werkproces waarin wordt bepaald welke deelnemers in de specifieke casus moeten deelnemen aan een casusoverleg, en de toetsing aan noodzaak, proportionaliteit en subsidiariteit.

Indien uit de controleresultaten blijkt dat niet wordt voldaan aan het bij of krachtens deze wet bepaalde, moet het samenwerkingsverband op grond van artikel 1.10, derde lid, van de wet binnen een jaar een hercontrole laten uitvoeren op die onderdelen die niet voldeden aan de regels. Uit artikel 1.10 WGS vloeit voort dat het dan aan de deelnemers van het samenwerkingsverband is om naar aanleiding van de auditresultaten maatregelen te nemen om geconstateerde onrechtmatigheden weg te nemen.

Derde lid

Dit artikellid verduidelijkt dat de auditor onafhankelijk moet zijn ten opzichte van de deelnemers van het samenwerkingsverband. Aan deze eis is bijvoorbeeld voldaan in het geval van de Auditdienst Rijk. Ook moet de auditor volgens dit artikellid beschikken over "deskundigheid en

⁴⁴ Kamerstukken I 2021/22, 35447, H, blz. 1, 2, 8, 16 en 19.

ervaring op het gebied van de werking van het samenwerkingsverband en de toepasselijke wetgeving inzake gegevensverwerking”.

De WGS en het onderhavige artikel verzetten zich er niet tegen dat een cluster van samenwerkingsverbanden – de RIEC’s of Zorg- en Veiligheidshuizen – kan beslissen om één gezamenlijke audit te doen verrichten.

Ook is het mogelijk dat anderszins een gecombineerde audit wordt gedaan, mits de auditor zich houdt aan zijn geheimhoudingsplicht met betrekking tot persoonsgegevens op grond van artikel 1.10, vierde lid, van de wet. Te denken valt aan een gecombineerde audit met een informatiebeveiligingsaudit.⁴⁵ Ook is een combinatie mogelijk met een audit die inzichtelijk maakt op welk kwaliteitsniveau of effectiviteitsniveau het betreffende samenwerkingsverband zich bevindt. De audit is in de voornoemde gevallen niet beperkt tot een audit in de zin van de WGS, maar richt zich ook op andere aspecten dan gegevensverwerking. De auditor kan echter op grond van artikel 1.8, tweede lid, onder b, van de wet uitsluitend worden geautoriseerd tot de systemen van het samenwerkingsverband ten behoeve van de “toetsing op rechtmatigheid”, en niet voor de andere aspecten dan de gegevensverwerking.

Volledigheidshalve wordt opgemerkt dat artikel 1.11 van dit besluit ook van toepassing is als minimumvereiste voor de screening van de onafhankelijke auditors die de privacy audits verrichten op grond van artikel 1.10 van de WGS. Ook zij zijn immers “geautoriseerde personen” in de zin van artikel 1.8, tweede lid, onder b, WGS.

HOOFDSTUK 2. BEPALINGEN INZAKE SPECIFIEKE SAMENWERKINGSVERBANDEN

PARAGRAAF 2.1 FINANCIËEL EXPERTISECENTRUM (FEC)

Artikel 2.1 Aanvullende deelnemers Programma Terrorismefinanciering

(grondslag: artikel 2.3, eerste lid, onder h, WGS)

Dit artikel wijst, in aanvulling op de deelnemers die in artikel 2.3 van de wet zijn aangewezen, de deelnemers aan het FEC aan voor het Programma Terrorismefinanciering. Het Programma Terrorismefinanciering brengt de strafrechtelijke, bestuursrechtelijke en fiscale informatie bij elkaar ten behoeve van de bestrijding van terrorismefinanciering, om deze informatie gedetailleerder te analyseren. Op basis van de verkregen inzichten kunnen passende interventies worden afgesproken. Interventies kunnen bijvoorbeeld de vorm krijgen van strafrechtelijke onderzoeken, onderzoeken en correcties door de Belastingdienst en onderzoeken en maatregelen door DNB.

Bij de aanwijzing van de aanvullende deelnemers is gekozen voor een continuering van de huidige situatie, op de wijze waarop die sinds 2018 structureel is ingeregeld. Artikel 2.3 van de WGS noemt de reguliere deelnemers, te weten OM, politie, Financiële inlichtingen eenheid (Financial Intelligence Unit - Nederland, hierna: FIU-Nederland), Belastingdienst, FIOD, AFM en DNB. Het onderhavige artikel voegt daaraan als deelnemers van het Programma Terrorismefinanciering toe: Bureau Financieel Toezicht, Koninklijke Marechaussee, Douane, Dienst Toeslagen en IND. Deze zijn alle nu ook al deelnemers aan dit programma.⁴⁶ Daarbij geldt de kanttekening dat de overige deelnemers tot op heden niet deelnemen aan de gezamenlijke verwerking en er derhalve geen

⁴⁵ Overheidsorganisaties – en dus ook samenwerkingsverbanden met overheidsorganisaties – zijn op grond van de Baseline Informatiebeveiliging Overheid verplicht tot beveiligingsaudits, indien sprake is van basisbeveiligingsniveau 2, waarvan hier sprake is. Zie maatregel 18.1.4.2, 18.2.1 en 18.2.1.2 van de Baseline Informatiebeveiliging Overheid.

⁴⁶ Bron: M. Wesseling / M. de Goede, *Beleid Bestrijding Terrorismefinanciering Effectiviteit en Effecten* (2013-2016), Universiteit van Amsterdam, 2018, blz. 171 en 175.

Consultatieversie nota van toelichting concept-BGS

gezamenlijke verwerkingsverantwoordelijkheid is. Onder de WGS is van beide elementen wel sprake. Dit vloeit voort uit artikel 1.4, eerste lid, van de wet. Dit betekent dat ook de aanvullende deelnemers gezamenlijke verwerkingsverantwoordelijken zijn, maar dan uitsluitend voor zover het gaat om gegevensverwerkingen ten behoeve van het Programma Terrorismedefinanciering. Er is één nieuwe partij ten opzichte van de bestaande situatie: het Bureau Toezicht Wwft is toegevoegd als deelnemer (onderdeel b), omdat dit als een van de toezichthouders op de naleving van de Wet ter voorkoming van witwassen en het financieren van terrorisme (hierna: Wwft) beschikt over relevante gegevens voor de bestrijding van terrorismedefinanciering. De FEC-deelnemers beogen met het Programma Terrorismedefinanciering (Programma TF) een bijdrage te leveren aan het tegengaan van financieren van terrorisme. Dat is een element van de doelstelling van het FEC uit artikel 2.3 WGS. De deelnemers beschikken over voor dit doel relevante (noodzakelijke) informatie en/of interventiemogelijkheden. Het programma richt zich meer concreet op:⁴⁷

- Het in kaart brengen van de financiële netwerken van bij de FEC-deelnemers bekende personen die in verband kunnen worden gebracht met terrorisme en andere relevante personen en entiteiten op basis van FEC-signalen. Daardoor wordt inzicht verkregen in de wijze waarop en door wie deze personen worden gefinancierd.
- Het opstellen van interventiestrategieën in alle gevallen waarin het verkregen inzicht daartoe aanleiding geeft.
- Het met de verworven kennis opstellen van getoetste typologieën van potentiële soorten terrorismedefinanciering en het verankeren van lessons learned bij betrokken partners.

De samenwerking in het Programma Terrorismedefinanciering geschiedt concreet in het FEC Terrorismedefinanciering Analyseteam. Dat is belast met de analyse van de tussen deelnemers uitgewisselde informatie op het gebied van bestrijding van terrorismedefinanciering ten behoeve van de samenwerking op het gebied van bestrijding van terrorismedefinanciering. Het FEC Terrorismedefinanciering analyseteam verzamelt, ordent, rangschikt, verrijkt, analyseert en registreert informatie in een signaledgebase met het oog op de uitvoering van haar taken. Hierop zijn de artikelen 2.6 (signalenoverleg) en 2.7 (gegevensanalyse) van de wet van toepassing, evenals de bijbehorende uitwerking in de artikelen 2.3 tot en met 2.5 van dit besluit.

Het Programma Terrorismedefinanciering moet worden onderscheiden van de Taskforce Terrorismedefinanciering van het FEC. In het Programma Terrorismedefinanciering gaat het om de vraag waar risico's en bepaalde netwerken zich bevinden. Dit kan bijvoorbeeld leiden tot het ontdekken van stichtingen die in verband kunnen worden gebracht met terrorismedefinanciering, waarna interventies kunnen worden afgesproken. Bij het Programma Terrorismedefinanciering wordt uitsluitend door overheidsinstanties samengewerkt. Bij de Taskforce Terrorismedefinanciering wordt daarentegen samengewerkt met banken en heeft de samenwerking een andere insteek (zie hierover de toelichting op artikel 2.2).

Artikel 2.2 Deelnemers aan publiek-private samenwerking

(grondslag: artikel 2.3, eerste lid, onder h, WGS en artikel 1.8, eerste lid, WGS)

Noodzaak publiek-private samenwerking binnen FEC

Het FEC zet in op het gezamenlijk voorkomen en bestrijden van het gebruik van het financiële stelsel voor financieel-economische criminaliteit, zoals witwassen, en andere vormen van ernstige, met name ondermijnende criminaliteit alsmede terrorismedefinanciering. Met het oog op dit doel werken de deelnemers aan het FEC al enige jaren samen met financiële instellingen. Dit artikel wijst deze private partijen aan als deelnemers aan het FEC voor activiteiten met dat doel. Tot op heden worden hiertoe met deze private partijen reeds gegevens gedeeld in zogeheten

⁴⁷ Bron: Informatieprotocol FEC 2019, blz. 7, FEC Jaarplan 2021, blz. 11 en Addendum bij het Informatieprotocol FEC 2014 inzake de samenwerking op het gebied van bestrijding van terrorismedefinanciering (Stcrt. 2015, nr. 18775).

Consultatieversie nota van toelichting concept-BGS

publiek-private "taskforces". Zoals in de memorie van toelichting bij de WGS is toegelicht,⁴⁸ is aanwijzing van bepaalde private partijen als deelnemers nodig omdat zij een bijdrage kunnen leveren aan het uitoefenen van publiekrechtelijke taken en bevoegdheden, zoals bedoeld in artikel 2.2 van de WGS.

Aanpak van misbruik financiële stelsel voor criminaliteit

De private deelnemers aan het FEC nemen uitsluitend deel voor zover het gaat om de in het onderhavige artikel beschreven specifieke verwerkingen in publiek-private taskforces. Concreet gaat het dan om twee taskforces die onder de vlag van het FEC functioneren: de Taskforce Terrorismefinanciering en de Serious Crime Taskforce. In deze taskforces werken enkele publieke deelnemers van het FEC samen met private partijen ten behoeve van het voorkomen en bestrijden van het gebruik van het financiële stelsel voor terrorismefinanciering, financieel-economische criminaliteit en andere ernstige vormen van criminaliteit, zoals witwassen. Deze publieke partijen delen daarover concrete aanknopingspunten met banken, zodat de banken gericht kunnen zoeken naar aanwijzingen voor terrorismefinanciering en (financiering van) andere ernstige vormen van criminaliteit, waarna zij deze aanwijzingen kunnen melden aan de bevoegde publieke autoriteiten. Dit betreft met name de FIU-Nederland en de politie. Ook worden in de taskforces interventiestrategieën opgesteld in de gevallen waarin het verkregen inzicht daartoe aanleiding geeft. Verder worden typologieën in kaart gebracht van potentiële soorten terrorismefinanciering en financiering van financieel-economische criminaliteit en andere ernstige vormen van criminaliteit.

Tot op heden nemen de volgende private partijen deel aan de taskforces: ING Bank, ABN Amro Bank, Rabobank, Volksbank, Aegon, Triodos en KNAB. Bij ministeriële regeling moeten de banken worden aangewezen. Het zou onevenredig zijn om alle banken te laten deelnemen, maar het is wel mogelijk om deze banken tezamen een groot marktaandeel te laten vertegenwoordigen. Er wordt ook samengewerkt met de Nederlandse Vereniging van Banken (NVB), maar daarmee worden geen persoonsgegevens uitgewisseld.⁴⁹ Buiten de taskforces vindt in de zogeheten "projecten" publiek-private samenwerking met de financiële instellingen plaats, zonder persoonsgegevens uit te wisselen.⁵⁰

Publieke partijen: OM, politie, FIU-Nederland en FIOD

Tot op heden nemen aan de Taskforce Terrorismefinanciering en de Serious Crime Taskforce van de publieke deelnemers van het FEC uitsluitend OM, politie, FIU-Nederland en FIOD deel. Zij zijn aangesloten omdat zij zich bezighouden met (voorbereiding van) opsporing en vervolging. Het onderhavige artikel bepaalt dat uitsluitend deze vier van de in artikel 2.3 in de wet genoemde partijen deelnemen aan de gegevensverwerkingen in de taskforces. Van de overige reguliere FEC-

⁴⁸ MvT, blz. 75-76: "Zo is bijvoorbeeld het voorkomen van witwassen en terrorismefinanciering een publiekrechtelijke taak, waarin niet alleen diverse publieke partijen, zoals de in artikel 2.3 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 en notarissen, de zogenoemde poortwachtersfunctie." Zie ook blz. 22 en 23: "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. (...) 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."

⁴⁹ De NVB kan aan de niet-deelnemende banken typologieën verstrekken inzake bepaalde financieringsstromen die verband houden met terrorismefinanciering, financieel-economische criminaliteit of andere ernstige vormen van criminaliteit. Hier kunnen de niet-deelnemende banken lering uit trekken, waarna zij de typologieën kunnen implementeren en de betreffende financieringsstromen waar nodig kunnen aanpakken. Indirect profiteren de niet-deelnemende banken via de NVB dus ook van de taskforces.

⁵⁰ Bijvoorbeeld projecten voor de aanpak van misbruik van het financiële stelsel voor corruptie, beleggingsfraude, witwassen in verband met uitbuitingssituaties en het gebruiken of opzetten van handelsstructuren om crimineel geld wit te wassen.

Consultatieversie nota van toelichting concept-BGS

deelnemers is deelname niet benodigd voor deze taskforces. Uit artikel 1.4, eerste lid, van de wet volgt dat deze niet-deelnemers geen verwerkingsverantwoordelijkheid dragen voor de taskforces.

Taskforce Terrorismedinanciering

De gegevensverwerking in de Taskforce Terrorismedinanciering houdt in dat vanuit de politie of FIOD de identificerende gegevens worden ingebracht van een persoon die in verband kan worden gebracht met (de financiering van) terrorisme. Vervolgens doen de banken hun werk op basis van de Wwft: monitoren op ongebruikelijke transacties. Door te beschikken over de naam kunnen zij gericht zoeken in hun systemen. Waar nodig wordt door de banken met de andere banken informatie uitgewisseld. Voor zover de gegevens onder de reikwijdte van de geheimhoudingsplicht van de Wwft vallen (zoals gegevens over ongebruikelijke transacties), mogen banken die onderling uitsluitend delen onder de voorwaarden van artikel 23, zesde lid, onder 3° Wwft. Als een bank een ongebruikelijke transactie vindt, beslist die bank of een melding aan de FIU-Nederland volgt. Door het delen van politiegegevens van subjecten die in verband kunnen worden gebracht met (de financiering van) terrorisme worden de banken beter in staat gesteld ongebruikelijke transacties met betrekking tot de financiering van terrorisme te identificeren en te melden aan de FIU-Nederland. Hiermee kunnen de banken onderzoek doen naar transacties van (rechts)personen waarmee het subject transacties uitvoert (tweedegraads transacties). De banken mogen advies vragen aan de FIU-Nederland om te bepalen of deze transacties meldingswaardig zijn en de FIU-NL zal hen desgevraagd daarover voorlichten.

Voor de publieke partijen dragen meldingen van ongebruikelijke transacties na analyse en verdacht-verklaring door de FIU-Nederland bij aan het voorkomen en opsporen van terrorisme en de financiering daarvan. Transacties die door de FIU-Nederland verdacht worden verklaard komen ter beschikking aan de opsporingsdiensten. Het is daarmee enerzijds voor publieke deelnemers van belang om zo gericht mogelijk ongebruikelijke transacties te kunnen detecteren, en daar is de Taskforce op gericht. Anderzijds is dit van belang voor de private deelnemers: zij zijn op grond van de Wwft verplicht om indien daartoe aanleiding is een Wwft-melding te doen.

De Terrorismedinanciering Taskforce is beschreven in een convenant uit 2019.⁵¹

Serious Crime Taskforce

Door de Serious Crime Taskforce is het mogelijk dat politie en FIOD in afstemming met het OM namen van adviseurs of rechtspersonen die in beeld zijn, doorgeven aan de deelnemende banken. De banken kunnen die namen op hun beurt weer koppelen aan bepaalde ongebruikelijke transacties. Wanneer de gegevens over die transacties worden teruggeleverd aan politie en FIOD kunnen die een opsporingsonderzoek beginnen. Het gaat om subjecten tegen wie nog geen concrete verdenking is in een situatie dat er wel duidelijke en objectieve aanwijzingen bestaan als bedoeld in artikel 2.4. Met Serious Crime wordt in het bijzonder gedoeld op criminaliteitsvormen waarbij tussenpersonen het financiële stelsel misbruiken voor het verplaatsen van omvangrijke criminele winsten en omzetten, zoals de handel in en de productie van harddrugs, het verhullen en witwassen van crimineel vermogen en het faciliteren van betalingen voor extreem geweld en corruptie, zoals geduid in het Nationaal Inlichtingen Beeld Ondernijning. De werkwijze van de Serious Crime Taskforce vertoont veel parallellen met de hiervoor beschreven werkwijze van de Taskforce Terrorismedinanciering, met dien verstande dat bij de Serious Crime Taskforce specifiek wordt gezocht naar andere typen transacties, namelijk transacties die zicht geven op het mogelijk criminele (faciliterende) netwerk van het ingebrachte subject, zoals transacties die zicht kunnen geven op een (financiële) modus operandi en transacties met witwassenmerken. De Serious Crime Taskforce is beschreven in een convenant uit 2019.⁵²

Artikel 2.3 Beperking gegevensverstrekking over kring van personen

(grondslag: artikel 2.4, tweede lid, WGS)

⁵¹ [Staatscourant 2019, 43628](#) met addendum in [Staatscourant 2020, 46050](#).

⁵² Zie [Staatscourant 2019, 43629](#) met addendum in [Staatscourant 2021, 25818](#).

Eerste lid

Dit lid regelt dat de deelnemers ten behoeve van het Programma FEC Terrorismefinanciering en de publiek-private taskforces *tot maximaal drie directe lijnen* vanaf de betrokken persoon gegevens verwerken over relevante relaties of contacten als bedoeld in artikel 2.4, eerste lid, onderdeel e, van de wet. Dat betreft relevante relaties of contacten van natuurlijke personen of rechtspersonen die mogelijk in verband gebracht kunnen worden met mogelijke financiering van terrorisme, met onverklaarbare of criminele vermogensbestanddelen of witwasconstructies, of andere financieel-economische criminaliteit. Dat er gegevens worden verwerkt tot en met de tweede graad – dat wil zeggen: drie lijnen – is conform de praktijk in het Programma Terrorismefinanciering en de publiek-private taskforces. Hierbij vindt een proportionaliteitstoets plaats, dus zodat aan de tweede graad alleen wordt toegekomen indien dat proportioneel is.

Tweede lid

Om rekening te kunnen houden met constructies waarbij het vermogen verderop in de keten wordt verhuisd, maakt dit lid een uitzondering: tot een ruimere verstrekking van gegevens over relaties of contacten kan worden overgegaan, indien sprake is van een keten van vermogensverschaffers, leidinggevenden, zeggenschaphebbenden of personen die in een zakelijk samenwerkingsverband staan tot de betrokken natuurlijk persoon of rechtspersoon, voor zover die gegevens noodzakelijk zijn voor het doel van het FEC. Gemotiveerd moet worden waarom de gegevensverstrekking in meer dan drie lagen noodzakelijk is. De motivering kan worden gegeven aan de hand van de taakstelling van de betrokken deelnemers. De motivering is naar zijn aard niet altijd vooraf in concreto te geven en kan er ook uit bestaan dat vermoedelijk sprake is van complexe criminele structuren, waarin relaties vaak diep verborgen zijn, die inzichtelijk moeten worden door de rapportage.

Het onderhavige artikel heeft geen betrekking op de reguliere activiteiten van het FEC. Een ruimere kring van personen moet daarbij namelijk mogelijk blijven voor reguliere signalen, in het geval daar noodzaak toe is voor het doel van het FEC. Dit is in overeenstemming met de huidige praktijk.

Artikel 2.4 Criteria voor behandeling van een signaal of verzoek

(grondslag: artikel 2.6, tweede lid, en 2.7, tweede lid, WGS)

In het FEC bestaat het startpunt van de gegevensverwerking concreet uit ingebrachte signalen (artikel 2.6 WGS) of een verzoek tot gezamenlijke gegevensanalyse (artikel 2.7 WGS). Het onderhavige artikel stelt cumulatieve criteria aan het signaal of verzoek. Wanneer niet wordt voldaan aan één of meerdere criteria, mogen signalen of verzoeken over een persoon niet in het FEC worden behandeld. Met dit artikel wordt tevens invulling gegeven aan de toezegging uit de Kamerbrief van 17 december 2021 om het startpunt van de gegevensverwerking zoveel mogelijk te concretiseren.⁵³

Eerste lid (criteria voor aanmelding signaal of verzoek)

Het is van groot belang dat een bij het FEC ingebracht signaal⁵⁴ of verzoek om een gegevensanalyse gedegen wordt onderbouwd. Daartoe strekken allereerst de criteria a en b. Er moet sprake zijn van duidelijke en objectieve aanwijzingen van risico's van inbreuken op de integriteit van het financiële stelsel als bedoeld in artikel 2.2 van de wet. Dit maakt concreter wanneer de gegevensverwerking noodzakelijk is voor het doel van het FEC. Het criterium van de "duidelijke en objectieve aanwijzingen" is overgenomen uit het advies van de Autoriteit Persoonsgegevens, waarin werd geadviseerd om een duidelijk en objectief signaal op basis van

⁵³ Kamerstukken II 2021/22, 35447, nr. 21, bijlage, punt 1.

⁵⁴ Signaal is gedefinieerd in artikel 1.1 WGS: "melding van een of meer deelnemers in een samenwerkingsverband dat bepaalde gedragingen of situaties betreffende natuurlijke personen, rechtspersonen of fenomenen aanleiding kunnen zijn om ten behoeve van het doel van het samenwerkingsverband gezamenlijk gegevens te verwerken".

Consultatieversie nota van toelichting concept-BGS

voldoende aanwijzingen als startpunt neer te leggen voor alle samenwerkingsverbanden.⁵⁵ In reactie hierop is in de Kamerbrief van 17 december 2021 aangegeven dat de regels over het startpunt voldoende precies en duidelijk moeten zijn en dat daarom bij amvb het startpunt van de gegevensverwerking zoveel mogelijk wordt geconcretiseerd door nadere criteria.⁵⁶ De criteria uit het eerste lid gelden ook voor het Programma Terrorismefinanciering. De criteria in de onderdelen a tot en met d zijn cumulatief.

Criterium a waarborgt dat er duidelijke en objectieve aanwijzingen moeten zijn dat het signaal of verzoek is gerelateerd aan een risico van een inbreuk op de integriteit van het financiële stelsel, zoals omschreven in artikel 2.2 van de WGS. Dit criterium vereist dat duidelijk gemaakt wordt dat het signaal of verzoek past binnen het doel van het FEC. Dit betekent dat de signalen of verzoeken betrekking moeten hebben op risico's van inbreuken op de integriteit van het financiële stelsel die door de uitoefening van publiekrechtelijke taken en bevoegdheden van de deelnemers kunnen worden bestreden of weggenomen. De integriteit van het financiële stelsel kan bedreigd worden door onder meer witwassen van criminele gelden (in de vastgoedsector), illegaal bankieren, beleggingsfraude of fiscale fraude. De signalen of verzoeken zien op alle onderwerpen van financieel economische criminaliteit in het financiële stelsel, zoals witwassen, belastingontwijking, overtredingen van sanctieregelgeving, fraude en oplichting, illegaliteit en het niet voldoen aan eisen van integere bedrijfsvoering zoals opgenomen in de Wft en de Wwft.⁵⁷

Criterium c vereist dat de analyse van het verzoek of signaal naar verwachting de samenwerking vergt met meerdere deelnemers van het Financieel Expertisecentrum. Immers, als het evident is dat de analyse van het signaal adequaat kan plaatsvinden met bevoegdheden tot onderlinge gegevensuitwisseling tussen twee deelnemers bij of krachtens een andere wet dan de WGS, dan moet die weg worden bewandeld. Dan zou behandeling in het FEC niet voldoen aan de vereisten van noodzakelijkheid, subsidiariteit en proportionaliteit. Overigens is voor dit criterium niet relevant of een signaal of verzoek naar verwachting slechts relevant is voor de *taakuitoefening van één deelnemer*.

Criterium d vereist dat het signaal of verzoek een vermelding omvat van de onderliggende feiten, omstandigheden en gedragingen, de betrokken rechtspersoon, natuurlijke persoon of het object en, indien een verzoek wordt gedaan tot een gegevensanalyse, een afbakening van de benodigde informatie.

Uit artikel 1.6 volgt overigens dat de deelnemer die het signaal of verzoek aanmeldt, bij de aanmelding bevestigt dat hij de daarbij verstrekte gegevens overeenkomstig artikel 1.6, eerste lid, voor zover mogelijk heeft getoetst op feitelijke juistheid en de kwaliteit.

Tweede lid (startpunt gegevensverwerking taskforces)

In de FEC Taskforce Terrorismefinanciering en de FEC Serious Crime Taskforce bestaat het startpunt van de gegevensverwerking uit concrete aanknopingspunten van politie en/of FIOD die financiële instellingen moeten helpen gericht te zoeken naar aanwijzingen voor financiering van terrorisme of (financiering van) serious crime). Dit betreft informatie over subjecten die in verband kunnen worden gebracht met (de financiering van) terrorisme of (financiering van) serious crime. De informatie bestaat uit NAW-gegevens, geboortedatum, indicatie van de periode die relevant is voor het onderzoek en indien noodzakelijk contextinformatie.

Derde lid (omschrijving andere ernstige vormen van criminaliteit)

Dit lid omschrijft uitsluitend *andere* ernstige vormen van criminaliteit dan financieel-economische criminaliteit en terrorismefinanciering. Artikel 2.2 van de wet maakt bij de omschrijving van het doel van het FEC onderscheid tussen financieel-economische criminaliteit, andere ernstige vormen

⁵⁵ Advies van 9 november 2021, Kamerstukken I 2021/22, 35447, G, blz. 5 en 18-19.

⁵⁶ Kamerstukken II 2021/22, 35447, nr. 21, bijlage, punt 1.

⁵⁷ Bron: FEC Jaarplan 2021, blz. 6.

Consultatieversie nota van toelichting concept-BGS

van criminaliteit en vormen van terrorismefinanciering. De termen terrorismefinanciering en financieel-economische criminaliteit vallen niet onder de definitie van dit lid. Zoals opgemerkt in de nota naar aanleiding van het verslag bij de WGS, is financieel-economische criminaliteit geen statisch begrip en is het daarom niet goed in wetgeving te definiëren. Wel is in de nota naar aanleiding van het verslag een toelichting gegeven.⁵⁸

Dit artikellid geeft gevolg aan de aankondiging uit de Kamerbrief van 17 december 2021 dat bij amvb wordt gepreciseerd wat wordt verstaan onder risico's met betrekking tot "andere ernstige vormen van criminaliteit".⁵⁹ Hiertoe bakent dit besluit de reikwijdte nader af met betrekking tot *andere* ernstige vormen van criminaliteit.

Zoals aangegeven in antwoord 168 van de nota naar aanleiding van het verslag bij de WGS moet onder ernstige vormen van criminaliteit in ieder geval worden verstaan "misdrijven die een ernstige inbreuk op de rechtsorde opleveren" en geeft dit een indicatie van de hier vereiste ernst van de criminaliteit. Dit criterium is ontleend aan diverse artikelen uit het Wetboek van Strafvordering, artikel 10 van de Wet politiegegevens, en artikel 3.22 van de Telecommunicatiewet. In de memorie van toelichting bij de invoering van dit criterium in het Wetboek van Strafvordering is het criterium toegelicht.⁶⁰

Het criterium is gecodificeerd in het onderhavige artikellid. Daar is het vereiste aan toegevoegd dat de betreffende misdrijven tevens de integriteit van het financiële stelsel raken. Voor zover het FEC is gericht op signalen of verzoeken die zien op andere ernstige vormen van criminaliteit, gaat het dus om (aanwijzingen van) misdrijven die een ernstige inbreuk op de rechtsorde vormen, mits die de integriteit van het financiële stelsel raken.

Artikel 2.5 Nadere waarborgen signalenoverleg en gegevensanalyse

(grondslag: artikel 2.7, tweede lid, en 1.8, negende lid, WGS)

Dit artikel regelt voor het signalenoverleg en de gegevensanalyse binnen het FEC een aantal waarborgen in aanvulling op de waarborgen uit de wet en dit besluit, zoals artikel 2.4.

⁵⁸ Kamerstukken II 2020/21, 35447, nr. 6, antwoord 164. Daarin is toegelicht dat financieel-economische criminaliteit een breed begrip is en dat daarmee niet alleen is bedoeld op strafrechtelijke gedragingen, omdat de bestrijding ervan al lang niet meer is voorbehouden aan alleen het strafrecht. Toegelicht werd dat onder de term klassieke vormen van financieel-economische criminaliteit vallen – zoals valsheid in geschrifte, oplichting, bedrog, verduistering, (bedrieglijke) bankbreuk en corruptie – maar ook andere varianten, zoals witwassen, overtreding van handels- en financiële sancties, handel met voorwetenschap en marktmanipulatie. Door de jaren heen komen nieuwe verschijningsvormen aan de oppervlakte, zoals manipulatie van financiële benchmarks (LIBOR-fraude) en cybercrime. Zoals blijkt uit de opsomming van de wetten ten behoeve van de uitvoering waarvan de deelnemers van het FEC worden aangewezen (artikel 2.3), gaat het bij financieel-economische criminaliteit in de WGS eveneens over niet-naleving van bepaalde bestuursrechtelijke wetten en prudentiële wetgeving.

⁵⁹ Kamerstukken II 2021/22, 35447, nr. 21, bijlage, punt 4.

⁶⁰ Kamerstukken II 1996/97, 25403, nr. 3, p. 24-25: "De concrete feiten en omstandigheden dienen meegewogen te worden bij de beoordeling of sprake is van een ernstige inbreuk op de rechtsorde. Het kan gaan om misdrijven als moord, handel in drugs, mensenhandel, omvangrijke milieudelicten, wapenhandel maar ook ernstige financiële misdrijven, zoals omvangrijke ernstige fraude, bijvoorbeeld een BTW-carrousel. Dergelijke misdrijven schokken de rechtsorde ernstig door hun gewelddadige karakter of door hun omvang en gevolgen voor de samenleving. Ook minder ernstige misdrijven kunnen een ernstige inbreuk maken op de rechtsorde, doordat zij in combinatie met andere misdrijven worden gepleegd, bijvoorbeeld valsheid in geschrifte in combinatie met omkoping van ambtenaren met het oog op verkrijging van vergunningen voor bedrijven, of kleine fraudes waarvan, gelet op de aard, kan worden vermoed dat deze deel uitmaken van een omvangrijke en ernstige vorm van fraude." Verderop in die memorie van toelichting is ook witwassen als voorbeeld genoemd (Kamerstukken II 1996/97, 25403, nr. 3, p. 73). Deze voorbeelden moeten omwille van de toekomstbestendigheid en flexibiliteit overigens niet uitputtend worden opgevat.

Onderdeel a bepaalt dat de deelnemer die het signaal of verzoek aanmeldt, moet zorgdragen dat uit de aanmelding blijkt in hoeverre is voldaan aan de criteria, bedoeld in artikel 2.4, eerste lid. De verplichting uit onderdeel c om vast te leggen in hoeverre is voldaan aan de criteria, is opgenomen om achteraf te kunnen vaststellen of hieraan is voldaan. De wijze waarop dit gebeurt, wordt aan de praktijk gelaten. Dit kan bijvoorbeeld blijken uit het aanmeldformulier of het dossier. Zoals in de eerder genoemde Kamerbrief van 17 december 2021 is opgemerkt, wordt aan het FEC niet de bevoegdheid tot geautomatiseerde gegevensanalyse verleend, omdat de noodzaak daartoe vooralsnog niet is gebleken.

PARAGRAAF 2.2 INFOBOX CRIMINEEL EN ONVERKLAARBAAR VERMOGEN (iCOV)

Artikel 2.6 Aanvullende deelnemers

(grondslag: artikel 2.11, eerste lid, onder j, WGS)

Onderdeel a (deelname AFM)

De betrokkenheid van financiële ondernemingen en accountantsorganisaties bij witwassen en fraude leidt tot verwevenheid van de criminele en reguliere economie en brengt schade toe aan de transparantie van en het vertrouwen in de financiële markt. Financiële ondernemingen vervullen bovendien een belangrijke rol in het tegengaan van dergelijk crimineel gedrag in de financiële sector. Op grond van haar wettelijke taken draagt de AFM dan ook bij aan het bestrijden van witwas- of fraudeconstructies door haar toezicht ten aanzien van het voorkomen van witwassen en terrorismefinanciering, het beschermen van consumenten tegen misleiding en de bestrijding van marktmisbruik zoals handel met voorwetenschap en marktmanipulatie.

Naast het bestrijden van witwas- of fraudeconstructies draagt het toezicht van de AFM ook bij aan het tegengaan van het op onrechtmatige wijze behalen van financieel gewin. Wanneer financiële ondernemingen hun rol ten aanzien van het tegengaan van witwassen en fraude onvoldoende invullen kan er sprake zijn van het op onrechtmatige wijze behalen van financieel gewin doordat zij ten onrechte kosten besparen die andere ondernemingen wel maken. Hetzelfde geldt voor het verrichten van vergunningplichtige activiteiten zonder vergunning. Ook hierbij wordt onrechtmatig financieel gewin behaald door toezicht- en nalevingskosten te ontwijken. De AFM houdt in dat kader toezicht op de invulling van de poortwachtersrol van financiële ondernemingen en het bewaken van een gelijk speelveld in de financiële markt.

De iCOV-vermogensrapportages van natuurlijke- en rechtspersonen zullen de AFM inzicht bieden in het vermogen en de inkomsten van (rechts)personen die onderwerp van onderzoek zijn. Dit inzicht draagt bij aan het detecteren van situaties waarin bestuurders zichzelf verrijken ten koste van klanten. De rapportage relaties draagt bij aan onderzoeken in het kader van handel met voorwetenschap, marktmanipulatie, belangenverstremgeling of het verrichten van vergunningplichtige activiteiten zonder vergunning (illegaliteit). Daarnaast zullen de producten van iCOV een belangrijke bijdrage leveren aan het toezicht dat de AFM in de nabije toekomst zal houden op de cryptomarkt na de inwerkingtreding van Verordening voor Markten in Crypto-Activa. Ten slotte zal de aansluiting bij iCOV de samenwerking met de inmiddels aangesloten partijen versterken. In dat kader levert de aansluiting bij iCOV ook meerwaarde op voor de overige deelnemers. Zo beschikt de AFM over informatie ten aanzien van personen en ondernemingen, zoals beleggingsondernemingen, financiële dienstverleners, kredietverstrekkers, accountantsorganisaties en beurshandelaren, die kan bijdragen aan de uitvoering van wettelijke taken van de overige deelnemers. De AFM beschikt daarmee over gegevens die het samenwerkingsverband in staat stellen om zijn doel effectiever te vervullen en die noodzakelijk zijn voor het doel.

De toevoeging van toezichtinformatie van de AFM – bijvoorbeeld door weergave van deze informatie in de Relatiescans van iCOV – geeft een aanvragend lid direct inzicht in de rol(len) en positie(s) die een subject heeft in de financiële sector, maar ook in besluiten en in bestuursrechtelijke sancties die het betreffende subject in het verleden opgelegd heeft gekregen. Op deze manier krijgen zij snel inzicht in de economische activiteiten, kennis en vaardigheden van

Consultatieversie nota van toelichting concept-BGS

de subjecten en hun relaties. Dit helpt om snel in beeld te krijgen wat hun mogelijke rol kan zijn binnen het te onderzoeken criminele netwerk. Zonder de iCOV-rapportage zou deze informatie in de meeste gevallen niet bij de aanvrager terecht komen.

Omgekeerd worden strafrechtelijke handhavers zich op deze manier bewuster van de restinformatie in hun onderzoeken, die mogelijk betrekking heeft op bestuursrechtelijke overtredingen en kan deze informatie – mits daartoe een bevoegdheid bestaat – worden gedeeld met de betreffende bestuursrechtelijke handhaver. Op deze wijze ondersteunen de strafrechtelijke handhavers de bestuursrechtelijke handhavers in hun streven malversaties aan te pakken en drempels op te werpen tegen de verwevenheid tussen de onderwereld en de bovenwereld. De deelnemende partijen aan iCOV onderschrijven dan ook de noodzaak van de deelname van de AFM voor het doel van het samenwerkingsverband.

Recentelijk heeft de Financial Action Task Force (FATF) een rapportage uitgebracht over de aanpak van de witwasproblematiek in Nederland. De departementen van JenV en Financiën dragen gezamenlijk de beleidsmatige verantwoordelijkheid voor deze aanpak. iCOV wordt in de betreffende rapportage expliciet genoemd als één van de samenwerkingsverbanden in Nederland, die een goede bijdrage leveren aan een datagedreven aanpak van fraude en witwassen. Het is daarmee ook een gezamenlijk belang van beide departementen om deze aanpak verder te versterken door de AFM toe te laten treden tot iCOV.

Onderdeel b (deelname Koninklijke Marechaussee)

Aan de Koninklijke Marechaussee (KMar) zijn, op grond van het bepaalde in artikel 4, eerste lid, van de Politiewet 2012, politietaken opgedragen. Zo is er sprake van ondermijnende criminaliteit op en rondom luchthaven Schiphol, waar de KMar de algemene dagelijkse politietaak (art. 4, eerste lid, onder c, Politiewet 2012) uitvoert. In het kader van de uitvoering van deze taken voert de KMar onderzoeken uit die, onder meer, gericht zijn op de aanpak van georganiseerde en ondermijnende criminaliteit op en rondom de luchthavens, witwassen, mensensmokkel en criminaliteit die de integriteit van de krijgsmacht raakt.

De KMar is een politieorganisatie die conform de politiewet haar taken uitvoert op specifieke genoemde terreinen. Dit betekent in de praktijk dat de KMar op de haar aangewezen terreinen en taken veelal een zelfde manier van optreden en werkzaamheden kent als de Nationale Politie. De KMar is een zelfstandig opererend orgaan dat handhaving en opsporing uitvoert met een eigen intelorganisatie. In vele gevallen werkt de KMar samen met onder andere de Nationale Politie, de FIOD en de Douane. De KMar verwacht met de aansluiting op iCOV toegang te hebben tot vermogens- en relatierapportages van natuurlijke- en rechtspersonen ten behoeve van opsporingsonderzoeken. Met deze rapportages zal de KMar inzicht krijgen in vermogens en inkomens van (rechts)personen en het onderkennen van onderlinge relaties. Ook ligt het in de rede dat de producten van iCOV eraan zullen bijdragen dat er binnen de KMar meer zicht op en kennis over financieel-economische criminaliteit zal ontstaan, als gevolg waarvan trends en ontwikkelingen beter en eerder kunnen worden onderkend. De rapportages vanuit iCOV kunnen tevens een bijdrage leveren aan de sturing op (strafrechtelijke) onderzoeken en de analyses voorafgaand aan de inzet van capaciteit. Daar staat tegenover dat de KMar beschikt over gegevens die het samenwerkingsverband in staat stellen om effectiever zijn doel te vervullen en die noodzakelijk zijn voor het bereiken van de doelstelling waarop het samenwerkingsverband zich richt. Ook dit element maakt dat wordt voldaan aan het vereiste dat deelname noodzakelijk is voor het doel van het samenwerkingsverband.

In lijn met de partners betreffen dit gegevens die de KMar op basis van haar taken uit de Politiewet 2012 (artikel 4) vastlegt, te weten art. 8 WPG-informatie voortkomend uit de politietaken:

- De politietaak ten behoeve van de luchthaven Schiphol en andere aangewezen luchtvaartterreinen. Denk hierbij aan de aanpak van ondermijnende criminaliteit en aanhoudingen van bijvoorbeeld geldkoeriers.
- Bestrijding van grensoverschrijdende criminaliteit. Denk hierbij aan de aanpak van mensenhandel, de aanpak van in- en export van verdovende middelen etc.
- Bestrijding van mensensmokkel en fraude met reis- en identiteitsdocumenten.

Artikel 2.7 Beperking gegevensverstrekking over kring van personen

(grondslag: artikel 2.12, derde lid, WGS)

Eerste lid

De iCOV Rapportage Relaties (iRR), ook wel relatiescan genoemd, bedoeld in artikel 2.13, aanhef en onderdeel b, van de wet is een rapportage die een overzicht geeft van de relevante relaties van natuurlijke of rechtspersonen die mogelijk in verband kunnen worden gebracht met mogelijke onverklaarbare of criminele vermogensbestanddelen of witwas- of fraudeconstructies.⁶¹ Zoals toegelicht in paragraaf 4.2 van de memorie van toelichting bij de WGS, komen in de iRR financieel-zakelijke relaties in beeld, maar ook directe familieleden en (ex-)partners. Bij een BV of VOF komt ook de eigenaar van het bedrijf in beeld en bij stichtingen en verenigingen komen eventuele bestuursfuncties in beeld. De relatiescan geeft een weergave tot drie lagen vanaf het bevroegde subject. In de memorie van toelichting is aangegeven dat dit inhoudt dat tot drie stappen vanaf het bevroegde subject de relevante relaties worden weergegeven.⁶² Vermogen wordt vaak verhuld verderop in het netwerk van de betrokkene, niet zozeer bij de directe relaties. Daarom is het noodzakelijk om meerdere lagen in kaart te brengen.

Tweede lid

Vanwege constructies waarbij het vermogen verderop in de keten wordt verhuld (bijvoorbeeld door ingewikkelde bedrijfsstructuren), bepaalt dit lid dat tot een ruimere verstrekking van gegevens over relaties of contacten kan worden overgegaan. Hiervan kan sprake zijn bij een keten van vermogensverschaffers, leidinggevendenden, zeggenschaphebbenden of van personen die in een zakelijk samenwerkingsverband staan tot de betrokken natuurlijk persoon of rechtspersoon. Hieronder vallen ook de achterliggende belanghebbenden of "Ultimate Beneficial Owners (UBO's)" van rechtspersonen. De deelnemer die een verzoek doet om een iRR motiveert aan de hand van diens taakstelling waarom de gegevensverwerking in meer dan drie lagen noodzakelijk is. Die motivering is naar zijn aard niet altijd vooraf te geven en kan er daarom ook uit bestaan dat vermoedelijk sprake is van complexe criminele structuren, waarin relaties vaak diep verborgen zijn, die inzichtelijk moeten worden door de rapportage.

Artikel 2.8 Criteria voor een rapportage over vermogen en inkomsten of financieel-zakelijke relaties

(grondslag: artikel 1.8, eerste lid, WGS)

Met dit artikel wordt mede invulling gegeven aan de aankondiging uit de Kamerbrief van 17 december 2021 dat het startpunt van de gegevensverwerking zoveel mogelijk wordt geconcretiseerd.⁶³ Het onderhavige artikel heeft betrekking op de cumulatieve criteria voor het kunnen doen van een verzoek om een iCOV Rapportage Vermogen en Inkomsten (iRVI) of een iCOV Rapportage Relaties (iRR), bedoeld in artikel 2.13, onder a en b, van de wet. De iRVI is een overzicht van het vermogen en de inkomsten van een of meer, op basis van vooraf vastgelegde criteria bevroegde natuurlijke personen (subjecten) of rechtspersonen. Een iRVI kan ook worden aangevraagd voor een specifiek object (bijvoorbeeld vastgoed). De iRVI bevat dan alleen gegevens die van toepassing zijn op het object (zoals eigenaar, gebruikers, hypotheek, de aard van het gebruik, etc.). Het doel van deze iRVI is inzicht geven in wie de eigenaren en gebruikers van een object zijn bij mogelijke criminele activiteiten in, om en met het object en het traceren van vermogen en het afpakken van dit zelfde vermogen bij de juiste persoon.

De iRR is hierboven beschreven in de toelichting op artikel 2.7.

⁶¹ Zie hierover uitgebreid Kamerstukken II 2019/20, 35447, nr. 3, blz. 26 en 81.

⁶² Kamerstukken II 2019/20, 35447, nr. 3, blz. 26.

⁶³ Kamerstukken II 2021/22, 35447, nr. 21, bijlage, punt 1.

Consultatieversie nota van toelichting concept-BGS

Bij de iRVI en de iRR is geen sprake van geautomatiseerde gegevensanalyse in de zin van artikel 1.1 van de wet, omdat er louter een overzicht wordt gegeven van gegevens uit meerdere bronnen, zonder dat daarbij methodisch onderzoek plaatsvindt.

Eerste lid, onderdeel a (duidelijke en objectieve aanwijzingen)

Uit onderdeel a volgt dat een verzoek om de iRVI of de iRR pas gedaan kan worden als sprake is van duidelijke en objectieve aanwijzingen dat op onrechtmatige wijze financieel gewin is of wordt behaald.

Het criterium van de "duidelijke en objectieve aanwijzingen" is overgenomen uit het advies van de Autoriteit Persoonsgegevens, waarin werd geadviseerd om een duidelijk en objectief signaal op basis van voldoende aanwijzingen als startpunt neer te leggen voor alle samenwerkingsverbanden.⁶⁴ In reactie hierop is in de Kamerbrief van 17 december 2021 aangegeven dat de regels over het startpunt voldoende precies en duidelijk moeten zijn en dat daarom bij amvb het startpunt van de gegevensverwerking zoveel mogelijk wordt geconcretiseerd door nadere criteria.

Verder wordt met de onderhavige bepaling uitvoering gegeven aan de aankondiging uit voornoemde Kamerbrief dat bij iCOV een ondergrens wordt gesteld met het oog op de proportionaliteit.⁶⁵ De AP heeft voorgesteld dat sprake moet zijn van aanwijzingen van een mogelijk substantieel vermogensbestanddeel van een bepaalde hoogte of van een bepaald misdrijf. Zoals is aangegeven in de Kamerbrief, kan met de AP worden ingestemd dat het niet gewenst is dat elk onderzoek door iCOV naar een crimineel en onverklaarbaar vermogensbestanddeel gelegitimeerd zou zijn. Daarom bevat de onderhavige bepaling minimumgrenzen. Met de term "bestuurlijke sanctie" is bedoeld op een bestuurlijke sanctie in de zin van artikel 5:2 van de Algemene wet bestuursrecht. Onder deze term vallen onder meer de bestuurlijke boete en de last onder dwangsom. Een rapportage over vermogen en inkomsten of over financieel-zakelijke relaties kan ook worden opgevraagd ten behoeve van de vaststelling van de bestuurlijke sanctie, zoals ter bepaling van de hoogte van een boete, of last onder dwangsom.

Eerste lid, onderdeel b (noodzaak voor taak deelnemer met het oog op doel iCOV)

Voordat een verzoek gedaan wordt om een iRVI of iRR, moet de deelnemer die het verzoek doet, de noodzaak en proportionaliteit van het verzoek beoordelen. Daartoe verplicht dit onderdeel. Met het oog op de doelstelling van iCOV moet de rapportage noodzakelijk en proportioneel zijn voor de uitoefening van publiekrechtelijke taken en bevoegdheden, zoals bedoeld in artikel 2.11 van de wet of artikel 2.6 van dit besluit. Kenmerkend voor iCOV-rapportages is namelijk dat deze zijn bestemd voor de deelnemers die deze hebben aangevraagd en worden ingezet ten behoeve van de taakstellingen waarvoor zij deelnemen aan iCOV. Op grond van artikel 1.7, eerste lid, onder a, van de wet ontvangt een deelnemer het resultaat van de gezamenlijke gegevensverwerking indien dit noodzakelijk is voor de vervulling van een publiekrechtelijke taak die aan de deelnemer is opgedragen, mits deze taak verenigbaar is met het doel van het samenwerkingsverband. Zoals opgemerkt in de memorie van toelichting, kan iCOV alleen een rapportage opstellen als het verzoek in relatie staat tot het doel van het samenwerkingsverband én de bijhorende publiekrechtelijke taak of bevoegdheid waarvoor de verzoekende deelnemer aan iCOV deelneemt, zoals omschreven in artikel 2.11 van de wet of artikel 2.6 van dit besluit.

Het proportionaliteitsvereiste houdt in dat het doel (in dit geval het in kaart brengen van onverklaarbaar of crimineel vermogen, etc.) en het middel (de iRVI of iRR) met elkaar in verhouding zijn. De verzoeker moet hierbij een belangenafweging maken.

Eerste lid, onderdeel c (samenwerking nodig met meerdere deelnemers)

Dit onderdeel vereist dat het samenstellen van de rapportage naar verwachting de samenwerking met meerdere deelnemers van iCOV vergt. Deze samenwerking kan, mits is voldaan aan onderdeel b, er ook uit bestaan dat via de infrastructuur van iCOV de rapportages op een efficiënte en betrouwbare manier opgesteld kunnen worden. Als het evident is dat de deelnemer die het

⁶⁴ Advies van 9 november 2021, Kamerstukken I 2021/22, 35447, G, blz. 5 en 18-19.

⁶⁵ Kamerstukken II 2021/22, 35447, nr. 21, bijlage, punt 3.

Consultatieversie nota van toelichting concept-BGS

verzoek doet van slechts één andere deelnemer informatie nodig heeft en voor de analyse van die informatie geen samenwerking via iCOV nodig is, moet hij die op bilaterale wijze opvragen bij die andere deelnemer en is geen samenwerking nodig met meerdere deelnemers van iCOV. Dan zou behandeling in iCOV niet voldoen aan de subsidiariteitseis, omdat een lichter alternatief bestaat.

Eerste lid, onderdeel d (administratieve vereisten)

Subonderdeel 1° (vermelding taak deelnemer en subdoelstelling iCOV)

Dit subonderdeel vereist dat de deelnemer die om een iRVI of iRR verzoekt, aangeeft voor welke van zijn taken hij deze rapportage nodig heeft. In het verzoek tot een rapportage moet ter verantwoording worden geregistreerd met het oog op welke publiekrechtelijke taak of bevoegdheid de deelnemer een rapportage vraagt.⁶⁶ Bovendien moet de relatie tot het doel van iCOV worden geregistreerd. Dit kan door aan te geven binnen welk van de vier subdoelstellingen van iCOV uit artikel 2.10 WGS het verzoek valt.

Subonderdeel 2° (vermelding van personen of objecten)

Het startpunt van de gegevensverwerking moet duidelijk zijn. De verzoeker dient daarom de betrokken natuurlijke perso(o)n(en) of rechtsperso(o)n(en) of het betrokken object bij het verzoek te vermelden. Om persoonsverwisseling te voorkomen moet het burgerservicenummer of RSIN uit het Handelsregister worden vermeld. Dit volgt uit artikel 2.12, eerste lid, onder a, van de wet en voor wat betreft het BSN bovendien uit artikel 10 Wet algemene bepalingen burgerservicenummer. Een iRVI kan ook worden aangevraagd ten aanzien van een object. Te denken valt aan een object waarbij een vermoeden is van criminele activiteiten in, om en met het object. Een iRVI die betrekking heeft op een onroerende zaak kan bijvoorbeeld bijdragen aan het in kaart brengen van onverklaarbaar of crimineel vermogen c.q. vastgoed.

Subonderdeel 3° (beschrijvingen feiten en omstandigheden)

Het is voor de bepaling welke informatie in de iRR moet worden opgenomen, van belang dat een bij iCOV ingediend verzoek om een iRR de feiten en omstandigheden vermeldt die relevant zijn om te kunnen bepalen welke relaties gezien de casus relevant zijn om op te nemen in een iRR.

Tweede lid (verantwoording)

Het verzoek moet toelichten in hoeverre is voldaan aan de criteria uit het eerste lid, zo volgt uit dit lid. Gelet op de verplichting tot dataminimalisatie en de mogelijkheid dat sprake is van een (strafvorderlijk) onderzoek onder embargo heeft deze bepaling in beginsel geen betrekking op het verstrekken van onderliggende zaaksinformatie. Het is aan de verzoeker zelf om die informatie op te nemen in de eigen administratie, zodat de verzoeker achteraf, bijvoorbeeld in de richting van de AP of de rechter, kan verantwoorden waarom aan de criteria is voldaan. Dit in het kader van de verantwoordingsplicht uit artikel 5, tweede lid, van de AVG.

Een rapportage is bestemd voor de deelnemer of deelnemers die het verzoek om de rapportage hebben gedaan. Bovendien kan een rapportage alleen worden verstrekt aan gemachtigde medewerkers van de betreffende deelnemer. Dit volgt uit de verplichting tot beveiliging van gegevensverwerkingen die in acht moet worden genomen (artikel 32 AVG). ICOV geeft hieraan invulling door het werkproces zodanig vorm te geven dat een verzoek uitsluitend kan worden gedaan door medewerkers van de deelnemers die daarvoor gemachtigd zijn door hun eigen organisatie. De machtigingen en de verzoeken om rapportages worden geregistreerd door middel van de systemen waarin de deelnemers gezamenlijk persoonsgegevens verwerken.

Artikel 2.9 Vaststelling van thema voor een themarapportage

(grondslag: artikel 2.14, tweede lid, WGS)

Themarapportages van iCOV

⁶⁶ Vgl. Kamerstukken II 2019/20, 35447, nr. 3, blz. 82.

Consultatieversie nota van toelichting concept-BGS

Volgens de definitie uit artikel 2.13, onder c, van de wet is een iCOV Rapportage Thema (iRT NN)⁶⁷ een "geanonimiseerde rapportage, op te stellen aan de hand van vooraf vastgestelde indicatoren en gegevens over bepaalde gepseudonimiseerde natuurlijke personen of rechtspersonen, die een ontwikkeling of trend in een bepaalde regio of met betrekking tot een bepaald fenomeen weergeeft teneinde inzicht te krijgen in problematiek met betrekking tot het doel van iCOV in de zin van het in artikel 2.10 van de wet vastgestelde doel". Zoals de aanhef van artikel 2.13 van de wet beschrijft, gaat aan de rapportage altijd vooraf een verzoek van één of meer deelnemers. De iRT NN is erop gericht om inzicht te bieden in de mate en manier waarop een bepaald fenomeen zich voordoet. De onderzochte fenomenen richten zich op gedragingen die wijzen op het onrechtmatig behalen van financieel gewin. Het samenbrengen van data van de verschillende deelnemers is noodzakelijk om inzicht in dit soort fenomenen te krijgen. Het analyseren van een fenomeen geschiedt met gebruikmaking van vooraf vastgestelde indicatoren. Zo kan iCOV bijvoorbeeld een rapportage samenstellen die vanuit vogelvluchtperspectief laat zien hoe vaak bepaalde indicatoren van bijvoorbeeld *witwassen via vastgoed* voorkomen in een bepaald gebied. Denk bijvoorbeeld aan panden die gefinancierd worden via een van de risicolanden zoals gedefinieerd door de Financial Action Task Force (FATF). De iRT NN geeft onder andere een overzicht zonder identificatiegegevens waarin per object en per subject wordt aangegeven hoe vaak er op de indicatoren wordt gescoord. De iRT NN bevat alleen informatie van subjecten die aan de vooraf vastgestelde minimumdrempel voldoen. Een nadere toelichting op de iRT NN is te vinden in de memorie van toelichting.⁶⁸

De iRT NN meet overigens geen toekomstig gedrag, maar detecteert wat er is gebeurd op basis van gevalideerde indicatoren waarvan wetenschappers en experts veronderstellen dat deze samenhangen met gedrag uit het verleden, bijvoorbeeld witwassen met vastgoed. De iRT NN kan iets zeggen over de mogelijkheid c.q. een verhoogd risico dat dit gedrag zich heeft voorgedaan en zich wellicht nog steeds voordoet in een vooraf gespecificeerde onderzoeksgroep.

Vaststelling van een gestandaardiseerde themarapportage

Het onderhavige artikel gaat over het ontwikkelen van een gestandaardiseerde iRT NN. Voordat een iRT NN daadwerkelijk aangevraagd kan worden moet deze namelijk eerst zijn ontwikkeld en door de rechtmatigheidsadviescommissie zijn beoordeeld. Bij de ontwikkeling van een gestandaardiseerde themarapportage komen de volgende onderdelen aan de orde: 1) het vaststellen van het thema, 2) de productbeschrijving en 3) de vaststelling van de indicatoren. Deze drie elementen komen overeen met de indeling van dit artikel. Een productbeschrijving gaat onder meer in op de relatie tot het doel van iCOV, de gehanteerde databronnen, methode en indicatoren, de invulling van de waarborgen en de manier waarop de resultaten worden gerapporteerd. Bij een aanvraag om een iRT voor het betreffende thema moet de gestandaardiseerde iRT NN die volgens dit artikel is vastgesteld, in acht worden genomen. Indien een deelnemer daadwerkelijk een iRT NN aanvraagt, moet hij de concrete onderzoeksgroep bepalen en de concrete noodzaak van de rapportage onderbouwen (zie artikel 2.11). Het thema, de indicatoren en de methode liggen vast.

Eerste lid (vaststelling thema)

Een themarapportage kan alleen worden opgesteld en verstrekt indien de deelnemers een thema hebben vastgesteld. De deelnemers van iCOV bepalen gezamenlijk voor welk thema een themarapportage ontwikkeld wordt. Na vaststelling van een thema waarvoor iCOV themarapportages kan opstellen, moet dit worden gepubliceerd op de website van iCOV. Dit artikellid bepaalt verder dat het thema betrekking moet hebben op het blootleggen van het op onrechtmatige wijze behalen van financieel gewin door middel van een misdrijf of overtreding als bedoeld in artikel 2.8, eerste lid, onder a, onderdelen 1° tot en met 3°, bestaande uit:

- a. ernstige strafrechtelijke of bestuursrechtelijke inbreuken door criminele netwerken;

⁶⁷ NN staat voor de Latijnse uitdrukking Nomen Nescio: 'ik weet de naam niet' of meer informeel 'naam onbekend', dan wel: Nomen Nominandum: 'de naam moet nog genoemd worden. De iRT NN bevat geen identificerende gegevens.

⁶⁸ Kamerstukken II 2019/20, 35447, nr. 3, blz. 27 en 81.

Consultatieversie nota van toelichting concept-BGS

- b. witwassen, ernstige fraude en daaraan gerelateerde vormen van financieel-economische criminaliteit, of
- c. marktmisbruik dat leidt tot verstoring of ontwrichting van het economisch verkeer of het toezicht daarop.

Bij de onderdelen a en b valt te denken aan:

- financiële verwevenheid en werkwijze van criminele netwerken,
- witwassen met vastgoed (waaronder hypotheekfraude), witwassen met grensoverschrijdende handel,
- financiële werkwijze bij mensenhandel en financiële uitbuiting in arbeidsrelaties, en
- misbruik van rechtspersonen (zoals misbruik met stichtingen, faillissementsfraude, subsidiefraude met rechtspersonen (zoals misbruik coronasubsidies).

Onderdeel c betreft ernstige inbreuken door (doorgaans) ondernemingen, zoals:

- kartelvorming (concurrentiebekerende afspraken tussen ondernemingen),
- misbruik van een economische machtspositie door ondernemingen (bijvoorbeeld het opdrijven van prijzen of het uit de markt drukken van opkomende concurrenten vanuit een sterke positie op een markt),
- koersmanipulatie (manipuleren van financiële koersen met als doel op onrechtmatige wijze koerswinst te boeken),
- stelselmatige en ernstige inbreuken op de bescherming van consumenten – bijvoorbeeld misbruik bij spoeddiensten (zoals slotenmakers) en datingsites, en
- ernstige inbreuken op administratieve verplichtingen door onder toezicht staande ondernemingen, zoals het ontduiken van vergunnings- en meldplichten of illegale bestuurlijke verwevenheden in de financiële sector.

Tweede lid (productbeschrijving)

De deelnemers moeten voor het betreffende thema ter verantwoording een toelichtende beschrijving opstellen. Deze wordt in de praktijk "productbeschrijving" genoemd. Er kan pas een iRT over het betreffende thema worden aangevraagd en verstrekt als de rechtmatigheidsadviescommissie over de productbeschrijving heeft geadviseerd en deze is vastgesteld. De rechtmatigheidsadviescommissie heeft op grond van artikel 1.8, zesde lid, van de wet tot taak de rechtmatigheid van de verwerking van persoonsgegevens in het samenwerkingsverband structureel te beoordelen bij nieuwe verwerkingen en wijziging in verwerkingen. Dit artikellid stelt buiten iedere twijfel dat de deelnemers advies moeten vragen over een nieuwe gestandaardiseerde iRT of wijzigingen in een bestaande iRT. Beoogd is in principe dat het gehele proces waarlangs tot een gestandaardiseerde iRT wordt gekomen onder de adviesplicht valt. Omdat de productbeschrijving hiervan de schriftelijke neerslag vormt, is de adviesplicht daaraan gekoppeld.

Overigens laat dit artikellid onverlet dat met de rechtmatigheidsadviescommissie een werkwijze kan worden afgesproken om te voorkomen dat dit bij ondergeschikte wijzigingen tot oponthoud leidt. Het ligt in de rede dat de rechtmatigheidsadviescommissie aandacht zal besteden aan de voorwaarden in de artikelen 2.9 tot en met 2.12. Geenszins is bedoeld de rechtmatigheidsadviescommissie daartoe te beperken. De adviesplicht strekt ertoe te verzekeren dat de rechtmatigheidsadviescommissie vooraf wordt geraadpleegd, zodat zij haar wettelijke taak ten volle kan uitoefenen waar het (wijzigingen in) iRT's betreft.

Voordat een samenwerkingsverband tot een nieuw type gezamenlijke geautomatiseerde gegevensanalyse overgaat, dient het een gegevensbeschermingseffectbeoordeling uit te voeren op grond van artikel 35 AVG.⁶⁹ Het onderhavige artikel staat er niet aan in de weg dat de productbeschrijving en de gegevensbeschermingseffectbeoordeling deels of geheel worden gecombineerd in één hybride document, om uitvoeringslasten te beperken.

Onderdeel a (beschrijving relatie tot doel iCOV, subsidiariteit en proportionaliteit)

⁶⁹ Dit is toegelicht in de nota n.a.v. het verslag. Kamerstukken II 2020/21, 35447, nr. 6, antwoord 85, blz. 71.

Consultatieversie nota van toelichting concept-BGS

ICOV moet bij de selectie van een nieuw thema rekening houden met de wijze waarop het thema inzicht geeft in de problematiek met betrekking het doel van iCOV en met de subsidiariteit en proportionaliteit van de gegevensverwerking. Dit volgt uit de basisbeginselen van de AVG.

In aansluiting hierop vereist onderdeel a dat in de productbeschrijving wordt toegelicht op welke wijze het thema inzicht geeft in de problematiek met betrekking tot het doel van iCOV. Dit betekent dat moet worden toegelicht waarom het thema past binnen de doelstelling van iCOV en de wijze waarop het inzicht geeft in een of meerdere (sub)doelstellingen van iCOV.

Ook moet de productbeschrijving ingaan op de subsidiariteit en proportionaliteit. Bij de subsidiariteit gaat het erom dat het thema alleen voldoende onderzocht kan worden door samenwerking van meerdere iCOV-deelnemers.

Bij de proportionaliteit wordt in ieder geval getoetst aan de geschatte ernst, stelselmatigheid, verspreiding en duur van het te onderzoeken thema.

In de praktijk zal overigens ook een rol spelen of er goede indicatoren beschikbaar zijn om het thema te onderzoeken, of het thema aansluit op Nationale of Supranationale Risico Assessments (NRA / SNRA), of iCOV kan beschikken over de noodzakelijke data en of er voldoende deskundige medewerkers voorhanden zijn om de themarapportage succesvol te kunnen ontwikkelen.

Onderdeel b (beschrijving te hanteren indicatoren, methode en gegevens)

Om een fenomeen te analyseren, moet dit eerst meetbaar worden gemaakt in data met behulp van indicatoren. De indicatoren die de deelnemers hebben vastgesteld op grond van artikel 2.10 moeten worden toegelicht in de productbeschrijving. Dit betekent dat onder meer moet worden vermeld op basis van welke informatiebronnen de indicatoren zijn vastgesteld en hoe ze zijn gevalideerd.

Ook moet de verwerkingsmethode worden beschreven. Hierbij valt te denken aan de wijze waarop de indicatoren worden toegepast, de wijze waarop ze gemeten kunnen worden in de data en de wijze waarop de indicatoren in een rapportage zichtbaar gemaakt worden. Bij de ontwikkeling wordt ook rekening gehouden met principes van privacy by design en security by design. ICOV gebruikt bij het ontwikkelen van de verwerkingsmethode en indicatoren door de landelijke overheid vastgestelde instrumenten voor het waarborgen van verantwoord datagebruik. Het gaat dan om het Kwaliteitskader Big Data van het Openbaar Ministerie en de Politie of een vergelijkbaar door de rechtmatigheidsadviescommissie goedgekeurd format. Het hanteren van een dergelijk kader zorgt ervoor dat al bij de ontwikkeling rekening gehouden wordt met aspecten op het gebied van onder meer ethiek, transparantie, herleidbaarheid, privacy, rechtmatigheid en informatiebeveiliging. Daarnaast zorgt het vastleggen ervoor dat de keuzes en gehanteerde methode inzichtelijk zijn voor bijvoorbeeld auditoren en eventuele gerechtelijke toetsing.

Onderdeel c (beschrijving invulling waarborgen)

Op grond van dit onderdeel moet de productbeschrijving ook een toelichting geven op de wijze waarop invulling wordt gegeven aan de waarborgen, bedoeld in de artikelen 2.11 en 2.12 van dit besluit en artikel 1.9 van de wet. Daartoe kan gebruik worden gemaakt van het bestaande format verantwoord datagebruik, dat is goedgekeurd door de deelnemers.

Onderdeel d (beschrijving relevante resultaten en ondergrens)

De deelnemers stellen in de productbeschrijving vooraf vast bij welke resultaten sprake is van een verhoogd risico op het op onrechtmatig behalen van financieel gewin. Dit kan bijvoorbeeld zijn bij het scoren op een minimaal aantal indicatoren. Alleen de gegevens over de gevallen waarin wordt voldaan aan die minimumscore, worden geautomatiseerd opgenomen in de rapportage.

In de gevallen waarin sprake is van een verhoogd risico, kan het resultaat op grond van artikel 1.9, vijfde lid, WGS worden gekoppeld aan de persoon: "De deelnemers koppelen alleen die gegevens opnieuw aan de persoon wanneer die op basis van de resultaten van een gegevensanalyse duiden op een verhoogd risico met betrekking tot het doel waarvoor het samenwerkingsverband gegevens verwerkt." Dit is nodig om toepassing te kunnen geven aan artikel 2.13, onder d, van de wet. Dat geeft iCOV de bevoegdheid om op verzoek van een deelnemer een iCOV Rapportage Thema Compact ("iRT compact") op te stellen. In een iRT

Compact wordt een subject uit de iRT NN van identificerende gegevens voorzien. Dit is uitgewerkt in artikel 2.11, tweede lid.

Artikel 2.10 Vaststelling van indicatoren voor een themarapportage

(grondslag: artikel 2.14, eerste lid, WGS)

Dit artikel stelt overeenkomstig artikel 2.14, eerste lid, van de WGS regels over de wijze van vaststelling van indicatoren aan de hand waarvan een themarapportage (iRT NN) wordt opgesteld. De deelnemers beslissen gezamenlijk welk thema relevant is voor de doelstellingen van iCOV. Een fenomeen of thema wordt verder geanalyseerd en meetbaar gemaakt in data, rekening houdend met vertekening (*bias*), transparantie, herleidbaarheid (navolgbaarheid), validiteit, betrouwbaarheid en representativiteit van de data. De indicatoren van het fenomeen worden gebaseerd op wetenschappelijke kennis, statistische validatie, en expertkennis.

Volledigheidshalve wordt opgemerkt dat artikel 1.7, vierde en vijfde lid, van de wet verplichten tot een periodieke terugkoppeling van de effectiviteit en bruikbaarheid van de resultaten. Daarbij moeten de gehanteerde indicatoren aan de hand van de ontvangen terugkoppelingen periodiek worden geëvalueerd ten behoeve van de verbetering van die indicatoren. De periodieke evaluatie wordt in het kader van haar wettelijke taak beoordeeld door de rechtmatigheidsadviescommissie.

Op grond van artikel 1.9, derde lid, van de wet moet er aan het publiek op toegankelijke wijze uitleg worden verschaft over de gehanteerde indicatoren.

Artikel 2.11 Criteria voor behandeling van een verzoek om een themarapportage

(grondslag: artikel 2.14, tweede lid, WGS en artikel 1.8, eerste lid, WGS)

Het onderhavige artikel geeft voor wat betreft de iCOV Rapportage Thema NN en de iCOV Rapportage Thema compact, samen met artikel 2.9, invulling aan de aankondiging uit de Kamerbrief van 17 december 2021 dat het startpunt van de gegevensverwerking zoveel mogelijk wordt geconcretiseerd.⁷⁰

Eerste lid (criteria iRT NN)

In overleg tussen de deelnemer die het verzoek wil doen en medewerkers van iCOV wordt het verzoek voor een specifieke iRT NN opgesteld. Het thema, de methode, de indicatoren en de te gebruiken databronnen staan vast (zie artikel 2.9 en 2.10).

Onderdeel a (onderzoeksvraag en onderzoeksgroep)

De deelnemer die het verzoek doet bepaalt in samenspraak met iCOV de onderzoeksgroep (bijvoorbeeld natuurlijke personen of rechtspersonen of objecten binnen een bepaald geografisch gebied) en onderzoeksvraag. Daarbij wordt kritisch gekeken naar mogelijke herleidbaarheid van subjecten. Herleidbaarheid kan ontstaan als de onderzoeksgroep onvoldoende groot of divers is zoals het bevragen van objecten binnen een bepaalde straat in plaats van een stad. De aanvrager verantwoordt de keuze van de onderzoekspopulatie voor zover dit mogelijk is kijkend naar onderzoeks- en opsporingsbelangen.

Onderdeel b (aanleiding en duidelijke en objectieve aanwijzingen)

Onderdeel b vereist dat een beschrijving wordt opgenomen voor de aanleiding en achtergrond van de onderzoeksvraag, met een vermelding van duidelijke en objectieve aanwijzingen dat bij de beoogde onderzoeksgroep sprake is van het type onrechtmatig financieel gewin waar het vastgestelde thema zich op richt. Deze motivering hoeft overigens niet zodanig gedetailleerd te

⁷⁰ Kamerstukken II 2021/22, 35447, nr. 21, bijlage, punt 1.

Consultatieversie nota van toelichting concept-BGS

zijn dat informatie wordt gegeven over de inhoud van een opsporings- of toezichtprocedure, aangezien dit opsporings- of toezichtbelangen zou kunnen doorkruisen.

Onderdeel c (noodzakelijkheid)

Onderdeel c vereist dat de deelnemer die een iRT NN aanvraagt, toelicht waarom de rapportage noodzakelijk is voor zijn taken en bevoegdheden, bedoeld in artikel 2.11 van de wet of artikel 2.6 van dit besluit. Ook hier geldt het voorbehoud uit de vorige alinea over de mate van detaillering van de toelichting.

Onderdeel d (proportionaliteit)

Onderdeel d schrijft voor dat ook de proportionaliteit moet worden toegelicht. De proportionaliteit verschilt per verzoek en is mede afhankelijk van de doelstelling van de deelnemer die het verzoek doet en van de grootte van de onderzoeksgroep. Dit is dus een specifiekere proportionaliteitstoets dan die op grond van artikel 2.9, tweede lid, onderdeel a, dat voortschrijft dat de evenredigheid van het vaststellen van een nieuw thema wordt getoetst aan de hand van de geschatte ernst, stelselmatigheid, verspreiding en duur van het te onderzoeken thema.

Deelnemers die persoonsgegevens zouden verstrekken, kunnen indien naar hun oordeel sprake is van zwaarwegende redenen die zich tegen gegevensverstrekking verzetten, weigeren om gegevens aan te leveren (artikel 1.5 WGS). Hierbij is maatwerk mogelijk in de beoordeling door de deelnemer wiens gegevens het betreft, zodat deze ten opzichte van andere iCOV-rapportages differentiatie kan aanbrengen in de afweging of sprake is van zwaarwegende redenen, gelet op de aard van de themarapportage.

Tweede lid (criteria iRT compact)

Algemeen: iRT compact

Met de iRT NN kan een fenomeen in kaart gebracht worden. Bijvoorbeeld: hoe wordt er in een bepaald gebied gescoord op de indicatoren van witwassen met vastgoed? Artikel 2.13, onder d, van de WGS geeft iCOV de bevoegdheid om op verzoek van een deelnemer een iCOV Rapportage Thema compact ("iRT compact") op te stellen. Hierdoor is het toegestaan om vanuit het vogelvluchtperspectief van de IRT NN in te zoomen op de betrokken personen of bedrijven. Met de iRT compact kunnen de betrokken subjecten en objecten geïdentificeerd worden. Zo wordt beter zicht verkregen op de betrokkenen bij bijvoorbeeld criminele geldstromen en witwassen. Dit is nader toegelicht in de memorie van toelichting.⁷¹

In de iRT NN wordt een (gepseudonimiseerd) overzicht verstrekt met daarin de scores van de subjecten en objecten die volgens de eerder bepaalde definitie (artikel 2.9, tweede lid, onder d) blijken geven van een verhoogd risico dat op onrechtmatige wijze financieel gewin is of wordt behaald. De deelnemer die het verzoek doet, bepaalt samen met een medewerker van iCOV welke (gepseudonimiseerde) subjecten en objecten gezien hun score op de indicatoren en de onderliggende onderzoeksvraag van de aanvrager, relevant zijn om verder te bevragen in een iRT Compact. Per subject of object wordt een iRT Compact opgesteld. Over die natuurlijke en rechtspersonen wordt dan een iRVI en iRR uitgevoerd om de score van de indicatoren nader in kaart te brengen.

Bij de iRT compact zelf is daarom – net als bij de iRVI en iRR – geen sprake van geautomatiseerde gegevensanalyse in de zin van artikel 1.1 van de wet, omdat er louter een overzicht wordt gegeven van gegevens uit meerdere bronnen, zonder dat daarbij methodisch onderzoek plaatsvindt.

In de iRT Compact wordt met behulp van een of meer iRVI's en iRR's context gegeven aan de scores op de indicatoren. Die iRVI en/of iRR geeft een nadere analyse van de score op de indicatoren en dient als validatie van de resultaten op de indicatoren. Deze validatie houdt in dat een medewerker van iCOV context geeft aan de scores op de indicatoren van een specifiek subject en een controle verricht op de geldigheid van de scoring op de indicatoren. Hierbij wordt extra

⁷¹ Kamerstukken II 2019/20, 35447, nr. 3, blz. 27.

informatie geraadpleegd die door zijn vorm niet gebruikt kan worden in de iRT NN. Het gaat daarbij om tekstbestanden zoals vastgoedaktes. Als blijkt dat onterecht gescoord is op indicatoren dan wordt een iRT compact niet verstrekt aan de aanvrager.

Voorwaarden

Volgens dit artikellid kan een iRT compact alleen worden aangevraagd ten aanzien van (tot dan toe) gepseudonimiseerde personen ten aanzien van wie op basis van de vooraf vastgestelde indicatoren duidelijke en objectieve aanwijzingen blijken dat op onrechtmatige wijze financieel gewin is of wordt behaald. Daarbij zijn de aanvraagcriteria die gelden voor een iRVI of iRR (artikel 2.8) van overeenkomstige toepassing.

Artikel 2.12 Uitvoering van de gegevensanalyse voor een themarapportage

(grondslag: art. 1.1, derde streepje, 1.9, vijfde lid, en 2.14, tweede lid, WGS)

Het onderhavige artikel stelt nadere regels over de uitvoering van de gegevensanalyse in het kader van de geanonimiseerde themarapportage (iRT NN). Het artikel stelt een aantal aanvullende waarborgen om een zorgvuldige analyse te bereiken. In de toelichting op artikel 2.9 van dit besluit is reeds een inleiding gegeven op wat wordt bedoeld met de bevoegdheid uit artikel 2.13, onder c, van de WGS om een iRT NN op te stellen, evenals de bevoegdheid uit artikel 2.13, onder d, van de WGS om een "iRT compact" op te stellen.

Eerste lid (omschrijving vormen van geautomatiseerde gegevensanalyse)

Voor zover is voorzien in de bevoegdheid tot geautomatiseerde gegevensanalyse, verplicht artikel 1.1, eerste streepje, van de wet om bij algemene maatregel van bestuur te omschrijven welke vormen van analyse van persoonsgegevens worden verricht zonder menselijke tussenkomst.

De iRT NN is een vorm van geautomatiseerde gegevensanalyse.⁷²

De vorm van geautomatiseerde gegevensanalyse bij de iRT NN houdt in dat de gegevens worden geanalyseerd aan de hand van vooraf vastgestelde gevalideerde indicatoren. De algoritmes die iCOV gebruikt zijn beschrijvend van aard. Dat betekent dat iCOV vooraf gedefinieerde ofwel gestandaardiseerde vragen (queries) stelt aan de data die een "navolgbaar en controleerbaar" resultaat opleveren, zoals artikel 1.9, zesde lid, van de wet vereist. Hiertoe kunnen de gegevens worden samengevoegd, opgeteld en gegroepeerd.

Doordat sprake is van geautomatiseerde gegevensanalyse, zijn de aanvullende waarborgen uit artikel 1.9 van de wet van toepassing. Dit betekent dat een iRT NN nooit zonder menselijke tussenkomst aan de aanvrager wordt geleverd. Bij de menselijke tussenkomst wordt beoordeeld of het resultaat op zorgvuldige wijze tot stand is gekomen (artikel 1.9, tweede lid, van de wet). De iRT NN wordt automatisch gegenereerd maar wordt niet één op één doorgezet naar de aanvrager. Er wordt eerst menselijke duiding gegeven door de rapporteur en daarnaast wordt een controle uitgevoerd door onder meer de teamleader productie en de privacyjurist. Ook wordt in het rapport uitgelegd hoe de resultaten geïnterpreteerd kunnen worden. De rapportage wordt zorgvuldig gecontroleerd alvorens deze wordt verstrekt. De iRT-NN bestaat feitelijk uit een eerste deel, dat geautomatiseerd tot stand is gekomen, en een tweede deel met handmatige hoofdstukken, waarin de rapporteur menselijke duiding geeft.

In de rapportage wordt overigens ook verantwoord hoe de resultaten zijn verkregen en op basis van welke databronnen. Dit volgt uit artikel 1.8, tweede lid.

Tweede lid (in acht nemen productbeschrijving)

⁷² Geautomatiseerde gegevensanalyse is volgens artikel 1.1 WGS een analyse van persoonsgegevens waarbij *tijdens* de analyse geen menselijke tussenkomst plaatsvindt. De gegevensanalyse wordt dus daadwerkelijk door een geautomatiseerd systeem uitgevoerd. Het wetsvoorstel vereist wel dat er menselijke tussenkomst plaatsvindt in de fase *nadat* de analyse is voltooid maar *voordat* de resultaten worden verstrekt aan de deelnemer van het samenwerkingsverband. Daarbij moet gecontroleerd worden op zorgvuldige totstandkoming van de analyse (artikel 1.9, tweede lid, WGS). Voor een nadere toelichting op de term geautomatiseerde gegevensanalyse wordt verwezen naar de nota van wijziging op de WGS. Kamerstukken II 2020/21, 35447, nr. 7.

Consultatieversie nota van toelichting concept-BGS

Een iRT NN brengt een bepaald fenomeen vanuit een afgebakende onderzoeksgroep gepseudonimiseerd in kaart om vervolgens door verschillende analysetechnieken de elementen te belichten die voor de domeinen opsporing, toezicht of inning van overheidsvorderingen relevant zijn. De indicatoren en de gebruikte methode zijn vastgelegd in de productbeschrijving, bedoeld in artikel 2.9. De gegevensanalyse moet deze vastgestelde indicatoren en onderzoeksmethode volgen, zo volgt uit dit lid.

Derde lid (in acht nemen aanvraag)

De aanvrager bepaalt in samenspraak met een medewerker van iCOV de onderzoeksgroep en onderzoeksvraag (zie artikel 2.11, eerste lid). De analyse beperkt zich tot het thema, de gedefinieerde onderzoeksgroep en de onderzoeksvraag.

Vierde lid (aanvullende voorwaarden)

Onderdeel a (representativiteit onderzoeksgroep)

Ook moet aandacht worden besteed aan het op dusdanige wijze selecteren van de onderzoeksgroep dat vooringenomenheid zoveel mogelijk wordt voorkomen.

Onderdeel b (uitlegbare en navolgbare methodiek)

Onderdeel b waarborgt dat de gehanteerde methodiek van de gegevensverwerking voor de themarapportage voldoet aan de eisen van uitlegbaarheid, navolgbaarheid en controleerbaarheid. Dit is van belang voor de validatie, transparantie en verantwoording. Dit wordt in de praktijk bevorderd door de productbeschrijving van de themarapportage, waarin een verantwoording wordt gegeven van voornoemde eisen.

Onderdeel c (fasen van pseudonimisering)

Onderdeel c wijst aan in welke fase van de gegevensverwerking pseudonimisering plaatsvindt. Pas nadat de ontvanger van de iRT NN ten aanzien van een bepaald subject een verzoek heeft gedaan om een iRT Compact (dat voldoet aan de voorwaarden), worden er identificerende gegevens toegevoegd. Dit is vastgelegd in onderdeel c. Hiermee wordt invulling gegeven aan artikel 1.9, vijfde lid, van de wet.

Er staan geen identificerende gegevens in de themarapportage NN. Als er gegevens in staan die te herleiden zijn naar een persoon dan worden deze gegevens niet opgenomen in de rapportage. Dat volgt uit artikel 2.13, onder c, van de wet. Voor de ontvanger is een iRT NN een geanonimiseerde rapportage. Vanuit iCOV gezien is een iRT NN gepseudonimiseerd. Zowel de betreffende medewerker die de rapportage opstelt als de ontvanger van de rapportage hebben geen toegang tot deze sleutel. Dit volgt uit artikel 1.9, vijfde lid, van de wet, dat verplicht tot het "apart bewaren" van de sleutel.

Onderdeel d (horizon)

Onderdeel d bepaalt dat, in verband met de actualiteit van de data, een verzoek om een iRT compact hooguit tot twee jaar na de verstrekking van de iRT-NN kan worden ingediend. Idealiter geschiedt dit overigens binnen één jaar.

PARAGRAAF 2.3 REGIONALE INFORMATIE- EN EXPERTISECENTRA (RIEC's)

Artikel 2.13 Territoriale werkgebieden

(grondslag: artikel 2.16, tweede lid, WGS)

Voor de kenbaarheid is het van belang dat wordt gepubliceerd wat het territoriale gebied is van elk Regionaal Informatie- en Expertisecentrum, zodat duidelijk is welke gemeenten en andere deelnemers aan de respectievelijke RIEC's deelnemen. Daarom moeten de RIEC's op grond van het onderhavige artikel de territoriale indeling publiceren op internet. De wijze van publicatie op

internet is daarin niet voorgeschreven: dit kan op de site van een RIEC, maar kan ook voor alle RIEC's centraal worden gepubliceerd.

Artikel 2.14 Nadere regels over wettelijke taken en bevoegdheden van deelnemers

(grondslag: artikel 2.19, tweede lid, WGS)

Artikel 2.19, tweede lid, van de wet bepaalt dat bij of krachtens algemene maatregel van bestuur nadere regels kunnen worden gesteld over de wettelijke taken en bevoegdheden van de deelnemers waarvoor gegevens kunnen worden verwerkt binnen de Regionale Informatie- en Expertisecentra.

Zoals toegelicht in de memorie van toelichting bij artikel 2.19 van de wet, kunnen krachtens deze bepaling "zo nodig ook aanvullende wettelijke taken en bevoegdheden worden aangewezen waarvoor de deelnemers gegevens kunnen verwerken in het RIEC." De Nederlandse Voedsel- en Warenautoriteit (hierna: NVWA) is in artikel 2.19, eerste lid, onderdeel I, van de wet aangewezen als deelnemer van het samenwerkingsverband RIEC. Dit is echter alleen gebeurd voor de uitoefening van de wettelijke taken, bedoeld in artikel 3 van de Wet op de bijzondere opsporingsdiensten en de daaruit voortvloeiende bevoegdheden. De toezichtstaken en (bestuursrechtelijke) handhaving zijn niet vermeld en ook ontbreekt de taakuitoefening door buitengewoon opsporingsambtenaren van de NVWA, waardoor de opsomming van de relevante taken onvolledig is. Dit zou afbreuk doen aan de integrale aanpak, die niet alleen strafrechtelijk kan zijn, maar ook bestuursrechtelijk. Daarom zijn de taken aldus aangevuld.

Artikel 2.15 Concretisering van te verstrekken gegevens

(grondslag: artikel 2.22, tweede lid, WGS)

Dit artikel geeft uitvoering aan artikel 2.22, tweede lid, van de wet. Artikel 2.22 van de wet bepaalt dat bij algemene maatregel van bestuur nadere regels worden gesteld over de categorieën van gegevens en de concretisering daarvan en de bronnen van waaruit die gegevens afkomstig zijn en dat aanvullende categorieën gegevens kunnen worden aangewezen, voor zover dat noodzakelijk is voor het doel van de RIEC's. Het onderhavige artikel codificeert de gegevens die volgens de procesbeschrijvingen van de RIEC's uit 2019 worden verwerkt.⁷³ Het onderhavige artikel heeft geen betrekking op de aanmelding van een signaal bij een RIEC op grond van artikel 2.23, eerste lid, van de wet, maar wel op de gezamenlijke gegevensverwerking die daarop volgt.

Hoewel het voorgestelde artikel een uitwerking biedt van de te verstrekken categorieën gegevens, laat dat onverlet dat de leverende deelnemers zelf beoordelen welke precieze persoonsgegevens, vergaard vanuit de eigen taakstelling, in het concrete geval noodzakelijk zijn om een goede invulling te kunnen geven aan de doelstelling van de RIEC's en dus moeten worden verstrekt. Het onderhavige artikel laat bovendien de voorwaarden uit artikel 1.5 van de wet onverlet, namelijk dat de verstrekking noodzakelijk moet zijn voor het doel van het samenwerkingsverband en dat zwaarwegende redenen zich niet tegen verstrekking mogen verzetten.

Op getrapte wijze verstrekken de deelnemers gegevens ten behoeve van het doel van de RIEC's op basis van signalen van de deelnemers. Dit geschiedt in maximaal drie fasen. Daarbij kan aan de tweede of derde fase eventueel worden toegekomen wanneer de deelnemers na een zorgvuldige afweging concluderen dat met de gegevens die in de eerdere fase zijn verstrekt het doel van de RIEC's nog niet (voldoende) kan worden bereikt en dat de verstrekking van de zwaardere categorieën gegevens noodzakelijk is. Deze afweging hangt onder meer af van de ernst van het signaal. Beginselen van proportionaliteit en subsidiariteit zijn in dit proces leidend. Er mogen niet

⁷³ Zie de Procesbeschrijving integrale casusaanpak uit 2019, de Procesbeschrijving Gebied-wijkscan en nulmeting uit 2019 en de Procesbeschrijving Handhavingsknelpunten uit 2019: <https://www.riec.nl/documenten?trefwoord=procesbeschrijving>

Consultatieversie nota van toelichting concept-BGS

meer gegevens worden verwerkt dan strikt noodzakelijk is ter verwezenlijking van het doel van de RIEC's. De belangenafweging vindt in het concrete geval plaats. Deze afweging geldt voor elke stap in het proces en wordt mede geborgd door de uitgewerkte fasering. Op basis van het verkregen inzicht in de (mogelijke) aard en omvang van de georganiseerde criminaliteit kan uiteindelijk een integraal interventieadvies worden geformuleerd, waarna de effectiviteit en bruikbaarheid hiervan moet worden geëvalueerd (artikel 1.7, vierde lid, WGS).

In de memorie van toelichting bij artikel 2.23 van de wet is de indeling in fasen toegelicht.⁷⁴ Aldaar is onder meer toegelicht: "Met dit stapsgewijze proces waarin verschillende categorieën van persoonsgegevens naar de mate van relatieve zwaarte worden verwerkt voor zover dat noodzakelijk is voor het doel, bedoeld in artikel 2.17, wordt invulling gegeven aan de beginselen van subsidiariteit en proportionaliteit. (...) 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 met het oog op het doel van artikel 2.17."

In eerste fase van de gegevensverwerking mogen Belastingdienstgegevens nog niet worden geleverd. Dit vloeit voort uit het systeem van artikel 2.22, eerste lid, onder a, van de wet, aangezien de fiscale gegevens pas worden genoemd in subonderdeel 2°. Voor de duidelijkheid is in het onderhavige artikel geëxpliciteerd dat met de categorieën "financiële gegevens" en "inkomensgegevens" – die in de eerste fase worden verstrekt – niet wordt bedoeld op gegevens van de Belastingdienst. Dit sluit tevens aan bij de memorie van toelichting bij de WGS, waarin is benadrukt dat Belastingdienstgegevens pas in de tweede fase mogen worden verwerkt.⁷⁵ In de eerste fase mogen evenmin politiegegevens in de zin van de artikelen 8 en 13 van de Wet politiegegevens of justitiële en strafvorderlijke gegevens en tenuitvoerleggingsgegevens worden verwerkt. Dat mag pas in de tweede fase.

Met het voorliggende artikel wordt tevens een afbakening gegeven van de categorie gegevens over seksueel gedrag of seksuele gerichtheid. Zoals gesteld in de memorie van toelichting⁷⁶ en de nota naar aanleiding van het verslag⁷⁷ bij de WGS, is het voor het doel van de RIEC's noodzakelijk om bijzondere persoonsgegevens over seksueel gedrag of seksuele gerichtheid te kunnen verwerken. Daarbij is erop gewezen dat bij de aanpak van mensenhandel in RIEC-verband namelijk ook onderzoeken plaatsvinden naar illegale prostitutie en uitbuiting, waarbij gegevens over seksueel gedrag en seksuele gerichtheid verwerkt (moeten) worden. Het onderhavige artikel verduidelijkt dat het dus uitsluitend gaat om persoonsgegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid wanneer de verwerking noodzakelijk is voor onderzoeken in het kader van bestrijding van mensenhandel, illegale prostitutie en uitbuiting, in aanvulling op de verwerking van persoonsgegevens van strafrechtelijke aard. Hiermee is deze gegevenscategorie uit artikel 2.21 van de wet scherper afgebakend en in overeenstemming gebracht met datgene wat volgens artikel 23, onder c, van de Uitvoeringswet AVG reeds is toegestaan.

Artikel 2.16 Criteria voor behandeling van een signaal

(grondslag: artikel 2.23, negende lid, WGS)

⁷⁴ Kamerstukken II 2019/20, 35447, nr. 3, blz. 101-103.

⁷⁵ Kamerstukken II 2019/20, 35447, nr. 3, blz. 99: "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 met fiscaalrechtelijke en strafrechtelijke bevoegdheden, zoals de rijksbelastingdienst, politie of openbaar ministerie. Het gaat hierbij om fiscale gegevens, 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 en om gegevens over iemands seksueel gedrag of seksuele gerichtheid."

⁷⁶ Kamerstukken II 2019/20, 35447, nr. 3, blz. 97.

⁷⁷ Kamerstukken II 2020/21, 35447, nr. 6, blz. 128.

Consultatieversie nota van toelichting concept-BGS

Eerste lid

Met dit lid wordt de delegatiegrondslag uit artikel 2.23, negende lid, van de wet gebruikt om nadere regels te stellen over de criteria waaraan een signaal moet voldoen.

Criterium a vereist dat sprake is van duidelijke en objectieve aanwijzingen van één of meerdere deelnemers dat bepaalde gedragingen of situaties verband houden met verschijningsvormen van georganiseerde criminaliteit. Die aanwijzingen moeten blijken uit feiten, omstandigheden en gedragingen die aan het signaal ten grondslag liggen, voor zover deze voortvloeien uit concrete waarnemingen van de deelnemer tijdens de uitoefening van diens wettelijke taken en bevoegdheden. Het criterium is in essentie gebaseerd op het Privacyprotocol RIEC's-LIEC uit 2021.⁷⁸ Het criterium van de "duidelijke en objectieve aanwijzingen" is overgenomen uit het advies van de Autoriteit Persoonsgegevens, waarin werd geadviseerd om een duidelijk en objectief signaal op basis van voldoende aanwijzingen als startpunt neer te leggen voor alle samenwerkingsverbanden.⁷⁹ In reactie hierop is in de Kamerbrief van 17 december 2021 aangegeven dat de regels over het startpunt voldoende precies en duidelijk moeten zijn en dat daarom bij amvb het startpunt van de gegevensverwerking zoveel mogelijk wordt geconcretiseerd door nadere criteria.⁸⁰

In het Privacyprotocol is georganiseerde criminaliteit omschreven als "misdaadverschijnselen met een maatschappij ondermijnend karakter, die tot stand komen in samenwerking tussen personen en worden gepleegd met het oog op het gezamenlijk behalen van financieel of materieel gewin".⁸¹ De Afdeling advisering van de Raad van State heeft in haar voorlichting over de rol van gemeenten in de bestuurlijke en integrale aanpak van ondermijning een aantal concrete kenmerken genoemd, die nader duiden wat moet worden verstaan onder georganiseerde criminaliteit, zoals dat hiermee meestal grote hoeveelheden geld worden verdiend, dat de grote winsten worden gebruikt om de bovenwereld te ondermijnen en dat de ondermijning dreigt door te werken naar de overheid.⁸²

Om een nadere concretisering te geven werkt criterium b uit om wat voor verschijningsvormen van georganiseerde criminaliteit het kan gaan. De opgesomde verschijningsvormen zijn afkomstig uit artikel 2 van het RIEC-convenant uit 2014 en zijn genoemd in de memorie van toelichting bij de WGS, met dien verstande dat "georganiseerde hennepsteelt" is geactualiseerd naar "georganiseerde drugscriminaliteit".⁸³ Omwille van de toekomstbestendigheid noemt de bepaling ook: misdrijven die een ernstige inbreuk op de rechtsorde opleveren als bedoeld in het Wetboek van Strafvordering, voor zover die georganiseerde criminaliteit betreffen. In de toelichting op artikel 2.4, derde lid, van dit besluit is beschreven wat hieronder wordt begrepen. Criterium b biedt tot slot de mogelijkheid dat een RIEC-stuurgroep of de Minister van Justitie en Veiligheid aanvullende verschijningsvormen van georganiseerde criminaliteit benoemen. Hierdoor kunnen de RIEC-stuurgroepen regionale prioriteiten aanwijzen, afhankelijk van de regionale problematiek. Ook bevordert deze aanvullende mogelijkheid de toekomstbestendigheid, omdat rekening kan worden gehouden met actuele ontwikkelingen inzake de georganiseerde criminaliteit. De mogelijkheid van de minister om verschijningsvormen te benoemen is van belang indien bepaalde verschijningsvormen in de meeste RIEC-regio's aan de orde zijn, en het benodigd is dat de RIEC's zich hierop kunnen richten. Omwille van de voorzienbaarheid en transparantie moeten de aanvullende verschijningsvormen worden gepubliceerd, bijvoorbeeld op de RIEC's-website.

Criterium d gaat over de verwachting dat het signaal de gezamenlijke aanpak met meerdere deelnemers van het RIEC vergt. Bij dit criterium is het van belang dat de betreffende deelnemer de intentie heeft om het signaal gezamenlijk met meerdere deelnemers op te pakken. De deelnemer heeft beoordeeld dat het oppakken van het signaal (enkel) monodisciplinair vanuit het

⁷⁸ Zie punt 9.1 in samenhang gelezen met de definitie van signaal uit punt 3.20 en voetnoot viii van het Privacyprotocol RIEC's-LIEC 2021.

⁷⁹ Advies van 9 november 2021, Kamerstukken I 2021/22, 35447, G, blz. 5 en 18-19.

⁸⁰ Kamerstukken II 2021/22, 35447, nr. 21, bijlage, punt 1.

⁸¹ Aldus punt 3.9 van het Privacyprotocol RIEC's-LIEC 2021.

⁸² Kamerstukken II 2018/19, 29911, nr. 223, bijlage, blz. 17.

⁸³ Kamerstukken II 2019/20, 35447, nr. 3, blz. 84.

eigen vakgebied niet het meest opportuun wordt gevonden. Als de deelnemer door zelf interventies te plegen het probleem voldoende kan aanpakken, moet die weg eerst worden bewandeld. Het kan echter ook op voorhand duidelijk zijn dat een integrale aanpak nodig is.

Op grond van criterium e moet worden getoetst of het signaal naar verwachting betrekking heeft op de regio van het betreffende RIEC. Het signaal moet ten minste binnen die regio vallen. Dat een signaal op meerdere regio's betrekking kan hebben is geen beletsel. Mocht gegevensuitwisseling tussen meerdere RIEC's nodig blijken voor het doel van de RIEC's, dan is dat mogelijk onder de voorwaarden van artikel 2.20 van de wet.

Tweede lid

De verplichting voor de deelnemer die het signaal aanmeldt om toe te lichten in hoeverre is voldaan aan de criteria is opgenomen om achteraf te kunnen vaststellen of hieraan is voldaan. De wijze waarop dit gebeurt, wordt aan de praktijk gelaten. Dit kan bijvoorbeeld blijken uit het aanmeldformulier of het dossier.

PARAGRAAF 2.4 ZORG- EN VEILIGHEIDSHUIZEN (ZVH)

Artikel 2.17 Definitiebepaling

Artikel 2.26 WGS gebruikt de term "gezamenlijke strategie voor de uitoefening van de wettelijke taken en bevoegdheden waarmee de deelnemers zijn belast alsmede daaraan gerelateerde noodzakelijke werkzaamheden die worden verricht door de deelnemers". In de praktijk van de Zorg- en Veiligheidshuizen is dat het zogeheten plan van aanpak. Gelet daarop en om wetseconomische redenen wordt de term gedefinieerd als plan van aanpak.

Artikel 2.18 Territoriale werkgebieden

(grondslag: artikel 2.24, tweede lid, WGS)

Voor de kenbaarheid is het van belang dat wordt gepubliceerd wat het territoriale gebied is van elk Zorg- en Veiligheidshuis, zodat duidelijk is welke gemeenten en andere deelnemers aan de respectievelijke Zorg- en Veiligheidshuizen deelnemen. Daarom moeten de Zorg- en Veiligheidshuizen op grond van het onderhavige artikel de territoriale indeling publiceren op internet. De wijze van publicatie op internet is daarin niet voorgeschreven: dit kan op de site van een Zorg- en Veiligheidshuis, maar kan ook voor alle Zorg- en Veiligheidshuizen centraal worden gepubliceerd. Mochten de territoriale werkgebieden wijzigen, dan moet de bekendgemaakte informatie uiteraard worden geactualiseerd.

Artikel 2.19 Beperking gegevensverstrekking over kring van personen

(grondslag: artikel 2.30, tweede lid, WGS)

De AP heeft in haar nadere advies over de WGS geadviseerd om de categorieën van te verstrekken persoonsgegevens bij de Zorg- en Veiligheidshuizen te beperken tot directe sociale contacten van betrokkene, en dus gegevensverstrekking over de tweede en derde schil rondom betrokkene uit te sluiten. De AP heeft signaleerd dat er een oneindig aantal schillen rondom een betrokkene kan ontstaan. Eerst de directe sociale omgeving, dan de sociale omgeving van mensen in die sociale omgeving, et cetera. Inderdaad kan de formulering van artikel 2.30 van de wet op dit punt aanleiding geven tot onduidelijkheid. Een oneindig aantal schillen is niet beoogd. Om dit buiten twijfel te stellen is conform het advies van de AP in het onderhavige artikel voor de Zorg- en Veiligheidshuizen geregeld dat de gegevensverstrekking wordt beperkt tot de eerste schil rond een betrokkene. Dit is aangekondigd in de Kamerbrief van de Minister van Justitie en Veiligheid van 17 december 2021 in reactie op het nadere advies van de AP over de WGS.⁸⁴

⁸⁴ Kamerstukken II 2021/22, 35447, nr. 21, bijlage, punt 5.

Gegevensverwerking over de eerste schil rond betrokkene is voldoende ten behoeve van het achterliggende doel van de gegevensverwerking over directe sociale contacten van de betrokkene, zoals toegelicht in de memorie van toelichting bij de WGS.⁸⁵

Artikel 2.20 Criteria voor behandeling van een casus

(grondslag: artikel 2.31, twaalfde lid, WGS)

Met dit artikel wordt voor de Zorg- en Veiligheidshuizen invulling gegeven aan de toezegging uit de Kamerbrief van 17 december 2021 om het startpunt van de gegevensverwerking zoveel mogelijk te concretiseren.⁸⁶

De formulering sluit inhoudelijk gezien zo nauwkeurig mogelijk aan bij de criteria en bedoeling zoals die zijn beschreven in memorie van toelichting bij artikel 2.25 van de WGS:⁸⁷

"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 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."*

Eerste lid

Bij aanvang van een casus staat niet 100% vast dat de betreffende problemen zich zullen (blijven) voordoen. Deel van het werk is immers het verder onderzoeken en analyseren van de casus om zicht te krijgen op de problemen die er spelen, en om tot een goede aanpak te komen. De aanmelder zal voldoende aannemelijk moeten maken dat de casus aan de criteria voldoet.

Onderdeel a (problemen bij betrokkene of relevante problemen in zijn gezinssituatie)

Gelet op artikel 2.31, eerste lid, van de wet kan een casus alleen worden aangemeld "naar aanleiding van gedragingen van een betrokkene of een situatie waarin een betrokkene verkeert" die verband houden met het doel van de Zorg- en Veiligheidshuizen. De formulering van het eerste lid, aanhef, sluit hierop aan door te verlangen dat het moet gaan om problemen van betrokkene zelf of problemen in de gezinssituatie waarin betrokkene verkeert die van belang zijn voor betrokkene.

De formulering biedt aldus ook ruimte om een casus in behandeling te nemen in het Zorg- en Veiligheidshuis als er sprake is van problemen in de gezinssituatie waarin betrokkene verkeert, waardoor er een groot risico is dat betrokkene afglijdt naar problematisch gedrag. Dat kan bijvoorbeeld gaan om een jeugdige in een gezin waar volwassen gezinsleden crimineel gedrag vertonen, en waar een groot risico bestaat dat de jeugdige het crimineel circuit ingetrokken wordt. Het moet daarbij gaan om serieuze en objectiveerbare risico's die blijken uit het gedrag van de jeugdige. In een dergelijke situatie kan de jeugdige aangemeld worden in het Zorg- en Veiligheidshuis. De casus heeft dan betrekking op dit individuele jeugdige gezinslid. In het casusoverleg mogen vervolgens tevens gegevens worden verwerkt over natuurlijke personen uit de directe kring van betrokkene, bedoeld in artikel 2.30, eerste lid, van de wet, voor zover dat noodzakelijk is voor het doel van het Zorg- en Veiligheidshuis.

⁸⁵ Kamerstukken II 2019/20, 35447, nr. 3, blz. 125-126.

⁸⁶ Kamerstukken II 2021/22, 35447, nr. 21, bijlage, punt 1.

⁸⁷ Kamerstukken II 2019/20, 35447, nr. 3, blz. 106.

Consultatieversie nota van toelichting concept-BGS

Onderdeel b (meerdere leefgebieden)

Onderdeel b noemt de term "leefgebieden". Zoals opgemerkt in de memorie van toelichting bij de WGS 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".⁸⁸ Kortom, het gaat om aspecten van het leven die criminogene factoren kunnen bevatten, zoals financiën, wonen, zorg, gezin en werk.

Onderdeel c (ernstige overlast, criminaliteit of onveilige situaties)

Onderdeel c vereist als criterium voor behandeling van de casus dat de problemen door toedoen van betrokkene tot ernstige overlast, criminaliteit of onveilige situaties voor personen of binnen een gebied leiden, hebben geleid, of zonder interventie, zouden gaan leiden, gelet op duidelijke en objectieve aanwijzingen daarvoor. Dit vereiste is het spiegelbeeld van artikel 2.25 van de wet, dat bepaalt dat de Zorg- en Veiligheidshuizen zijn gericht op 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 criterium omvat dus mede de situaties die een hoog risico inhouden op afglijden naar ernstige overlast, criminaliteit of onveilige situaties. Daarover moeten dan duidelijke en objectieve aanwijzingen bestaan dat, indien niet wordt geïntervenieerd, de problemen daartoe zullen leiden. Dat betekent dat 'niets doen' vrijwel zeker leidt tot het veroorzaken van genoemde problemen. Betrokkene hoeft zich nog niet per se schuldig gemaakt te hebben aan die gedragingen.

Onderdeel d (multidisciplinaire samenwerking nodig)

Onderdeel d geeft aan dat samenwerking tussen meerdere ketens noodzakelijk moet zijn. Gedoeld wordt op samenwerking tussen deelnemers van het Zorg- en Veiligheidshuis uit enerzijds het strafrecht- of openbare orde en veiligheidsdomein met anderzijds deelnemers uit het zorg en/of sociaal domein.

Tweede lid (afstemming meerdere casussen)

Dit lid maakt het mogelijk om, indien er binnen Zorg- en Veiligheidshuizen meerdere casussen lopen rond betrokkenen die deel uit maken van elkaars directe kring (bijvoorbeeld omdat zij elkaar kennen van eenzelfde problematische groep), er tevens coördinatie kan plaatsvinden tussen deze individuele aanpakken. Het kan hier bijvoorbeeld gaan om leden van een problematische jeugdgroep die criminele activiteiten hebben ontplooid of ernstige overlast hebben veroorzaakt en waarbij de leden een sterke invloed hebben op elkaar. Het kan ook gaan om leden van families, waarbij de familieverbanden het bindmiddel zijn voor een groep die het probleemgedrag vertoont. Mits de individuele leden voldoen aan de criteria van het eerste lid, de betrokkenen behoren tot elkaars directe kring, er afhankelijkheden zijn tussen de problemen bij deze betrokkenen (de problemen, bedoeld in het eerste lid), of tussen de problemen die zij veroorzaken (bedoeld in het eerste lid, onder c), en de afstemming noodzakelijk is voor het doel van het Zorg- en Veiligheidshuis, kan het Zorg- en Veiligheidshuis zorgdragen voor coördinatie tussen deze aanpakken.

Overigens vloeit uit artikel 2.30, eerste lid, van de wet, dat bepaalt dat gegevens over personen uit de directe kring van betrokkene mogen worden verwerkt, reeds voort dat gegevens (waaronder een plan van aanpak) inzake een persoon uit de directe kring van betrokkene in een casusoverleg mogen worden betrokken in het casusoverleg indien dat nodig is met het oog op het plan van aanpak, maar duidelijkheidshalve is de mogelijkheid van afstemming van plannen van aanpak in het onderhavige artikellid uitgewerkt en geclausuleerd.

Derde lid (registreren of aan de criteria is voldaan)

De verplichting om te registreren of is voldaan aan de criteria dient meerdere doelen. Registratie maakt het mogelijk om aan betrokkene te kunnen verantwoorden waarom tot behandeling in het

⁸⁸ Dit staat in voetnoot 41 van de memorie van toelichting op WGS (Kamerstukken II 2019/20, 35447, nr. 3, blz. 106).

Zorg- en Veiligheidshuis is over gegaan. Een tweede doel is dat het hierdoor mogelijk wordt om in de audit op grond van artikel 1.10 van de wet na te gaan of de criteria in de praktijk ook op de juiste wijze worden gehanteerd. Ook kunnen de deelnemers deze informatie gebruiken voor eigen evaluaties. Ten derde kan de informatie gebruikt worden om zicht te krijgen op typen problematiek ten behoeve van beleidsinformatie. Bij de verwerking voor evaluatie en beleid zal uiteraard in passende waarborgen voor de privacy van betrokkene(n) moeten worden voorzien.

Artikel 2.21 Nadere criteria voor incidentele deelname aan Zorg- en Veiligheidshuis

(grondslag: artikel 2.31, twaalfde lid, WGS)

Zoals opgemerkt in de memorie van toelichting bij de wet kan incidentele deelname nodig zijn indien dat naar het oordeel van de betrokken deelnemers voor een goede behandeling van complexe persoonsgebonden casuïstiek noodzakelijk is.⁸⁹ Bij amvb kunnen uitdrukkelijke criteria worden gesteld op grond van artikel 2.31, twaalfde lid, van de wet. Daartoe dient het onderhavige artikel. Hiermee wordt tevens gevolg gegeven aan de aankondiging uit de Kamerbrief van 17 december 2021 dat uitdrukkelijk wordt voorzien in criteria voor incidentele deelname van derden aan de Zorg- en Veiligheidshuizen.⁹⁰ Volgens artikel 2.31, negende lid, van de wet moeten de in artikel 2.27, eerste lid, van de wet bedoelde deelnemers (de reguliere publieke deelnemers), indien zij een casus in behandeling nemen, beoordelen of het voor het doel van de Zorg- en Veiligheidshuizen noodzakelijk is om een partij als incidentele deelnemer te betrekken.

Eerste lid, algemeen

Dit lid stelt nadere criteria voor de incidentele deelname van derden door de voorwaarden waaronder zij deel mogen nemen te specificeren. Incidentele deelname aan een casuoverleg is mogelijk indien deze derden (1.) over deskundigheid beschikken die noodzakelijk is bij de aanpak van een specifieke casus en (2.) zij gelet op hun onderscheidenlijke *wettelijke of publieke* taken en bevoegdheden een rol kunnen vervullen bij het opstellen, uitvoeren of evalueren van het integrale plan van aanpak. Een publieke taak is een taak die niet wettelijk is geregeld, een maatschappelijke of politieke relevantie kent en waarbij de overheid betrokken is bij het beleidsterrein waartoe de taak gerekend kan worden.⁹¹

Bij de incidentele deelnemers kan worden gedacht aan de volgende partijen, uiteraard mits wordt voldaan aan de twee voornoemde voorwaarden:

- zorgpartijen (zoals bepaalde zorginstellingen of wijkverplegers),
- partijen die ondersteuning bieden op grond van een van de sociaal domeinwetten (bijv. een instelling voor gehandicaptenzorg, een aanbieder van jeugdhulp of bemoeizorg, een instelling voor beschermd wonen of professionals die als jeugdhulpverlener, maatschappelijk werker, of medewerker van de maatschappelijke opvang hulp of ondersteuning verlenen),
- welzijnsorganisaties (bijv. jongerenwerk),
- onderwijsinstellingen (de school waar betrokkene ingeschreven staat),
- bepaalde partijen uit het veiligheidsdomein (bijv. een organisatie voor resocialisatie),
- de woningcorporatie waarvan betrokkene een woning huurt en waar betrokkene ernstige overlast veroorzaakt, of
- experts die vanwege hun specifieke expertise, gelet op hun publieke taak, een rol kunnen vervullen bij het opstellen, uitvoeren of evalueren van het plan van aanpak. Daaronder valt ook het analyseren van de problematiek.

Bij deze laatste categorie valt te denken aan deskundigen van een hogeschool of ander kennisinstituut die met hun expertise bijdragen aan het plan van aanpak, zoals een deskundige op

⁸⁹ Kamerstukken II 2019/20, 35447, nr. 3, blz. 129.

⁹⁰ Kamerstukken II 2021/22, 35447, nr. 21, bijlage, punt 6.

⁹¹ Daarmee is een publieke taak te onderscheiden van een private taak. Met de voorgaande omschrijving van publieke taak wordt aangesloten bij artikel 5.2, derde lid, van de Comptabiliteitswet 2016. Zie de memorie van toelichting, [Kamerstukken II 2015/16, 34426, nr. 3](#), blz. 113.

Consultatieversie nota van toelichting concept-BGS

het gebied van interventies ten aanzien van jeugdgroep-leden, of een deskundige die duiding kan geven aan culturele aspecten die een rol kunnen spelen in de problematiek. De deskundigheid moet noodzakelijk zijn ten aanzien van de analyse van de problematiek en de totstandkoming van een effectief plan van aanpak. Op grond van de vereisten van proportionaliteit en subsidiariteit van de AVG betekent dat dat indien de advisering ook plaats kan vinden op basis van geanonimiseerde gegevens, of via een bilateraal advies aan een van de deelnemers, voor deze minder ingrijpende inbreuk op de persoonlijke levenssfeer van betrokkene wordt gekozen. Bij de vraag in hoeverre experts worden uitgenodigd, moet eerst worden gekeken of intern – bij de deelnemers – voldoende expertise is om te raadplegen. Zo niet, dan kunnen dit ook externe experts zijn.

Deelname persoon uit directe kring betrokkene

Voor zover dat naar het oordeel van de deelnemers, bedoeld in artikel 2.27, eerste lid, van de wet, een bijdrage levert aan het analyseren van de problematiek of het opstellen, uitvoeren of evalueren van het plan van aanpak, kunnen zij ook mensen uit de directe kring van betrokkene uitnodigen. Bij de complexe problematiek die in het Zorg- en Veiligheidshuis aan de orde is, is betrokkenheid van het sociale systeem rond betrokkene vaak van belang om de interventies, hulpverlening of ondersteuning succesvol te laten zijn en tot een duurzame oplossing te komen. Te denken valt aan situaties van ernstig en structureel huiselijk geweld waar bepaalde personen uit de omgeving een positieve invloed kunnen hebben, of jongvolwassenen bij wie ouders, grootouders of een oudere broer of zus een positieve rol kunnen spelen om verder afglijden naar criminaliteit te voorkomen. Een dergelijke rol heeft echter alleen zin als betrokkene daar zelf ook de waarde van inziet, en er geen conflicten of belangentegenstellingen spelen. Mede daarom is deelname van deze incidentele deelnemers alleen mogelijk met uitdrukkelijke toestemming van betrokkene. Gedoeld is hierbij op toestemming als bedoeld in artikel 6, eerste lid, onder a, gelezen in samenhang met artikel 9, tweede lid, onder a, van de AVG. Onder toestemming verstaat de AVG "elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling een hem betreffende verwerking van persoonsgegevens aanvaardt" (artikel 4, onderdeel 11, AVG). Er mag geen druk worden uitgeoefend op de betrokkene om diens toestemming te verkrijgen. Toestemming is immers geen geldige rechtsgrond voor de gegevensverwerking in een specifiek geval wanneer er sprake is van een duidelijke disbalans tussen de betrokkene en de verwerkingsverantwoordelijke, bijvoorbeeld als de verwerkingsverantwoordelijke een overheidsinstantie is én dit het onwaarschijnlijk maakt dat de toestemming in alle omstandigheden van die specifieke situatie vrijelijk is verleend (overweging 43 van de AVG). De toestemming moet dus daadwerkelijk vrijelijk zijn verleend. Bij de beoordeling is in de praktijk van belang dat een deel van de besproken betrokkenen in beeld is bij justitie of dat er sprake is van ten minste een vermoeden van psychiatrische problematiek. Hiermee dient rekening te worden gehouden bij de vraag of toestemming zou voldoen aan de voornoemde vereisten.

Deelname door betrokkene

Volledigheidshalve wordt opgemerkt dat noch het wetsvoorstel, noch dit besluit eraan in de weg staan dat betrokkene zelf wordt uitgenodigd voor deelname aan het casusoverleg, mits betrokkene dat zelf wenst en dit naar het oordeel van de deelnemers, bedoeld in artikel 2.27, eerste lid, van de wet, de kans op succes van de aanpak vergroot en het doel en de effectiviteit van het casusoverleg niet in de weg staat. Het betreft dan geen incidentele deelname van een derde, maar van de betrokkene. Het is aan de deelnemers, bedoeld in artikel 2.27, eerste lid, van de wet, om te bepalen of zij de betrokkene uitnodigen om deel te nemen. Deze deelnemers kunnen er ook voor kiezen om betrokkene niet te laten deelnemen, bijvoorbeeld omdat deelname opsporingsbelangen zou doorkruisen of zou bijten met de ruimte die professionals ervaren om hun strategieën op tafel te leggen.

Verder kan een wettelijk vertegenwoordiger of gevolmachtigde van de betrokkene namens hem deelnemen, waarbij de voornoemde condities voor deelname door betrokkene mutatis mutandis gelden. Het kan daarbij bijvoorbeeld gaan om ouders met gezag, een voogd of een door de rechter aangewezen curator of mentor.

Tweede lid (geheimhoudingsverklaring)

Dit lid bepaalt dat incidentele deelnemers een geheimhoudingsverklaring moeten tekenen. De geheimhoudingsplicht geldt op grond van artikel 1.11 WGS in samenhang met artikel 2.31, tiende lid, WGS ook voor derden die op incidentele basis deelnemen. Met de geheimhoudingsverklaring verklaart de derde dat hij bekend is met deze geheimhoudingsplicht en deze zal naleven.

Derde lid (geen autorisatie voor systemen)

Dit lid geeft een concretisering van artikel 2.31, negende lid, WGS, dat bepaalt dat de derden uitsluitend toegang krijgen tot de persoonsgegevens die in het Zorg- en Veiligheidshuis worden verwerkt voor zover dat noodzakelijk is voor het doel, bedoeld in artikel 2.25. Derden krijgen geen toegang tot de systemen. Deze beperking vooraf voorkomt onnodige risico's, onder meer omdat derden in principe niet worden gescreend voor een incidentele deelname. Wel kan de derde voor een beperkt deel in kennis worden gesteld van beschikbare informatie. Daarom opent het derde lid de mogelijkheid dat deelnemers, bedoeld in artikel 2.27, eerste lid, WGS, aan de derde relevante persoonsgegevens verstrekken om de derde in staat te stellen zijn rol uit te voeren.

Artikel 2.22 Objectieve criteria voor plaatsing op een lijst van geprioriteerde casussen

(grondslag: artikel 2.32, vijfde lid, WGS)

Artikel 2.32 van de wet bepaalt dat de in artikel 2.27, eerste lid, van de wet bedoelde deelnemers (de reguliere publiekrechtelijke deelnemers) objectieve criteria opstellen op basis waarvan de casus van een betrokkene op de lijst met geprioriteerde casussen van een Zorg- en Veiligheidshuis wordt geplaatst.

Het onderhavige artikel bepaalt de ondergrens voor de te hanteren criteria. Volgens onderdeel a moet betrokkene ten minste voldoen aan de criteria voor behandeling in het Zorg- en Veiligheidshuis, bedoeld in artikel 2.20. Onderdeel b bepaalt dat de deelnemers in aanvulling daarop objectieve criteria moeten stellen als bedoeld in artikel 2.32, eerste lid, WGS. Zoals is beschreven in de memorie van toelichting, is het vaststellen van een lijst van geprioriteerde casussen, ook wel "Top X"-aanpak genoemd, nodig om extra aandacht te schenken aan personen die het meest bijdragen aan de criminaliteit of onveiligheid dan wel een hoog veiligheidsrisico hebben, en om de beschikbare middelen bij voorrang in te zetten op de aldus geselecteerde casussen.⁹²

Het kan dus niet zo zijn dat iemand op de lijst wordt geplaatst op grond van uitsluitend de criteria van artikel 2.20. Bij deze objectieve criteria kan het bijvoorbeeld gaan om het aanvullende criterium dat iemand binnen een periode van een jaar meerdere malen is aangehouden in verband met overlastgevend criminaliteit. Een ander aanvullend criterium kan bijvoorbeeld zijn dat iemand deel uitmaakt van een jeugdgroep die ernstige overlast veroorzaakt. De aanvullende criteria kunnen per Zorg- en Veiligheidshuis verschillen. Ook is het mogelijk dat in een Zorg- en Veiligheidshuis geprioriteerde lijsten bestaan voor verschillende problematieken, met eigen aanvullende criteria. Dit biedt de mogelijkheid om in te spelen op de veiligheidsproblematieken die in een bepaalde regio spelen.

De aanvullende criteria kunnen in de loop van de tijd aangepast worden. Bijvoorbeeld als een bepaald probleem weer tot beheersbare proporties is teruggebracht, is er geen reden meer voor die betreffende geprioriteerde lijst en zal deze vervallen. Als zich een nieuw veiligheidsprobleem aandient waarvoor het prioriteren van casussen noodzakelijk wordt geacht, kan een nieuwe lijst met nieuwe aanvullende criteria opgesteld worden.

Artikel 2.32, eerste lid, van de wet bepaalt dat de objectieve criteria voor plaatsing op een lijst met geprioriteerde casussen openbaar moeten worden gemaakt. Onderdeel c van het onderhavige artikellid voegt daaraan toe dat dit geschiedt op internet.

⁹² Kamerstukken II 2019/20, 35447, nr. 3, blz. 110 en 131.

HOOFDSTUK 3. WIJZIGING VAN ANDERE BESLUITEN

Artikel 3.1 Wijziging Besluit politiegegevens

(grondslag: artikel 4.1 WGS)

De nieuwe grondslag voor verstrekking van politiegegevens aan de RIEC's is artikel 20, derde lid, van de Wet politiegegevens. Die bepaling is toegevoegd door artikel 4.1 van de WGS. Hierdoor is artikel 4:3, zevende lid, van het Besluit politiegegevens overbodig geworden als grondslag voor de verstrekking van politiegegevens die worden verwerkt op grond van artikel 9 of 10, eerste lid onder a of c, van de Wpg. Het nieuwe artikel 20, derde lid, Wpg biedt immers een grondslag om politiegegevens te verstrekken aan een RIEC, ook als het gaat om politiegegevens in de zin van artikelen 9 en 10, eerste lid, onderdelen a en c, Wpg. Daarbij stelt artikel 20, derde lid, als voorwaarden dat de verstrekking geschiedt in overeenstemming met het bevoegd gezag (het Openbaar Ministerie of de burgemeester), dat de verstrekking noodzakelijk is voor het doel van het RIEC en dat zich naar het oordeel van de verwerkingsverantwoordelijke geen zwaarwegende redenen tegen verstrekking verzetten. Overigens is van artikel 20 Wpg uitsluitend het derde lid van toepassing op de verstrekking aan een RIEC, dus niet het eerste en tweede lid.

In artikel 2.23, zesde lid, in samenhang gelezen met artikel 2.22, eerste lid, onderdeel a, onder 2^o en 3^o, van de WGS is geregeld dat politiegegevens in de zin van artikel 8 en 13 Wpg pas in de zogeheten tweede fase van gegevensverwerking aan een RIEC worden verstrekt en dat politiegegevens die worden verwerkt overeenkomstig artikel 9 of 10, eerste lid onder a of c, Wpg pas in de derde fase van gegevensverwerking aan een RIEC worden verstrekt. Dat laatste mag op grond van artikel 2.23, zesde lid, onder c, WGS uitsluitend als het gaat om een activiteit als bedoeld in artikel 2.18, eerste lid, onderdeel a (aanwijzen en analyseren van handhavingsknelpunten) of onderdeel b (het voeren een casusoverleg).

De Minister van Justitie en Veiligheid,