

380

Besluit van 29 november 2024 tot uitvoering van de Wet gegevensverwerking door samenwerkingsverbanden (Besluit gegevensverwerking door samenwerkingsverbanden) en tot vaststelling van het tijdstip van inwerkingtreding van die wet en van de Wet van 26 juni 2024 tot wijziging van de Wet gegevensverwerking door samenwerkingsverbanden in verband met het waarborgen van de parlementaire betrokkenheid bij de aanwijzing van andere samenwerkingsverbanden (Stb. 2024, 254)

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

Op de voordracht van Onze Minister van Justitie en Veiligheid van 13 juni 2024, directie Wetgeving en Juridische Zaken, nr. 5546793;

Gelet op de artikelen 1.1, derde streepje, 1.4, vierde lid, 1.8, 1.9, vijfde lid, 1.10, vijfde lid, 2.3, eerste lid, onder h, 2.4, tweede lid, 2.6, tweede lid, 2.7, tweede lid, 2.11, eerste lid, onder j, 2.12, derde lid, 2.14, 2.16, tweede lid, 2.19, tweede lid, 2.22, tweede lid, 2.23, negende lid, 2.24, tweede lid, 2.30, tweede lid, 2.31, twaalfde lid, 2.32, vijfde lid, 4.1 en 5.2 van de Wet gegevensverwerking door samenwerkingsverbanden;

De Afdeling advisering van de Raad van State gehoord (advies van 2 oktober 2024, no. W16.24.00142/II);

Gezien het nader rapport van Onze Minister van Justitie en Veiligheid, van 26 november 2024, directie Wetgeving en Juridische Zaken, nr. 5844557;

Hebben goedgevonden en verstaan:

HOOFDSTUK 1. ALGEMENE BEPALINGEN

Artikel 1.1 Aanwijzing contactpunt

1. De betrokkene richt een verzoek tot uitoefening van diens rechten op grond van hoofdstuk III van de Algemene verordening gegevensbescherming aan het contactpunt, voor zover dat verzoek betrekking heeft op persoonsgegevens die door het samenwerkingsverband worden verwerkt. Een verzoek aan het contactpunt geldt als een verzoek aan alle

gezamenlijke verwerkingsverantwoordelijken in het samenwerkingsverband.

2. Als contactpunt voor een betrokkene voor de uitoefening van diens rechten op grond van hoofdstuk III van de Algemene verordening gegevensbescherming treedt op namens de deelnemers aan het samenwerkingsverband:

a. in het geval van het Financieel Expertisecentrum: De Nederlandsche Bank N.V.;

b. in het geval van de Infobox Crimineel en Onverklaarbaar Vermogen: het Openbaar Ministerie;

c. in het geval van een Regionaal Informatie- en Expertisecentrum: de burgemeester van een deelnemende gemeente waarvan de deelnemers overeenkomen dat die burgemeester als contactpunt optreedt;

d. in het geval van een Zorg- en Veiligheidshuis: het college van burgemeester en wethouders of de burgemeester van een deelnemende gemeente waarvan de gezamenlijke verwerkingsverantwoordelijken overeenkomen dat dat college of die burgemeester als contactpunt optreedt.

3. De website van het samenwerkingsverband vermeldt de overheidsinstantie die als contactpunt fungeert en de voor indiening van een verzoek benodigde contactgegevens.

4. In dit besluit wordt onder «wet» verstaan: Wet gegevensverwerking door samenwerkingsverbanden.

Artikel 1.2 Verantwoordelijkheid voor nakoming verzoeken AVG

1. Het contactpunt besluit namens de deelnemers aan het samenwerkingsverband op een verzoek van een betrokkene tot uitoefening van diens rechten op grond van hoofdstuk III van de Algemene verordening gegevensbescherming voor zover dat verzoek betrekking heeft op persoonsgegevens die door het samenwerkingsverband worden verwerkt.

2. Het contactpunt besluit na overleg met de deelnemers die betrokken waren of zijn bij de verwerking van de persoonsgegevens over de betrokkene, en wijst het verzoek af indien of voor zover naar het oordeel van één of meer van die deelnemers een uitzonderingsgrond van toepassing is op grond van artikel 41 van de Uitvoeringswet Algemene verordening gegevensbescherming.

3. Zodra de uitzonderingsgrond naar het oordeel van de betreffende deelnemer niet langer van toepassing is, meldt de deelnemer dit zo spoedig mogelijk aan het contactpunt.

4. Een andere deelnemende overheidsinstantie of ander deelnemend overheidsorgaan kan met het contactpunt overeenkomen om het besluit te nemen indien die andere deelnemer daartoe beter in staat is. In dat geval informeert het contactpunt de betrokkene hierover. Het eerste tot en met het derde lid zijn van overeenkomstige toepassing op de andere deelnemer die het besluit neemt.

Artikel 1.3 Verantwoordelijkheid voor nakoming informatieplicht

1. Het contactpunt draagt namens de deelnemers aan het samenwerkingsverband zorg voor de nakoming van de verplichting om de informatie te verstrekken, bedoeld in artikel 14 van de Algemene verordening gegevensbescherming, inzake de verwerking van persoonsgegevens door het samenwerkingsverband.

2. Het contactpunt overlegt met de deelnemers die betrokken waren of zijn bij de verwerking van de persoonsgegevens over de betrokkene en laat de uitvoering van het eerste lid achterwege indien naar het oordeel van één of meer van die deelnemers, een uitzonderingsgrond van toepassing is op grond van artikel 14, vijfde lid, onder b, van de Algemene

verordening gegevensbescherming of artikel 41 van de Uitvoeringswet Algemene verordening gegevensbescherming.

3. Zodra de uitzonderingsgrond naar het oordeel van de betreffende deelnemer niet langer van toepassing is, meldt de deelnemer dit zo spoedig mogelijk aan het contactpunt.

Artikel 1.4 Verantwoordelijkheid voor nakoming meldplicht datalekken

1. Het contactpunt draagt namens de deelnemers aan het samenwerkingsverband zorg voor de nakoming van de artikelen 33 en 34 van de Algemene verordening gegevensbescherming met betrekking tot de verwerking van persoonsgegevens door het samenwerkingsverband, mits de deelnemers aan het contactpunt zo spoedig mogelijk de informatie verstrekken die het contactpunt nodig heeft voor de uitvoering van de voornoemde artikelen.

2. Het contactpunt overlegt met de deelnemers die betrokken waren of zijn bij de verwerking van de persoonsgegevens en laat de uitvoering van artikel 34 van de Algemene verordening gegevensbescherming achterwege indien naar het oordeel van één of meer van die deelnemers een uitzonderingsgrond van toepassing is op grond van artikel 41 van de Uitvoeringswet Algemene verordening gegevensbescherming.

Artikel 1.5 Rechtmatig verwerkte gegevens

De deelnemers verstrekken uitsluitend gegevens die zij rechtmatig verwerken aan het samenwerkingsverband.

Artikel 1.6 Kwaliteit van een aangemeld signaal, verzoek of casus

1. Een deelnemer mag uitsluitend een signaal, verzoek of casus aanmelden bij het samenwerkingsverband na, voor zover mogelijk, de feitelijke juistheid en de kwaliteit van de daarbij te verstrekken gegevens te hebben getoetst.

2. De deelnemer die een signaal, verzoek of casus heeft aangemeld bij het samenwerkingsverband blijft verantwoordelijk voor de feitelijke juistheid van de daarbij verstrekte gegevens.

Artikel 1.7 Correctie van onjuistheden tijdens gezamenlijke gegevensverwerking

1. Mocht tijdens de verwerking van gegevens door het samenwerkingsverband blijken dat gegevens onjuist zijn, dan wordt de deelnemer die deze aan het samenwerkingsverband heeft verstrekt daarop gewezen en draagt deze deelnemer zorg dat alle redelijke maatregelen worden genomen om de gegevens onverwijld te vernietigen of rectificeren.

2. De deelnemer die de onjuiste gegevens heeft verstrekt aan het samenwerkingsverband doet, indien van toepassing, een melding aan de organisatie waarvan de gegevens afkomstig zijn, opdat ook in de gegevensbestanden van die organisatie kan worden gecontroleerd of de gegevens juist zijn geregistreerd en deze na validatie kunnen worden gecorrigeerd.

Artikel 1.8 Kwaliteit van de resultaten

1. Een samenwerkingsverband verstrekt uitsluitend het resultaat van de gezamenlijke gegevensverwerking aan een deelnemer of derde overeenkomstig artikel 1.7 van de wet, na, voor zover mogelijk, de feitelijke

juistheid en de kwaliteit van de daarbij te verstrekken gegevens te hebben getoetst.

2. Voor zover mogelijk vermeldt het samenwerkingsverband bij de verstrekking van een resultaat dat bestaat uit sturingsinformatie of een interventieadvies, op basis van welke informatie het resultaat tot stand is gekomen, tenzij het resultaat is gebaseerd op een casusoverleg of signalenoverleg.

Artikel 1.9 Nationaliteit

De samenwerkingsverbanden verwerken geen persoonsgegevens inzake nationaliteit, tenzij de verwerking geschiedt met het oog op de identificatie van de betrokkene, en slechts voor zover de verwerking voor dat doel onvermijdelijk is.

Artikel 1.10 Nadere inkadering van gegevensuitwisseling tussen samenwerkingsverbanden

1. De bevoegdheid tot verstrekking van de resultaten aan een ander samenwerkingsverband, bedoeld in artikel 1.7, achtste lid, van de wet, kan uitsluitend op de navolgende wijzen worden toegepast:

a. Indien een samenwerkingsverband vaststelt dat een betrokkene tevens bekend is bij een ander samenwerkingsverband, mogen beide samenwerkingsverbanden gegevens uitwisselen over welke deelnemers in beide samenwerkingsverbanden bij de betreffende gegevensverwerking betrokken zijn of zijn geweest.

b. In aanvulling op onderdeel a mogen een Zorg- en Veiligheidshuis en een Regionaal Informatie- en Expertisecentrum gegevens uitwisselen die noodzakelijk zijn om afspraken over interventies van de deelnemers in de beide samenwerkingsverbanden op elkaar af te stemmen.

c. In aanvulling op onderdeel a mogen een Regionaal Informatie- en Expertisecentrum en het Financieel Expertisecentrum gegevens uitwisselen die noodzakelijk zijn om afspraken over interventies van de deelnemers in de beide samenwerkingsverbanden op elkaar af te stemmen;

d. De aanvrager van een rapportage van de Infobox Crimineel en Onverklaarbaar Vermogen die tevens deelneemt aan een Regionaal Informatie- en Expertisecentrum of het Financieel Expertisecentrum mag een ontvangen rapportage verstrekken aan dat verband indien aldaar een signaal wordt besproken over een persoon die onderwerp is van die rapportage.

2. Tussen samenwerkingsverbanden worden geen gegevens uitgewisseld waarop een wettelijke geheimhoudingsplicht rust als bedoeld in de volgende artikelen:

a. artikel 457 van Boek 7 van het Burgerlijk Wetboek;

b. artikel 88 van de Wet op de beroepen in de individuele gezondheidszorg;

c. artikel 7.3.11 van de Jeugdwet;

d. artikel 8:34 van de Wet verplichte geestelijke gezondheidszorg;

e. artikel 18c, vierde lid, van de Wet zorg en dwang psychogeriatrische en verstandelijke gehandicapte cliënten.

3. Bij de toepassing van het eerste lid worden geen gegevens van de rijksbelastingdienst, met uitzondering van de Fiscale Inlichtingen- en Opsporingsdienst, verstrekt aan een private deelnemer van een samenwerkingsverband voor de behartiging van diens gerechtvaardigde belangen.

Artikel 1.11 Betrouwbaarheid geautoriseerde personen

1. Personen die zijn aangewezen ten behoeve van de inzet in het samenwerkingsverband worden uitsluitend geautoriseerd voor de toegang tot de systemen waarin de deelnemers gezamenlijk persoonsgegevens verwerken overeenkomstig artikel 1.8, tweede lid, van de wet, indien zij ten minste:

a. in het bezit zijn van een verklaring omtrent het gedrag die voor indiensttreding bij de betreffende deelnemer vereist is; of

b. zijn gescreend overeenkomstig de wettelijke bepalingen die van toepassing zijn op de betreffende deelnemers waar zij in dienst zijn.

2. In afwijking van het eerste lid worden personen die zijn aangewezen ten behoeve van de inzet in de Infobox Crimineel en Onverklaarbaar Vermogen uitsluitend geautoriseerd indien zij zijn gescreend op basis van de eisen die gelden voor het hoogste rubriceringsniveau dat van toepassing is op de gegevens die de deelnemers verwerken.

Artikel 1.12 Logging

De vastlegging langs elektronische weg (logging) van verwerkingen van persoonsgegevens in de systemen van het samenwerkingsverband, bedoeld in artikel 1.8, vierde lid, van de wet, geschiedt overeenkomstig de door Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties vastgestelde richtlijnen voor informatiebeveiliging.

Artikel 1.13 Werkwijze van de rechtmatigheidsadviescommissie

1. De rechtmatigheidsadviescommissie van een samenwerkingsverband kan ter uitoefening van haar taak, bedoeld in artikel 1.8, zesde lid, van de wet, adviseren op verzoek van de deelnemers of op eigen initiatief. De deelnemers zorgen ervoor dat de rechtmatigheidsadviescommissie daartoe naar behoren vooraf wordt betrokken bij in ieder geval nieuwe verwerkingswijzen en wijzigingen daarvan.

2. De rechtmatigheidsadviescommissie adviseert, zonder voorafgaande toestemming, rechtstreeks aan de bestuurders van de deelnemers die het samenwerkingsverband aansturen.

3. Een uit te brengen advies wordt vastgesteld in overleg tussen de leden die zijn benoemd door de deelnemers die het advies aangaat dan wel, bij de Regionale Informatie- en Expertisecentra en de Zorg- en Veiligheidshuizen, met personen uit koepelorganisaties of brancheverenigingen, bedoeld in artikel 1.15, tweede lid, indien het advies de deelnemers aangaat die door de koepelorganisaties of brancheverenigingen worden vertegenwoordigd.

4. Een lid dat een standpunt heeft ingebracht dat afwijkt van het standpunt van de andere leden, kan over dat standpunt een afzonderlijke nota bij het advies voegen.

5. Een rechtmatigheidsadviescommissie kan haar werkwijze nader vaststellen in een reglement van orde.

6. Afwijking van een advies van de rechtmatigheidsadviescommissie door de bestuurders, bedoeld in het tweede lid, kan uitsluitend beargumenteerd plaatsvinden. De afwijking wordt door de deelnemers gedocumenteerd en gerapporteerd aan de rechtmatigheidsadviescommissie en de coördinerend functionaris voor gegevensbescherming voor het samenwerkingsverband, bedoeld in artikel 1.4, tweede lid, van de wet.

Artikel 1.14 Samenstelling van de rechtmatigheidsadviescommissie

1. Elke deelnemer benoemt een of enkele personen als lid van de rechtmatigheidsadviescommissie, op basis van deskundigheid en ervaring op het gebied van de toepasselijke wetgeving inzake gegevensverwerking en de werking van het samenwerkingsverband.
2. Zolang niet in de benoeming van een lid in de rechtmatigheidsadviescommissie is voorzien, kan de betreffende deelnemer een lid van een andere deelnemer verzoeken om waar te nemen.
3. In afwijking van het eerste lid zijn deelnemende private partijen niet verplicht maar bevoegd om een of enkele personen als lid van de rechtmatigheidsadviescommissie te benoemen.
4. De leden dragen er zorg voor dat in de rechtmatigheidsadviescommissie aandacht is voor het tegengaan van risico's op ongelijke behandeling en discriminatie.
5. De rechtmatigheidsadviescommissie kiest uit haar midden een voorzitter en een plaatsvervangend voorzitter.

Artikel 1.15 Rechtmatigheidsadviescommissie voor cluster van samenwerkingsverbanden

1. Zowel de Regionale Informatie- en Expertisecentra als de Zorg- en Veiligheidshuizen beschikken over één gezamenlijke rechtmatigheidsadviescommissie, die optreedt ten behoeve van het betreffende cluster van samenwerkingsverbanden.
2. De lokale en regionale deelnemers worden vertegenwoordigd door personen uit koepelorganisaties of brancheverenigingen, die deelnemen als lid van de gezamenlijke rechtmatigheidsadviescommissie, op basis van de deskundigheid en ervaring, bedoeld in artikel 1.14, eerste lid.

Artikel 1.16 Precisering maximale bewaartermijn

1. Onverminderd artikel 1.8, zevende lid, van de wet dragen de deelnemers zorg voor de vernietiging of anonimisering van persoonsgegevens die door het samenwerkingsverband gezamenlijk worden verwerkt in het geval dat:
 - a. 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; of
 - b. een aangemeld signaal, verzoek of casus niet in behandeling wordt genomen door het samenwerkingsverband.
2. Van bijzondere gevallen waarin hernieuwde verwerking van gezamenlijke verwerkte persoonsgegevens overeenkomstig artikel 1.8, zevende lid, van de wet is toegestaan, is uitsluitend sprake indien de deelnemers van een Zorg- en Veiligheidshuis een casus behandelen die:
 - a. na het verstrijken van de maximale bewaartermijn nog niet is afgesloten omdat de problematiek dermate complex is dat deze casus nog steeds voldoet aan de criteria voor behandeling in het Zorg- en Veiligheidshuis, bedoeld in artikel 2.20 van dit besluit;
 - b. minder dan een jaar voor het verstrijken van de maximale bewaartermijn is afgesloten, maar waarbij gezien de complexiteit van de problematiek een groot risico bestaat op terugval waardoor weer zou worden voldaan aan de voornoemde criteria.
3. Bij toepassing van het tweede lid is de bewaartermijn voor gegevens die ter beschikking zijn gesteld voor hernieuwde verwerking maximaal twee jaar gerekend vanaf de hernieuwde beschikbaarstelling. Indien daarna nog steeds sprake is van een bijzonder geval als bedoeld in het tweede lid, onderdeel a of b, kan het tweede lid opnieuw toepassing vinden.

Artikel 1.17 Opleiding en training ten aanzien van gegevensverwerking

De deelnemers aan een samenwerkingsverband dragen er zorg voor dat de medewerkers die zij hebben aangewezen voor de inzet in het samenwerkingsverband, voor zover relevant voor hun functie, en de leden van de rechtmatigheidsadviescommissie passende opleidingen en trainingen krijgen ter bevordering van hun kennis en vaardigheden op het gebied van:

- a. een zorgvuldige omgang met persoonsgegevens;
- b. de regels die op het samenwerkingsverband van toepassing zijn;
- c. de werkprocessen van het samenwerkingsverband;
- d. methoden en technieken van informatieanalyse;
- e. informatiebeveiliging;
- f. data-ethiek.

Artikel 1.18 Uitwerking auditbepaling

1. Twee jaren na inwerkingtreding van de artikelen in de wet en dit besluit inzake het betreffende samenwerkingsverband, en vervolgens eenmaal in de vier jaren, laat het samenwerkingsverband de naleving van de wettelijke regels, bedoeld in artikel 1.10, eerste lid, van de wet, controleren door middel van een audit overeenkomstig artikel 1.10 van de wet.

2. De audit wordt uitgevoerd door middel van een privacy audit. Hiertoe vindt een beoordeling plaats van de opzet en het bestaan van maatregelen en procedures die in de adequate uitvoering van de regels, bedoeld in artikel 1.10, eerste lid, van de wet, moeten voorzien, en van de werking van de getroffen maatregelen en procedures.

3. De auditor is onafhankelijk ten opzichte van de deelnemers van het samenwerkingsverband en beschikt over deskundigheid en ervaring op het gebied van de werking van het samenwerkingsverband en de toepasselijke wetgeving inzake gegevensverwerking.

4. De auditor zendt een afschrift van de controleresultaten van de privacy audits aan de rechtmatigheidsadviescommissie en de coördinerend functionaris voor gegevensbescherming voor het samenwerkingsverband, bedoeld in artikel 1.4, tweede lid, van de wet.

5. Bij ministeriële regeling kunnen nadere regels worden gesteld over de wijze waarop de audits worden verricht.

HOOFDSTUK 2. BEPALINGEN INZAKE SPECIFIEKE SAMENWERKINGSVERBANDEN

Paragraaf 2.1 Financieel Expertisecentrum (FEC)

Artikel 2.1 Aanvullende deelnemers Programma Terrorismedinanciering

Voor zover in het Financieel Expertisecentrum als onderdeel van zijn doelstelling gezamenlijk gegevens worden verwerkt ten behoeve van het programma voor het tegengaan en bestrijden van terrorismedinanciering worden, in aanvulling op artikel 2.3, eerste lid, van de wet, als deelnemers van het Financieel Expertisecentrum aangewezen:

- a. het Bureau Financieel Toezicht, ten behoeve van de uitvoering en de handhaving van de Wet ter voorkoming van witwassen en financieren van terrorisme en ten behoeve van de in artikel 110 van de Wet op het notarisambt en de in artikel 30 van de Gerechtsdeurwaarderswet opgedragen taken;

- b. het Bureau Toezicht Wet ter voorkoming van witwassen en financieren van terrorisme, ten behoeve van het toezicht op de naleving van die wet;
- c. de Koninklijke Marechaussee, voor de uitoefening van de wettelijke taken en bevoegdheden bij of krachtens artikel 4 van de Politiewet 2012;
- d. de Douane, voor het uitvoeren van de wettelijke taken en bevoegdheden bij of krachtens het Douanewetboek van de Unie en de Algemene douanewet;
- e. de Dienst Toeslagen, bedoeld in artikel 11 van de Algemene wet inkomensafhankelijke regelingen, voor het uitvoeren van de wettelijke taken en bevoegdheden bij of krachtens de hoofdstukken 2 en 3 van die wet;
- f. de Immigratie- en Naturalisatiedienst, voor de uitvoering van de wettelijke taken en bevoegdheden op het terrein van toezicht en handhaving bij of krachtens de Vreemdelingenwet 2000 en de Rijkswet op het Nederlanderschap;
- g. de Algemene Inlichtingen- en Veiligheidsdienst, voor de uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten 2017, met dien verstande dat uitsluitend gegevens aan het Financieel Expertisecentrum worden verstrekt voor zover dat noodzakelijk is voor het duiden van bepaalde financieringsstromen en het verstrekken van gegevens over een bredere internationale context.

Artikel 2.2 Deelnemers aan publiek-private samenwerking

Voor zover in het Financieel Expertisecentrum gezamenlijk gegevens worden verwerkt in publiek-private taskforces 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, nemen uitsluitend deel:

- a. het Openbaar Ministerie, de politie, de Financiële inlichtingen eenheid en de Fiscale Inlichtingen- en Opsporingsdienst, voor de in artikel 2.3 van de wet genoemde taken;
- b. ABN Amro Bank, Aegon, ING Bank, KNAB, Rabobank, Triodos en Volksbank, voor de uitvoering van hun verplichtingen op grond van de Wet ter voorkoming van witwassen en financieren van terrorisme en voor de voornoemde doeleinden van de publiek-private taskforces.

Artikel 2.3 Beperking gegevensverwerking over kring van personen

1. Voor zover in het Financieel Expertisecentrum gezamenlijk gegevens worden verwerkt voor het programma ter bestrijding van terrorismefinanciering of in publiek-private taskforces 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, verwerken de deelnemers in het kader van dat programma of die taskforces, gegevens over een relatie of een contact als bedoeld in artikel 2.4, eerste lid, onderdeel e, van de wet, tot maximaal drie directe lijnen vanaf de betrokken rechtspersoon of natuurlijke persoon.

2. Tot een ruimere verwerking van gegevens over relaties of contacten kan worden overgegaan, voor zover sprake is van een keten van vermogensverschaffers, leidinggevendenden, zeggenschaphebbenden of van personen die in een zakelijk samenwerkingsverband staan tot de betrokken rechtspersoon of natuurlijke persoon, en wordt gemotiveerd waarom de gegevens noodzakelijk zijn voor het doel, bedoeld in artikel 2.2 van de wet.

Artikel 2.4 Criteria voor behandeling van een signaal of verzoek

1. Een signaal of verzoek van een deelnemer kan in het Financieel Expertisecentrum uitsluitend aanleiding vormen tot het signalenoverleg, bedoeld in artikel 2.6 van de wet, onderscheidenlijk een gegevensanalyse, bedoeld in artikel 2.7 van de wet, indien:

a. sprake is van duidelijke en objectieve aanwijzingen van een of meerdere deelnemers dat bepaalde gedragingen of situaties verband kunnen houden met:

1° een inbreuk op de integriteit van natuurlijke of rechtspersonen die binnen het financiële stelsel werkzaam zijn, of

2° het gebruik van het financiële stelsel, of onderdelen daarvan, voor financieel-economische criminaliteit, terrorismefinanciering en andere ernstige vormen van criminaliteit;

b. gezamenlijke gegevensverwerking noodzakelijk is in relatie tot het doel van het Financieel Expertisecentrum, bedoeld in artikel 2.2 van de wet;

c. de analyse van het signaal of verzoek naar verwachting de samenwerking met meerdere deelnemers van het Financieel Expertisecentrum vergt; en

d. het signaal of verzoek een vermelding omvat van:

1°. de feiten, omstandigheden en gedragingen die relevant zijn voor het signaal of verzoek;

2°. de rechtspersoon, de natuurlijke persoon of het object waarop het signaal of verzoek ziet en zijn relatie met de gevraagde gegevens;

3°. indien een verzoek wordt gedaan tot een gegevensanalyse: een afbakening welke informatie hiervoor nodig is, met een toelichting daarop.

2. Bij een signaal of verzoek dat betrekking heeft op het gezamenlijk verwerken van gegevens in een publiek-private taskforce, bedoeld in artikel 2.2, geldt in aanvulling op het eerste lid als vereiste dat het signaal of verzoek is ingediend door de politie of de Fiscale Inlichtingen- en Opsporingsdienst, onder vermelding van de identificerende gegevens van een persoon die in verband kan worden gebracht met een voornoemde vorm van criminaliteit of de financiering daarvan.

3. Voor de toepassing van het eerste lid, onderdeel a, onder 2°, wordt onder «andere ernstige vormen van criminaliteit» dan financieel-economische criminaliteit en terrorismefinanciering verstaan: misdrijven die een ernstige inbreuk op de rechtsorde opleveren als bedoeld in het Wetboek van Strafvordering, voor zover die tevens de integriteit van het financiële stelsel raken.

Artikel 2.5 Nadere waarborgen signalenoverleg en gegevensanalyse

Bij het signalenoverleg, bedoeld in artikel 2.6, eerste lid, van de wet, en de gegevensanalyse op grond van artikel 2.7, eerste lid, van de wet, gelden de volgende aanvullende waarborgen:

a. de deelnemer die het signaal voor het signalenoverleg of verzoek om een gegevensanalyse aanmeldt, draagt er zorg voor dat in de aanmelding is toegelicht in hoeverre is voldaan aan de criteria, bedoeld in artikel 2.4;

b. bij de afweging of een signaal of verzoek voldoende aanleiding geeft tot gezamenlijke verwerking van gegevens in het Financieel Expertisecentrum toetsen de deelnemers aan de vraag of is voldaan aan de criteria, bedoeld in artikel 2.4;

c. de deelnemers registreren een signaal of verzoek in het systeem waarin zij gezamenlijk gegevens verwerken, met de vermelding of naar hun oordeel is voldaan aan de criteria voor het in behandeling nemen van dat signaal onderscheidenlijk verzoek;

d. de vergelijking van gegevens van de deelnemers houdt verband met de feiten, omstandigheden en gedragingen die via het signaal of het verzoek zijn aangemeld.

Paragraaf 2.2 Infobox Crimineel en Onverklaarbaar Vermogen (iCOV)

Artikel 2.6 Aanvullende deelnemers

In aanvulling op artikel 2.11, eerste lid, van de wet worden als deelnemers aan de Infobox Crimineel en Onverklaarbaar Vermogen aangewezen:

a. de Stichting Autoriteit Financiële Markten, voor de uitoefening van haar wettelijke taken en bevoegdheden bij of krachtens de Wet handhaving consumentenbescherming, Wet op het financieel toezicht, Wet ter voorkoming van witwassen en financieren van terrorisme, Wet toezicht accountantsorganisaties, Wet toezicht financiële verslaggeving, Pensioenwet, Wet verplichte beroepspensioenregeling, Sanctiewet 1977 en bindende rechtshandelingen van de Europese Unie;

b. de Koninklijke marechaussee, voor de uitoefening van de wettelijke taken en bevoegdheden bij of krachtens artikel 4 van de Politiewet 2012.

Artikel 2.7 Beperking gegevensverwerking over kring van personen

1. Ten behoeve van de rapportage over de financieel-zakelijke relaties rondom natuurlijke of rechtspersonen (iRR), bedoeld in artikel 2.13, aanhef en onderdeel b, van de wet, verwerken de deelnemers gegevens over relaties of contacten als bedoeld in artikel 2.12, eerste lid, onderdeel e, van de wet, in een rapportage tot drie directe lijnen vanaf de natuurlijke persoon of rechtspersoon waarop het verzoek betrekking heeft.

2. Tot een ruimere verwerking van gegevens over relaties of contacten kan worden overgegaan, voor zover sprake is van een keten van vermogensverschaffers, leidinggevend, zeggenschaphebbenden of van personen die in een zakelijk samenwerkingsverband staan tot de betrokken natuurlijke persoon of rechtspersoon, en wordt gemotiveerd waarom de gegevens noodzakelijk zijn voor het doel, bedoeld in artikel 2.10, van de wet.

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

1. Een verzoek van een deelnemer om een rapportage over vermogen en inkomsten of over financieel-zakelijke relaties, bedoeld in artikel 2.13, onder a en b, van de wet, wordt uitsluitend in behandeling genomen indien:

a. sprake is van duidelijke en objectieve aanwijzingen dat op onrechtmatige wijze financieel gewin is of wordt behaald door middel van:

1°. een misdrijf als omschreven in artikel 67, eerste lid, van het Wetboek van Strafvordering;

2°. een overtreding van een wettelijk voorschrift waarvoor naar verwachting een bestuurlijke sanctie van ten minste € 5000 kan worden opgelegd of die kan leiden tot weigering, inperking, of intrekking van een vergunning of integriteitsverklaring;

3°. een fiscale overtreding bij een vermoeden van benadeling van ten minste € 5000, of

4°. een overheidsvordering die oninbaar dreigt te worden van ten minste € 5000 vanwege een onherroepelijke boete, ontnemingsmaatregel of schadevergoedingsmaatregel;

b. de gevraagde rapportage met het oog op het doel van de Infobox Crimineel en Onverklaarbaar Vermogen, bedoeld in artikel 2.10 van de wet, noodzakelijk en evenredig is voor de uitoefening van publiekrechtelijke taken en bevoegdheden van de verzoekende deelnemer, bedoeld in artikel 2.11 van de wet of artikel 2.6 van dit besluit;

c. het verkrijgen van de gevraagde rapportage naar verwachting de samenwerking met meerdere deelnemers van de Infobox Crimineel en Onverklaarbaar Vermogen vergt; en

d. het verzoek een vermelding omvat van:

1°. de taak of bevoegdheid van de deelnemer en het betrokken element van het doel, bedoeld in artikel 2.10 van de wet, met het oog waarop het verzoek wordt gedaan;

2°. de natuurlijke of rechtspersonen waarop het verzoek ziet, of, in geval van een rapportage over vermogen en inkomsten, eventueel het object waarop het verzoek ziet, en

3°. indien het een verzoek om een rapportage over financieel-zakelijke relaties betreft, de feiten en omstandigheden die relevant zijn om te kunnen bepalen welke relaties moeten worden opgenomen in de rapportage.

2. De deelnemer die het verzoek aanmeldt, draagt er zorg voor dat daarin is toegelicht in hoeverre is voldaan aan de criteria, bedoeld in het eerste lid. De deelnemers registreren een verzoek om een rapportage in het systeem waarin zij gezamenlijk gegevens verwerken, met daarbij de vermelding of is voldaan aan de criteria voor het in behandeling nemen van dat verzoek.

Artikel 2.9 Vaststelling van thema voor een themarapportage

1. Een themarapportage, bedoeld in artikel 2.13, onder c, van de wet wordt uitsluitend verstrekt over een thema dat door de deelnemers is vastgesteld, is gepubliceerd op de website van het samenwerkingsverband en betrekking heeft 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;

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.

2. Onder raadpleging van de rechtmatigheidsadviescommissie stellen de deelnemers bij de vaststelling van het betreffende thema een toelichtende beschrijving op van:

a. de wijze waarop het thema inzicht geeft in de problematiek met betrekking tot het doel, bedoeld in artikel 2.10, van de wet, waarom dit inzicht niet voldoende kan worden bereikt zonder een themarapportage, en van de evenredigheid van een themarapportage, gelet op de geschatte ernst, stelselmatigheid, verspreiding en duur van het te onderzoeken thema;

b. de te hanteren indicatoren, verwerkingsmethode en gegevens;

c. de invulling van de waarborgen, bedoeld in de artikelen 2.11 en 2.12 van dit besluit en artikel 1.9 van de wet, en

d. de voorwaarden waaronder de resultaten worden opgenomen in de rapportage en waarbij sprake is van een verhoogd risico als bedoeld in artikel 1.9, vijfde lid, van de wet.

Artikel 2.10 Vaststelling van indicatoren voor een themarapportage

Bij het opstellen van een themarapportage, bedoeld in artikel 2.13, onder c, van de wet hanteren de deelnemers uitsluitend door hen vooraf vastgestelde indicatoren voor het betreffende thema, die:

- a. wijzen op het op onrechtmatige wijze behalen van financieel gewin;
- b. zijn gebaseerd op wetenschappelijke literatuur, statistische validatie en kennis van experts, en
- c. objectief en nauwkeurig zijn en zijn gecontroleerd op geldigheid en juistheid, rekening houdend met vertekening, navolgbaarheid, betrouwbaarheid en representativiteit van de gegevens.

Artikel 2.11 Criteria voor behandeling van een verzoek om een themarapportage

1. Een verzoek van een deelnemer of meerdere deelnemers om een themarapportage, bedoeld in artikel 2.13, onder c, van de wet, wordt uitsluitend in behandeling genomen indien het verzoek de volgende informatie bevat:

- a. de onderzoeksvraag, met een beschrijving van het vastgestelde thema, bedoeld in artikel 2.9, de beoogde onderzoeksgroep, de afbakening van de onderzoeksvraag en een toelichting waarom de informatie uit de themarapportage de onderzoeksvraag kan beantwoorden;
- b. 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;
- c. een toelichting op de noodzaak van de rapportage voor de uitoefening van publiekrechtelijke taken en bevoegdheden, bedoeld in artikel 2.11 van de wet of artikel 2.6 van dit besluit, van de verzoekende deelnemer, en
- d. een toelichting op de proportionaliteit van het verzoek, gelet op de onderzoeksvraag en de grootte van de beoogde onderzoeksgroep.

2. Indien uit de themarapportage, bedoeld in artikel 2.13, onder c, van de wet, op basis van de vooraf vastgestelde voorwaarden, bedoeld in artikel 2.9, tweede lid, onder d, van dit besluit ten aanzien van bepaalde natuurlijke personen of rechtspersonen of objecten duidelijke en objectieve aanwijzingen blijken dat sprake is van een verhoogd risico dat op onrechtmatige wijze financieel gewin is of wordt behaald, kan de ontvanger voor die personen of objecten verzoeken om een themarapportage compact, bedoeld in artikel 2.13, onder d, van de wet. Op de indiening van dit verzoek is artikel 2.8 van dit besluit van overeenkomstige toepassing, met dien verstande dat niet de natuurlijke of rechtspersonen waarop het verzoek ziet, worden vermeld, maar de betreffende subjectnummers uit de themarapportage.

3. De deelnemers registreren een verzoek om een rapportage in het systeem waarin zij gezamenlijk gegevens verwerken, met daarbij de vermelding of is voldaan aan de criteria voor het in behandeling nemen van dat verzoek.

Artikel 2.12 Uitvoering van de gegevensanalyse voor een themarapportage

1. De themarapportage (iRT NN), bedoeld in artikel 2.13, onder c, van de wet, wordt opgesteld op basis van een geautomatiseerde gegevensanalyse waarbij door de deelnemers verstrekte gegevens worden geanalyseerd aan de hand van de vooraf vastgestelde gevalideerde

indicatoren, bedoeld in artikel 2.10. Hiertoe kunnen de gegevens worden samengevoegd, opgeteld en gegroepeerd.

2. De deelnemers nemen bij de gegevensanalyse de toelichtende beschrijving, bedoeld in artikel 2.9, tweede lid, in acht.

3. De deelnemers beperken de gegevensanalyse tot het thema, de afbakening van de onderzoeksvraag en onderzoeksgroep, bedoeld in artikel 2.11, eerste lid.

4. De deelnemers treffen de volgende aanvullende waarborgen:

a. de deelnemers zorgen voor een representatieve onderzoeksgroep en hebben aandacht voor het risico van vooringenomenheid;

b. de gehanteerde methodiek is uitlegbaar, navolgbaar en controleerbaar;

c. met inachtneming van artikel 1.9, vijfde lid, van de wet worden gegevens uit de themarapportage enkel aan identificerende gegevens gekoppeld nadat een verzoek is gedaan om een themarapportage compact voor het betreffende subject, mits dat verzoek voldoet aan de voorwaarden, bedoeld in artikel 2.11, tweede lid, en

d. ten hoogste twee jaar na de verstrekking van een themarapportage kan een deelnemer naar aanleiding daarvan een verzoek doen om een themarapportage compact, bedoeld in artikel 2.13, onder d, van de wet.

5. Over de toepassing van dit artikel wordt de rechtmatigheidsadviescommissie periodiek geïnformeerd ten behoeve van de uitoefening van haar taak, bedoeld in artikel 1.8, zesde lid, van de wet.

Paragraaf 2.3 Regionale Informatie- en Expertisecentra (RIEC's)

Artikel 2.13 Territoriale werkgebieden

De Regionale Informatie- en Expertisecentra dragen er zorg voor dat hun territoriale werkgebieden worden bekendgemaakt door plaatsing op internet.

Artikel 2.14 Nadere regels over wettelijke taken en bevoegdheden van deelnemers

De Nederlandse Voedsel- en Warenautoriteit neemt in aanvulling op de wettelijke taken, genoemd in artikel 2.19, eerste lid, onder l, van de wet, tevens deel voor de uitvoering van de wettelijke taken en bevoegdheden waar haar toezicht en bestuursrechtelijke handhaving zich bij of krachtens de wet over uitstrekt, alsmede voor de opsporing van strafbare feiten krachtens artikel 142 van het Wetboek van Strafvordering voor zover buitengewoon opsporingsambtenaren van deze autoriteit hiermee belast zijn.

Artikel 2.15 Concretisering van te verstrekken gegevens

De op grond van artikel 2.22, eerste lid, van de wet te verstrekken categorieën gegevens, genoemd in de eerste kolom, hebben uitsluitend betrekking op de gegevens, genoemd in de tweede kolom, mits de gegevens met het oog op het doel van het Regionale Informatie- en Expertisecentrum toereikend, ter zake dienend en niet bovenmatig zijn.

Categorie gegevens	Nadere regels, concretisering en bronnen van de gegevens
<i>Tijdens de eerste fase van gegevensverwerking, bedoeld in artikel 2.23, zesde lid, onder a, van de wet</i>	
identificerende gegevens, contactgegevens en het burgerservicenummer	gegevens van een deelnemer met de volledige personalia, titulatuur, aliassen, adres, eerdere adressen, contactgegevens, het burgerservicenummer en het gegeven welke personen behoren tot de directe kring van betrokkene, bedoeld in artikel 2.22, eerste lid, onder b, van de wet
gegevens betreffende de verblijfsstatus	gegevens van de Immigratie- en Naturalisatiedienst over de verblijfsrechtelijke positie van een vreemdeling
gegevens omtrent de woonsituatie	gegevens van een deelnemer over of de betreffende persoon de woonruimte huurt, heeft gekocht of inwoont, de samenstelling van het huishouden, de ligging, staat en inrichting van de woonruimte, en de aard en aantallen van inschrijvingen op het adres
voertuiggegevens	gegevens van een deelnemer over kenteken, jaartal van uitgave, eigenaar, voormalige eigenaren, historie, soort voertuig, catalogus- en dagwaarde, uiterlijke kenmerken, overschrijvende instantie en gegevens over eventuele in- en uitvoer of sloop van het voertuig
financiële gegevens	gegevens van een deelnemer, niet zijnde de rijksbelastingdienst, over de financiële en eigendomspositie, waaronder gegevens over ruimtelijke ontwikkeling en vastgoed, te weten: pacht, huur, verhuur, ingebruikgeving van objecten en gronden, erfpacht, opstalrecht en erfdienstbaarheden, grondexploitatie en gegevens over aan- en verkoop en eigendom van onroerend goed
kadastrale gegevens	gegevens van een deelnemer over de datum van aankoop en de voorwaarden waaronder de koop is gesloten en gefinancierd, de notaris, personalia van verkoper of koper, verkoopbedrag, hypotheekgegevens, gegevens over de Wet waardering onroerende zaken en gegevens over het gebruik of de bestemming van een pand
bedrijfsgegevens	gegevens van de Kamer van Koophandel die bij een deelnemer bekend zijn
inkomensgegevens	gegevens van een deelnemer, niet zijnde de rijksbelastingdienst, over loon, uitkering, beleggingen, andere inkomsten, spaarsaldo, onrechtmatig verkregen inkomsten of indicaties daarvoor
gegevens betreffende zakelijke relaties	gegevens van een deelnemer over de aard van de zakelijke relaties
gegevens betreffende vergunning- of subsidieaanvragen, hierop genomen besluiten en juridische procedures	gegevens van de gemeente, provincie, het Uitvoeringsinstituut werknemersverzekeringen of de Nederlandse Voedsel- en Warenautoriteit betreffende vergunning- of subsidieaanvragen, hierop genomen besluiten en juridische procedures
gegevens inzake toezicht en handhaving alsmede getroffen bestuurlijke maatregelen	gegevens van een deelnemer over voornemens, genomen besluiten en juridische procedures in het kader van toezicht, handhaving of bestuurlijke maatregelen, mede omvattende gegevens omtrent conservatoir beslag en meldingen ten behoeve van toezicht of handhaving inzake openbare orde en veiligheid

Categorie gegevens	Nadere regels, concretisering en bronnen van de gegevens
<i>Tijdens de tweede fase van gegevensverwerking, bedoeld in artikel 2.23, zesde lid, onder b, van de wet</i>	
fiscale gegevens	gegevens van de rijksbelastingdienst of de gemeente over genomen besluiten, met inbegrip van boeten en aanslagen, juridische procedures, boekenonderzoeken, aangiften, openstaande schulden, aanslagen en betalingen en gegevens van de gemeente in het kader van de Wet waardering onroerende zaken over de gebruiker en eigenaar van een object en de waardebe-paling en -vaststelling
politiegegevens in de zin van de artikelen 8 en 13 van de Wet politiegegevens	politiegegevens in de zin van de artikelen 8 en 13 van de Wet politiegegevens
justitiële en strafvorderlijke gegevens en tenuitvoerleggingsgegevens	justitiële en strafvorderlijke gegevens en tenuitvoerleggingsge-gevens als bedoeld in artikel 1 van de Wet justitiële en strafvor-derlijke gegevens
gegevens over seksueel gedrag of seksuele gerichtheid	persoonsgegevens van een deelnemer met betrekking tot iemands seksueel gedrag wanneer de verwerking noodzakelijk is in aanvulling op de verwerking van persoonsgegevens van strafrechtelijke aard, voor onderzoeken in het kader van bestrijding van mensenhandel, illegale prostitutie en uitbuiting, met uitsluiting van persoonsgegevens met betrekking tot seksuele gerichtheid
<i>Tijdens de derde fase van gegevensverwerking, bedoeld in artikel 2.23, zesde lid, onder c, van de wet</i>	
politiegegevens in de zin van de artikelen 9 en 10, eerste lid, onderdelen a en c, van de Wet politiegegevens	politiegegevens in de zin van de artikelen 9 en 10, eerste lid, onderdelen a en c, van de Wet politiegegevens

Artikel 2.16 Criteria voor behandeling van een signaal

1. Onverminderd de criteria, bedoeld in artikel 2.23, derde lid, van de wet, kan een signaal van een deelnemer uitsluitend aanleiding vormen tot gezamenlijke gegevensverwerking in het Regionaal Informatie- en Expertisecentrum indien:

a. sprake is van duidelijke en objectieve aanwijzingen dat het signaal verband houdt met verschijningsvormen van georganiseerde criminaliteit, blikende uit feiten, omstandigheden en gedragingen die aan het signaal ten grondslag liggen, voor zover deze voortvloeien uit concrete waarne-mingen van de deelnemer tijdens de uitoefening van diens wettelijke taken en bevoegdheden;

b. het signaal gerelateerd is aan een van de volgende verschijnings-vormen van georganiseerde criminaliteit:

1°. mensenhandel en -smokkel;

2°. georganiseerde drugscriminaliteit;

3°. fraude of misbruik in de vastgoedsector;

4°. witwassen en daaraan gerelateerde vormen van financieel-ekonomische criminaliteit;

5°. misdrijven die een ernstige inbreuk op de rechtsorde opleveren als bedoeld in het Wetboek van Strafvordering, voor zover die georgani-seerde criminaliteit betreffen, of

6°. verschijningsvormen van georganiseerde criminaliteit die na toetsing van de evenredigheid zijn aangewezen door de bestuurders van de deelnemers die het samenwerkingsverband aansturen of door de Minister van Justitie en Veiligheid, en zijn bekendgemaakt door plaatsing op internet;

c. gezamenlijke gegevensverwerking noodzakelijk is in relatie tot de doelstelling van het Regionaal Informatie- en Expertisecentrum;

d. het signaal naar verwachting de gezamenlijke aanpak vergt met meerdere deelnemers van het Regionaal Informatie- en Expertisecentrum, en

e. het signaal naar verwachting betrekking heeft op de regio van het betreffende Regionaal Informatie- en Expertisecentrum.

2. De deelnemer die het signaal aanmeldt, draagt er zorg voor dat in de aanmelding wordt toegelicht in hoeverre is voldaan aan de criteria, bedoeld in het eerste lid. De deelnemers registreren in het systeem waarin zij gezamenlijk gegevens verwerken of naar hun oordeel is voldaan aan de criteria voor het in behandeling nemen van een signaal.

Paragraaf 2.4 Zorg- en Veiligheidshuizen (ZVH)

Artikel 2.17 Definitiebepaling

In deze paragraaf wordt verstaan onder:

plan van aanpak: plan dat invulling geeft aan de gezamenlijke strategie, bedoeld in artikel 2.26 van de wet, 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.

Artikel 2.18 Territoriale werkgebieden

De Zorg- en Veiligheidshuizen dragen er zorg voor dat hun territoriale werkgebieden worden bekendgemaakt door plaatsing op internet.

Artikel 2.19 Beperking gegevensverstrekking over kring van personen

Op grond van artikel 2.30, eerste lid, onder b, van de wet worden uitsluitend gegevens verstrekt over personen die een gezinslid of ander direct sociaal contact zijn van een betrokkene die is aangemeld op grond van artikel 2.31, eerste lid, van de wet.

Artikel 2.20 Criteria voor behandeling van een casus

1. Een casus die wordt aangemeld op grond van artikel 2.31, eerste lid, van de wet is in overeenstemming met het doel, bedoeld in artikel 2.25 van de wet, indien er sprake is van problemen:

a. bij betrokkene, of in de gezinssituatie waarin betrokkene verkeert indien die problemen voor betrokkene relevant zijn;

b. op meerdere leefgebieden waarin sprake is van criminogene factoren;

c. die leiden, hebben geleid, of, gelet op duidelijke en objectieve aanwijzingen daarvoor, zonder interventie zouden gaan leiden tot het veroorzaken door betrokkene van ernstige overlast, criminaliteit, of onveilige situaties voor personen of binnen een gebied, en

d. waarvoor samenwerking tussen deelnemers van het Zorg- en Veiligheidshuis uit meerdere domeinen noodzakelijk is om te komen tot een effectief plan van aanpak om deze problemen te voorkomen, verminderen of bestrijden.

2. De deelnemers aan het Zorg- en Veiligheidshuis kunnen plannen van aanpak van meerdere personen over wie in Zorg- en Veiligheidshuizen casusoverleggen worden gevoerd, op elkaar afstemmen voor zover:

a. de betrokkenen behoren tot elkaars directe kring als bedoeld in artikel 2.30, eerste lid, onder b, van de wet;

b. er afhankelijkheden bestaan tussen de problemen bij deze betrokkenen als bedoeld in het eerste lid, of tussen de problemen die zij veroorzaken als bedoeld in het eerste lid, onderdeel c, en

c. de afstemming noodzakelijk is voor het doel, bedoeld in artikel 2.25 van de wet.

3. De deelnemer die de casus aanmeldt, draagt er zorg voor dat uit de aanmelding blijkt in hoeverre is voldaan aan de criteria, bedoeld in het eerste lid. De deelnemers registreren in het systeem waarin zij gezamenlijk gegevens verwerken of naar hun oordeel is voldaan aan de criteria voor het in behandeling nemen van een casus.

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

1. De deelnemers, bedoeld in artikel 2.27, eerste lid, van de wet, kunnen op grond van artikel 2.31, negende lid, van de wet, derden op incidentele basis laten deelnemen aan het casusoverleg van een Zorg- en Veiligheidshuis indien zij over deskundigheid beschikken die noodzakelijk is bij de aanpak van een specifieke casus en zij gelet op hun onderscheidenlijke wettelijke of publieke taken en bevoegdheden een rol kunnen vervullen bij het opstellen, uitvoeren of evalueren van het plan van aanpak.

2. Een derde mag op grond van het eerste lid uitsluitend deelnemen aan een casusoverleg na ondertekening van een verklaring waarmee hij verklaart de geheimhoudingsplicht, bedoeld in artikel 1.11 van de wet, na te leven.

3. Een derde wordt niet geautoriseerd voor de toegang tot de systemen waarin de deelnemers gezamenlijk persoonsgegevens verwerken. De deelnemers, bedoeld in artikel 2.27, eerste lid, van de wet kunnen aan de derde persoonsgegevens verstrekken voor zover dat naar hun oordeel noodzakelijk is om de derde in staat te stellen om zijn rol te vervullen.

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

Plaatsing van een betrokkene op de lijst met geprioriteerde casussen, bedoeld in artikel 2.32, eerste lid, van de wet, is slechts mogelijk indien:

- a. de betrokkene voldoet aan de criteria voor behandeling in het Zorg- en Veiligheidshuis, bedoeld in artikel 2.20 van dit besluit,
- b. is voldaan aan de objectieve criteria die op grond van artikel 2.32, eerste lid, van de wet zijn geformuleerd, en
- c. deze objectieve criteria openbaar zijn gemaakt door plaatsing op het internet.

HOOFDSTUK 3. WIJZIGING VAN ANDERE BESLUITEN

Artikel 3.1 Wijziging Besluit politiegegevens

Artikel 4:3, zevende lid, van het Besluit politiegegevens vervalt.

HOOFDSTUK 4. SLOTBEPALINGEN

Artikel 4.1 Inwerkingtreding

Met ingang van 1 maart 2025 treden in werking:

- a. De wet, met uitzondering van de artikelen 1.3, vijfde lid, en 1.4, derde lid, eerste volzin, die in werking treden met ingang van 1 juli 2025;
- b. Dit besluit, met uitzondering van de artikelen 2.1, 2.2 en 2.6, die in werking treden op een bij koninklijk besluit te bepalen tijdstip;

c. De Wet van 26 juni 2024 tot wijziging van de Wet gegevensverwerking door samenwerkingsverbanden in verband met het waarborgen van de parlementaire betrokkenheid bij de aanwijzing van andere samenwerkingsverbanden (Stb. 2024, 254).

Artikel 4.2 Citeertitel

Dit besluit wordt aangehaald als: Besluit gegevensverwerking door samenwerkingsverbanden.

Lasten en bevelen dat dit besluit met de daarbij behorende nota van toelichting in het Staatsblad zal worden geplaatst.

's-Gravenhage, 29 november 2024

Willem-Alexander

De Minister van Justitie en Veiligheid,
D.M. van Weel

De Staatssecretaris van Justitie en Veiligheid,
T.H.D. Struycken

Uitgegeven de *vierde* december 2024

De Minister van Justitie en Veiligheid,
D.M. van Weel

NOTA VAN TOELICHTING

Inhoud

Algemeen	20
1. Inleiding	20
2. Uitgangspunten WGS en BGS	21
3. Ontvangen consultatieadviezen	22
4. Advies van de Autoriteit persoonsgegevens	23
5. Uitvoerbaarheid	29
6. Financiële gevolgen	29
7. Evaluatie	30
Artikelsgewijs	31
Hoofdstuk 1. Algemene bepalingen	31
Artikel 1.1 Aanwijzing contactpunt	31
Artikel 1.2 Verantwoordelijkheid voor nakoming verzoeken AVG	33
Artikel 1.3 Verantwoordelijkheid voor nakoming informatieplicht	36
Artikel 1.4 Verantwoordelijkheid voor nakoming meldplicht datalekken	39
Artikel 1.5 Rechtmatig verwerkte gegevens	40
Artikel 1.6 Kwaliteit van een aangemeld signaal, verzoek of casus	41
Artikel 1.7 Correctie van onjuistheden tijdens gezamenlijke gegevensverwerking	41
Artikel 1.8 Kwaliteit van de resultaten	42
Artikel 1.9 Nationaliteit	44
Artikel 1.10 Nadere inkadering van gegevensuitwisseling tussen samenwerkingsverbanden	45
Artikel 1.11 Betrouwbaarheid geautoriseerde personen	49
Artikel 1.12 Logging	51
Artikel 1.13 Werkwijze van de rechtmatigheidsadviescommissie	52
Artikel 1.14 Samenstelling van de rechtmatigheidsadviescommissie	57
Artikel 1.15 Rechtmatigheidsadviescommissie voor cluster van samenwerkingsverbanden	59
Artikel 1.16 Precisering maximale bewaartermijn	60
Artikel 1.17 Opleiding en training ten aanzien van gegevensverwerking	63
Artikel 1.18 Uitwerking auditbepaling	64
Hoofdstuk 2. Bepalingen inzake specifieke samenwerkingsverbanden	65
Paragraaf 2.1 Financieel Expertisecentrum (FEC)	65
Artikel 2.1 Aanvullende deelnemers Programma Terrorismefinanciering	65
Artikel 2.2 Deelnemers aan publiek-private samenwerking	66
Artikel 2.3 Beperking gegevensverstrekking over kring van personen	69
Artikel 2.4 Criteria voor behandeling van een signaal of verzoek	70
Artikel 2.5 Nadere waarborgen signalenoverleg en gegevensanalyse	73
Paragraaf 2.2 Infobox Crimineel en Onverklaarbaar Vermogen (iCOV)	73
Artikel 2.6 Aanvullende deelnemers	73
Artikel 2.7 Beperking gegevensverstrekking over kring van personen	75
Artikel 2.8 Criteria voor een rapportage over vermogen en inkomsten of financieel-zakelijke relaties	76
Artikel 2.9 Vaststelling van thema voor een themarapportage	79
Artikel 2.10 Vaststelling van indicatoren voor een themarapportage	83
Artikel 2.11 Criteria voor behandeling van een verzoek om een themarapportage	83
Artikel 2.12 Uitvoering van de gegevensanalyse voor een themarapportage	86
Paragraaf 2.3 Regionale Informatie- en Expertisecentra (RIEC's)	88
Artikel 2.13 Territoriale werkgebieden	89
Artikel 2.14 Nadere regels over wettelijke taken en bevoegdheden van deelnemers	89
Artikel 2.15 Concretisering van te verstrekken gegevens	89
Artikel 2.16 Criteria voor behandeling van een signaal	92
Paragraaf 2.4 Zorg- en Veiligheidshuizen (ZVH)	94
Artikel 2.17 Definitiebepaling	94
Artikel 2.18 Territoriale werkgebieden	94
Artikel 2.19 Beperking gegevensverstrekking over kring van personen	95
Artikel 2.20 Criteria voor behandeling van een casus	95
Artikel 2.21 Nadere criteria voor incidentele deelname aan Zorg- en Veiligheidshuis	97
Artikel 2.22 Objectieve criteria voor plaatsing op een lijst van geprioriteerde casussen	101
Hoofdstuk 3. Wijziging van andere besluiten	102
Artikel 3.1 Wijziging Besluit politiegegevens	102

Algemeen

1. Inleiding

In het onderhavige Besluit gegevensverwerking door samenwerkingsverbanden (hierna: dit besluit of BGS) wordt uitvoering gegeven aan verplichtingen uit de Wet gegevensverwerking door samenwerkingsverbanden (hierna: de wet of WGS). 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 algemene maatregel van bestuur (hierna: 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

¹ Kamerstukken II 2021/22, 35 447, 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».

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);

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).

2. Uitgangspunten WGS en BGS

Verstrekking aan het samenwerkingsverband

De deelnemers aan de samenwerkingsverbanden zijn verplicht om bij of krachtens de WGS aangewezen categorieën van gegevens aan het samenwerkingsverband te verstrekken, voor zover dat noodzakelijk is voor het doel van het samenwerkingsverband, tenzij naar het oordeel van de deelnemer zwaarwegende redenen zich daartegen verzetten. Voor de vraag of gegevens aan het samenwerkingsverband moeten worden verstrekt, is dus leidend of de gegevensverstrekking noodzakelijk is voor het doel van het samenwerkingsverband en niet het individuele doel van de deelnemer. Het voorgaande volgt uit artikel 1.5 van de wet, en voor zover het gaat om de politie, de Koninklijke marechaussee en het Openbaar Ministerie, uit artikel 20, derde lid, van de Wet politiegegevens (hierna: Wpg) en de artikelen 8b, 39fa en 51ca van de Wet justitiële en strafvorderlijke gegevens (hierna: Wjsg) (toegevoegd door de artikelen 4.1 en 4.2 van de WGS). De taak van een verstreckende deelnemer is dus niet bepalend voor gegevensverstrekking aan het samenwerkingsverband. Weliswaar dient de gegevensverwerking mede noodzakelijk te zijn voor de uitoefening van publiekrechtelijke taken en bevoegdheden *van de deelnemers*³, maar *welke* deelnemers dit zijn kan afhankelijk van de casus verschillen.

³ Zie de doelomschrijvingen van de samenwerkingsverbanden in de artikelen 2.2, 2.10, 2.17 en 2.25 WGS.

De gegevensverstrekking van een deelnemer aan het samenwerkingsverband valt overigens onder de zelfstandige verantwoordelijkheid van de betreffende deelnemer die de gegevens verstrekt.

Verwerking binnen het samenwerkingsverband

Nadat de deelnemers de gegevens aan het samenwerkingsverband hebben verstrekt, verwerkt het samenwerkingsverband de ontvangen gegevens gezamenlijk voor het doel van het samenwerkingsverband.⁴ 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). Dit betreft bijvoorbeeld een signalenoverleg of gegevensanalyse (FEC), het opstellen van een rapportage (iCOV), een casusoverleg (RIEC's en Zorg- en Veiligheidshuizen) of een gebieds- of thematische scan (RIEC's).

Verstrekking uit het samenwerkingsverband

De gezamenlijke verwerkingsverantwoordelijkheid eindigt na verstrekking van een resultaat van de gezamenlijke gegevensverwerking door het samenwerkingsverband, aan 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.

Uitgangspunt is dat resultaten van de gegevensverwerking volgens artikel 1.7 van de wet alleen verstrekt mogen worden als de taak van de ontvangende deelnemer verenigbaar is met het doel van het samenwerkingsverband. Een resultaat kan bijvoorbeeld sturingsinformatie betreffen, of interventieadviezen in de vorm van concrete producten. Dit betreft iCOV-rapportages, thematische of gebiedscans van RIEC's of gegevensanalyses van het FEC. Bij de casusoverleggen van een RIEC of Zorg- en Veiligheidshuis of een signalenoverleg van het FEC is daarentegen geen sprake van een concreet product maar van mondelinge overleggen, waarin afstemming plaatsvindt over eventuele interventies. Het resultaat heeft dan bijvoorbeeld de vorm van een plan van aanpak.

3. Ontvangen consultatieadviezen

Van medio februari tot medio april 2023 heeft de (internet)consultatie plaatsgevonden over het ontwerpbesluit. Het ontwerpbesluit is in de consultatie voorgelegd aan de Autoriteit persoonsgegevens (AP), het Financieel Expertisecentrum (FEC), de Infobox Crimineel en Onverklaarbaar Vermogen (iCOV), de stuurgroepen Regionale Informatie- en Expertisecentra (stuurgroepen RIEC's), de Zorg- en Veiligheidshuizen, het Openbaar Ministerie, de Politie, de Vereniging van Nederlandse Gemeenten (VNG), Regioburgemeesters, het Nederlands Genootschap van burgemeesters, het Adviescollege toetsing regeldruk (ATR) en de Nederlandse Vereniging van Banken.

Van deze partijen zijn adviezen ontvangen, behalve van het FEC, de Politie en het Nederlands Genootschap van burgemeesters, die hebben laten weten geen formeel advies uit te brengen. Het advies van de AP is uitgebracht op 3 november 2023 (zie paragraaf 4 hierna). Het ATR heeft

⁴ Zoals is beschreven in de memorie van toelichting op de WGS, moet dit worden beschouwd als een taak van algemeen belang als bedoeld in 6, eerste lid, onder e, van de AVG (Kamerstukken II 2019/20, 35 447, nr. 3, blz. 8).

laten weten het dossier niet te selecteren voor een formeel advies, omdat het naar verwachting geen (nieuwe) gevolgen voor de regeldruk heeft.

Via de internetconsultatie zijn reacties ontvangen van particulieren, Aedes, Amnesty International, gemeente Rotterdam, KNMG, Nederlandse GGZ, Platform Burgerrechten, Public Action B.V., Reclassering Nederland, en Zorg- en Veiligheidshuis Rotterdam Rijnmond.

De adviezen hebben geleid tot wetstechnische en enige inhoudelijke aanpassingen van het ontwerpbesluit. Een inhoudelijke aanpassing is dat aan artikel 1.2 is toegevoegd dat een AVG-verzoek van een betrokkene kan worden afgedaan door een andere deelnemer dan het contactpunt, indien die daartoe beter in staat is, mits dat wordt gecommuniceerd aan betrokkene.

In het artikelsgewijze deel is op diverse plaatsen nader toegelicht hoe de adviezen bij de keuzes inzake de voorliggende amvb een rol hebben gespeeld. Daartoe is de artikelsgewijze toelichting aangevuld bij diverse artikelen. Dit is steeds aangeduid met het trefwoord «consultatie»

Voor de goede orde zij vermeld dat opmerkingen die de kaders van de voorliggende amvb te buiten gaan, buiten beschouwing zijn gelaten. Beperkte en technische aanpassingen naar aanleiding van de consultatie zijn doorgevoerd maar worden niet allemaal in de toelichting besproken. Het expliciet ingaan op alle opmerkingen zou de toelichting dermate omvangrijk en onoverzichtelijk maken dat deze niet meer hanteerbaar zou zijn.

4. Advies van de Autoriteit persoonsgegevens

De AP ziet veel betekenisvolle verbeteringen waardoor er gaandeweg een veel beter doordacht geheel is ontstaan. Toetsbaarheid en transparantie zijn materieel in orde gebracht. Veel zal volgens de AP echter afhangen van de striktheid waarmee de criteria voor het mogen inschakelen van het samenwerkingsverband zullen worden bewaakt. Om te komen tot rechtmatige gegevensdeling adviseert de AP om een preventieve rechterlijke toets van de voorgenomen gegevensverwerkingen op te nemen in de WGS. Dit kan volgens de AP geschieden via het op 13 november 2023 ingediende wetsvoorstel tot wijziging van de WGS.⁵ In afwachting daarvan zou de Eerste Kamer de WGS nog niet moeten aannemen, aldus de AP. Verder kan volgens de AP bij die gelegenheid ook de delegatiesystematiek van de WGS worden gewijzigd (facultatieve delegatiegrondslagen vervangen door imperatieve grondslagen).

Over het BGS heeft de AP drie opmerkingen, voornamelijk van wetstechnische aard. De laatstbedoelde drie opmerkingen van de AP zijn overgenomen.

Vanwege de hierna volgende overwegingen bestaat er geen voornemen om een voorstel tot wijziging van de WGS bij de Tweede Kamer in te dienen of om het voornoemde wetsvoorstel tot wijziging van de WGS aan te passen.

Rechterlijke toets van gegevensverwerkingen

De AP adviseert om voor iedere voorgenomen verwerking van persoonsgegevens binnen een samenwerkingsverband een onafhankelijke rechterlijke toetsing in te voeren in de WGS, omdat dit volgens de AP

⁵ Het bij koninklijke boodschap van 13 november 2023 ingediende voorstel van wet tot wijziging van de Wet gegevensverwerking door samenwerkingsverbanden in verband met het waarborgen van de parlementaire betrokkenheid bij de aanwijzing van andere samenwerkingsverbanden (Kamerstukken 36 461). Dit wetsvoorstel is inmiddels tot wet verheven (Wet van 26 juni 2024, Stb. 2024, 254).

een noodzakelijke en gebruikelijke waarborg is om toetsing op de noodzaak van de verwerking voor elke deelnemer te garanderen en een disbalans in de bescherming van de burger te voorkomen. De AP vindt dat een burgemeester of officier van justitie bij iedere voorgenomen gegevensverwerking aan een rechter-commissaris moet verzoeken om bindend te toetsen of de voorgenomen gegevensverwerking voldoet aan de wettelijke criteria, met welke deelnemers er informatie moet worden gedeeld en welke informatie. De kern van de argumentatie van de AP is tweeledig:

1. De AP is bezorgd dat er onvoldoende op wordt toegezien dat er niet te veel gegevensdeling plaatsvindt. De deelnemers aan een samenwerkingsverband hebben geen belang bij het blokkeren van door één of meer deelnemers nuttig geachte gegevensverwerkingen. De rechtmatigheidscommissie brengt geen onafhankelijk voorafgaand oordeel over de beoogde verwerking en de inmenging in grondrechten.

2. De impact van de gegevensverwerking op betrokkenen (die nog geen verdachten zijn) zonder hun medeweten is minimaal vergelijkbaar met de impact van de inzet van zware opsporingsmiddelen, zoals de huiszoeking en de telefoontap.

Zoals de AP terecht opmerkt, moet worden voorkomen dat er ongecontroleerde en overmatige gegevensdeling plaatsvindt. Een belangrijke waarborg daartegen bestaat evenwel al met de Algemene verordening gegevensbescherming. Ingevolge de beginselen daarvan moet elke verwerking van persoonsgegevens immers gebonden zijn aan specifieke doelen en moet worden voldaan aan de eis van dataminimalisatie. De verwerkingsverantwoordelijke moet kunnen aantonen dat daarvan sprake is. In aanvulling hierop wordt met de WGS en het BGS voorzien in verdere voorwaarden en waarborgen voor een rechtmatige gegevensverwerking in de betreffende samenwerkingsverbanden. Uit de Algemene verordening gegevensbescherming of ander hoger recht volgt niet dat voor de samenwerkingsverbanden een voorafgaande rechterlijke toets vereist is. De toevoeging aan deze waarborgen van een preventieve rechterlijke toets zou voorts (a.) nauwelijks werkbaar zijn, (b.) niet in het systeem voor de bescherming van persoonsgegevens passen en (c.) een breuk vormen met het stelsel uit het Wetboek van Strafvordering.

Hierna wordt een en ander puntsgewijs toegelicht.

Werkbaarheid

Een vereiste dat inhoudt dat de rechter-commissaris vooraf toestemming moet geven voor elke gegevensverwerking in een samenwerkingsverband, laat zich in de praktijk nauwelijks realiseren en zou met zich brengen dat de rechter intensief wordt betrokken bij een bestuurlijke afweging. En zoals hierna nader zal worden toegelicht, hoort deze afweging in het systeem voor de bescherming van persoonsgegevens te worden gemaakt door de (bevoegde en op hun handelen aan te spreken) deelnemers aan het samenwerkingsverband.⁶ De deelnemers zijn bij uitstek op de hoogte van de elementen die op hun specifieke werkerreinen afgewogen moeten worden. Het werkveld van de rechter-commissaris verhoudt zich hier bezwaarlijk toe. Dat is vooral gericht op de opsporing en vervolging van strafbare feiten; zijn kennis en kunde bevindt zich diensgevolge op het domein van strafrecht en strafvordering en niet op het meer bestuursrechtelijk georiënteerde terrein van het gegevensbeschermingsrecht en de sectorale regelgeving die op de deelnemers van toepassing is.

⁶ Zie in soortgelijke zin het advies van de Afdeling advisering van de Raad van State over de aanvankelijke bepaling volgens welke de AP voorafgaande toestemming zou moeten geven voor geautomatiseerde gegevensanalyse: Kamerstukken II 2019/20, 35 447, nr. 4, blz. 19.

Dit klemmt temeer daar het verlenen van toestemming voor iedere voorgenomen gegevensverwerking een enorm beslag zal leggen op de personele capaciteit van de rechterlijke macht, waarbij het daarenboven gaat om materie die vreemd is aan de gebruikelijke taken van de rechter-commissaris. Dat capaciteitsbeslag zou ook gelden voor de officieren van justitie onderscheidenlijk de burgemeesters, omdat zij in het voorstel van de AP degenen zijn die voor de gegevensverwerkingen om toestemming zouden moeten vragen van de rechter-commissaris.

ICOV telt nu circa 16.000 bevragingen per jaar, de RIEC's werken aan circa 1300 casus per jaar en bij het FEC vinden circa 80 verwerkingen per jaar plaats. Naast de omvangrijke lasten die een dergelijke nieuwe taak voor de toch al zwaar belaste kabinetten van rechters-commissarissen en voor de officieren van justitie en burgemeesters met zich zou brengen, zou deze ook ernstig afbreuk doen aan de beoogde verbetering van de slagkracht van de samenwerkingsverbanden. Daarmee zou het doel van dit wetgevingstraject, te weten de verbetering van de gegevensdeling voor het doel van de betrokken samenwerkingsverbanden, niet worden gerealiseerd.

Voorname bezwaren zouden ook opgaan indien niet de rechter-commissaris maar een andere rechter de preventieve toets op alle gegevensverwerkingen doet: ook dat zou voorbijgaan aan de benodigde specialistische kennis en expertise inzake de werking van de samenwerkingsverbanden en de specifiek toepasselijke regelgeving, het enorme beslag op de capaciteit van rechters, officieren van justitie en burgemeesters, en de nadelige gevolgen voor de slagkracht.

Systeem gegevensbeschermingsrecht

Een preventieve rechterlijke toets – ongeacht welke rechter het betreft – past om diverse redenen ook niet in het Unierechtelijke systeem voor de bescherming van persoonsgegevens:

- Een voorafgaande rechterlijke toets staat haaks op de rolverdeling uit de AVG. Die rolverdeling is dat *de verwerkingsverantwoordelijken* – in dit geval de deelnemers aan het samenwerkingsverband – verantwoordelijk zijn voor de naleving van de regels van het gegevensbeschermingsrecht. De deelnemers dragen de gezamenlijke verwerkingsverantwoordelijkheid in de zin van artikel 26 van de AVG voor de gezamenlijke gegevensverwerking in het samenwerkingsverband, zoals toegelicht in het nader rapport inzake de WGS en de toelichting op artikel 1.4 WGS.⁷ Zij hebben een eigen verantwoordingsplicht op grond van de AVG (artikel 5, tweede lid, AVG). Bij niet-naleving dragen zij – en niet de rechter – de verantwoordelijkheid en kan de AP bestuursrechtelijke sancties opleggen.⁸ De AVG gaat dus uit van het nemen van verantwoordelijkheid, met achteraf de mogelijkheid van toetsing door de AP dan wel de rechter.

- Met de voorgestelde toets door de rechter-commissaris zou de regelgeving ter bescherming van persoonsgegevens, die voor de overheid meer bestuursrechtelijk georiënteerd is, in een strafrechtelijke context worden geplaatst. Dit leidt echter tot complicaties, zoals ook blijkt uit de door de AP voorgestane rol van de burgemeester en de officier van justitie. De verantwoordelijkheid van deze gezagsdragers voor respectievelijk de handhaving van de openbare orde⁹ en de strafrechtelijke handhaving van de rechtsorde¹⁰ zijn niet verenigbaar met de bestaande verantwoordelijkheden voor het functioneren van de instanties die

⁷ Kamerstukken II 2019/20, 35 447, nr. 4, blz. 17 en Kamerstukken II 2019/20, 35 447, nr. 3, blz. 66–67.

⁸ Zie nader antwoord 46 van de memorie van antwoord, Kamerstukken I 2022/23, 35 447, K.

⁹ Artikel 172, eerste lid, Gemeentewet.

¹⁰ Artikel 124 Wet op de rechterlijke organisatie.

deelnemen aan een samenwerkingsverband. Daarmee worden de verantwoordelijkheden juist diffuser. Dat de burgemeester of de officier van justitie aan de rechter om toestemming zou moeten vragen voor een gegevensverwerking, verdraagt zich bovendien niet goed met het feit dat ook de andere deelnemers het initiatief kunnen nemen voor een gegevensverwerking. Dat hiermee het toezicht op de verwerking van persoonsgegevens over meerdere partijen en fases (vooraf en achteraf) wordt verdeeld zal leiden tot overlap en daarmee tot onduidelijkheid.

– Een toets door de rechter-commissaris zou tot rechtsonzekerheid kunnen leiden over het toepasselijke gegevensbeschermingsrecht. Als een rechter-commissaris toestemming geeft op verzoek van een officier van justitie, wekt dat de indruk dat het gaat om de opsporing en vervolging van strafbare feiten en dat op de voorgenomen gegevensverwerking dus niet de AVG, maar de richtlijn gegevensbescherming opsporing en vervolging toepasselijk is,¹¹ die in Nederland is geïmplementeerd in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens. Vermenging van stelsels ware te voorkomen. Dat is niet alleen van belang voor de deelnemers aan de samenwerkingsverbanden, die dan zouden worden geconfronteerd met verschillende privacyregimes, maar ook voor de betrokkenen, voor wie duidelijk moet zijn wat hun rechten zijn. Beoogd is dat alleen de AVG van toepassing is op de samenwerkingsverbanden.

Stelsel Wetboek van Strafvordering

Een voorafgaande toets door de rechter-commissaris zou ook een breuk vormen met het stelsel uit het Wetboek van Strafvordering. De rechter-commissaris houdt toezicht op de voortgang en rechtmatigheid van het opsporingsonderzoek, dat onder leiding staat van de officier van justitie, en kan toestemming geven om bepaalde opsporingsmethoden in te zetten die een ernstige inbreuk op de persoonlijke levenssfeer met zich meebrengen. Bij de gegevensverwerking door de samenwerkingsverbanden is echter meestal (nog) geen sprake van een opsporingsonderzoek; het doel is immers te beoordelen welke aanpak in de voorliggende situatie het beste is. Die aanpak zal doorgaans niet strafrechtelijk zijn, maar zal dan bijvoorbeeld een bestuursrechtelijke of een sociale interventie inhouden. De WGS gaat immers over een multidisciplinaire aanpak. De opmerking van de AP, dat alle samenwerkingsverbanden in de kern in het teken staan van strafrechtelijke handhaving en handhaving van de openbare orde, laat zich dan minder goed plaatsen.

De impact van gegevensverwerkingen op grond van de WGS rechtvaardigt evenmin dat de toets van de rechter-commissaris uit het Wetboek van Strafvordering wordt overgenomen. De impact van de WGS is bezwaarlijk te vergelijken met de impact van zware opsporingsmiddelen zoals het doorzoeken van woningen, het zetten van telefoontaps en het vorderen van telecomdata. De rechter-commissaris geeft dan toestemming voor de verkrijging van nieuwe informatie met behulp van bepaalde ingrijpende opsporingsbevoegdheden en niet voor het verder verwerken van informatie waarover men al rechtmatig beschikt, zoals in de WGS. Overigens is de strafvorderlijke bevoegdheid tot het vorderen van gegevens bij derden in beginsel toebedeeld aan de officier van justitie; de rechter-commissaris is daarbij niet betrokken (artikelen 126nd/126ud Sv). Het komt vreemd voor wanneer de officier van justitie

¹¹ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PbEU 2016, L 119).

toestemming nodig heeft van de rechter-commissaris voor de verdere verwerking van gegevens tot de verkrijging waarvan hij zelfstandig bevoegd is.

Dat betrokkenen volgens de AP onder de WGS vaak niet weten dat gegevens over hen worden verwerkt en dat ook niet hoeven te verwachten, behoeft nuancering: de WGS laat de informatieplicht uit de AVG onverlet. Het hangt van het geval af of er een uitzonderingsgrond uit de AVG van toepassing is.¹² Dat er uitzonderingen op de informatieplicht mogelijk zijn, wil nog niet zeggen dat de impact te vergelijken is met die van zware opsporingsmiddelen. De impact verschilt per samenwerkingsverband en per soort gegevensverwerking. In een Zorg- en Veiligheidshuis worden zorg en sociale voorzieningen ingezet om recidive te voorkomen, in aanvulling op reeds lopende straf- en bestuursrechtelijke maatregelen of om de inzet van deze maatregelen zo mogelijk te voorkomen. Bij een iCOV-themaraapportage kan de impact groter zijn; daarom regelt dit besluit daarvoor diverse voorwaarden en waarborgen. De WGS biedt in ieder geval geen basis voor het vergaren van nieuwe informatie; de deelnemers aan een samenwerkingsverband mogen alleen gegevens uitwisselen waarover zij al rechtmatig beschikken. De impact is bovendien in zoverre beperkt dat de WGS geen *andere* bevoegdheden regelt dan inzake gegevensverwerking.

Andere waarborgen

De AP wijst er terecht op dat het van belang is dat gegevensdeling binnen de perken blijft, gelet op het uitgangspunt van dataminimalisatie dat aan de AVG ten grondslag ligt. Om de risico's te minimaliseren, bevatten de WGS en het BGS echter talrijke waarborgen en vormen van toezicht en verantwoording in aanvulling op de AVG. Met de getroffen waarborgen kan worden volstaan. Naast de rechtmatigheidsadviescommissies gaat het dan om de onafhankelijke coördinerend functionaris voor de gegevensbescherming (FG) voor het samenwerkingsverband (artikel 1.4, tweede lid, WGS). Deze houdt samen met de FG's van de deelnemers toezicht op de gegevensverwerking. Dit kunnen zij intensiveren afhankelijk van onder meer de risico's en de aard en omvang van de verwerking (artikel 39, tweede lid, AVG). Verder zijn onafhankelijke, periodieke privacy audits verplicht, waarvan de resultaten aan de AP moeten worden gezonden (artikel 1.10 WGS). Ook de AP houdt toezicht en kan handhaven, evenals de rechter die de rechtmatigheid kan toetsen. De deelnemers aan de samenwerkingsverbanden hebben dan ook evident een belang bij het tegengaan van onrechtmatige gegevensverwerkingen. Een voorafgaande rechterlijke toets ligt, alles overziend, niet in de rede.

Delegatiesystematiek

Vanuit een oogpunt van wetgevingsarchitectuur en democratische legitimatie vindt de AP dat wezenlijke bepalingen uit het concept-BGS in de WGS zouden kunnen worden opgenomen en/of dat de betreffende delegatiegrondslagen zoveel mogelijk imperatief zouden kunnen worden geformuleerd. De AP zou het vanuit rechtsstatelijk en democratisch oogpunt bijvoorbeeld ook moeilijk voorstelbaar vinden indien het Wetboek van strafvordering (de formele wet) aan opsporingsambtenaren een algemeen geformuleerde aanhoudingsbevoegdheid verleent, met daarbij de bepaling dat bij amvb voorwaarden en beperkingen kunnen worden gesteld.

¹² Een uitzondering op de verplichting om een betrokkene te informeren geldt onder meer bij doorkruising van opsporings- en toezichtbelangen. Vervalt die uitzondering, dan moet een betrokkene in principe alsnog worden geïnformeerd (zie ook de toelichting op artikel 1.3, derde lid, BGS).

Het belangrijkste aspect hierbij is welke rechtsbescherming het samenstel van wet en amvb onder de streep bieden. Daarover kan worden vastgesteld dat de delegatiegrondslagen uit de WGS in zeer uitgebreide mate worden ingevuld met het onderhavige besluit, en dat elke gegevensverwerking moet voldoen aan het gegevensbeschermingsrecht. Zoals de AP erkent, staat hoger recht deze vorm van delegatie toe.

Hoe de verdeling over de wet en amvb is, hangt ervan af welke elementen volgens de wetgever zo gewichtig zijn dat de volksvertegenwoordiging rechtstreeks bij de vaststelling moet worden betrokken. De hoofdelementen van een regeling moeten in de wet worden opgenomen. De hoofdelementen van de vier (clusters van) samenwerkingsverbanden zijn in voldoende mate opgenomen in de WGS. Dit heeft de Afdeling advisering van de Raad van State ook bevestigd in haar voorlichting.¹³ Voor een nadere toelichting op de redenen voor de delegatiesystematiek wordt verwezen naar de memorie van antwoord.¹⁴

De bevoegdheden onder de WGS zijn in zoverre anders dan onder het Wetboek van Strafvordering dat de WGS geen bevoegdheden creëert om interventies te plegen, en vanwege de hierboven genoemde redenen inzake de impact van de gegevensverwerking. Alleen gegevensverwerking wordt geregeld. De gezamenlijke gegevensverwerking op grond van de WGS staat ten dienste aan de uitoefening van bestaande wettelijke taken en bevoegdheden van de deelnemers.

Evaluatie

De evaluatie ingevolge artikel 5.1 van de WGS zal zich volgens de AP ook moeten richten op de vraag of de samenwerkingsverbanden onverminderd noodzakelijk zijn en of de bescherming van persoonsgegevens uiteindelijk op een voldoende niveau in de uitvoering voldoende gestalte krijgt. De AP stelt dat de noodzaak in de toekomst een punt van aandacht blijft, omdat er voor het aanpakken van min of meer dezelfde problematiek (witwassen, ondermijning) vaak ook andere, eveneens ingrijpende wettelijke mogelijkheden zijn, zodat stelsels kunnen gaan doubleren. Er moet dan een keuze worden gemaakt, op straffe van verval van rechtmatigheid van een stelsel.

Volgens artikel 5.1 van de WGS richt de evaluatie zich op de doeltreffendheid en effecten van deze wet in de praktijk. Formeel gezien is het niet een doel van de WGS om deze samenwerkingsverbanden op te richten, aangezien ze al geruime tijd bestaan. Toch ligt het in de rede om ook de doeltreffendheid en effecten van de samenwerkingsverbanden te betrekken in de wetsevaluatie, voor zover deze verband houden met de doeltreffendheid en effecten van de WGS.

Wat betreft de noodzaak van samenwerkingsverbanden in relatie tot doublures, bestaat er enige overlap tussen de samenwerkingsverbanden FEC, iCOV en de RIEC's, maar dat laat onverlet dat de betreffende samenwerkingsverbanden meerwaarde hebben. Dit is toegelicht in de Kamerbrief van de Minister van Justitie en Veiligheid van 17 december 2021.¹⁵ In die brief is ook beschreven dat de WGS niet overlapt met de wetgeving over witwassen.¹⁶

De vraag of de bescherming van persoonsgegevens in de uitvoering op een voldoende niveau voldoende gestalte krijgt, zal onderdeel zijn van de wetsevaluatie. De WGS is er immers bij uitstek op gericht om gegevens-

¹³ Kamerstukken II 2021/22, 35 447, H, blz. 9.

¹⁴ Kamerstukken II 2021/22, 35 447, K, antwoord 32.

¹⁵ Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 13.

¹⁶ Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 12.

verwerkingen – in dit geval door samenwerkingsverbanden – in goede en rechtmatige banen te leiden. De wetsevaluatie zal daarom ook betrekking hebben op de doeltreffendheid en effecten van de waarborgen die de WGS en het BGS bevatten om de bescherming van persoonsgegevens te versterken. De onafhankelijke privacy audits kunnen voor de wetsevaluatie worden gebruikt als input.

5. Uitvoerbaarheid

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, is mede aan bod gekomen in de uitvoerings-toetsen die zijn uitgevoerd ten tijde van de consultatie inzake deze amvb. Bedacht moet allereerst 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 en de Baseline Informatiebeveiliging Overheid (BIO) moeten toepassen en dat de in de WGS opgenomen samenwerkingsverbanden bestendig zijn en kunnen bogen op ruime ervaring en expertise.

De Belastingdienst/Dienst Toeslagen oordeelt dat het besluit uitvoerbaar is. Er zal moeten worden voorzien in eenmalige aanscherping/actualisering van procedures en werkprocessen en in extra inzet van capaciteit ten opzichte van de huidige inzet in deelname aan rechtmatighedsadviescommissies, toezichtactiviteiten en ten aanzien van de gezamenlijke verwerking binnen de samenwerkingsverbanden inclusief (begeleiding van externe) audits.

Ook het Openbaar Ministerie verwacht dat dit besluit uitvoerbaar is, mits daartoe de nodige voorbereidingen worden getroffen om de organisatie hiervoor gereed te maken. Daartoe zullen, naar de inschatting van het OM, werkinstructies en (model)documenten moeten worden aangepast. Daarnaast verwacht het OM productaanpassingen te zullen realiseren om waarborgen in te richten, onder meer op het punt van de kwaliteit van de geautomatiseerde gegevensanalyse. Voorts kan extra personele inzet nodig zijn op het gebied van toezicht en verantwoording.

De politie heeft ervan afgezien een inhoudelijke reactie in te dienen en heeft aangegeven het besluit uitvoerbaar te achten.

6. Financiële gevolgen

De Belastingdienst/Toeslagen verwacht een incidentele uitgave van € 390.000 voor automatisering en een structurele uitgave van € 540.000 voor personeel. Het UWV (dat eigener beweging een uitvoeringstoets heeft gedaan) oordeelt dat het besluit uitvoerbaar is en dat dat eenmalig 41.000 euro kost. De voornoemde kosten zullen door respectievelijk de ministeries van Financiën en SZW gedekt worden. De politie heeft geen wens tot het doen van een claim. Het OM voorziet incidentele kosten in 2025 van 2,7 miljoen en structurele kosten in 2026 en verder van 2,0 miljoen. Het OM heeft laten weten deze kosten vanaf 2025 zelf te kunnen dragen door reeds toegekende middelen voor de versterking van opsporing in het kader van ondermijning daarvoor te gebruiken. Dat betekent dat er dekking is voor de incidentele kosten in 2025 van 2,7 miljoen en de structurele kosten in 2026 e.v. van 2,0 miljoen. Daarnaast verwacht het OM incidentele kosten van 2,4 miljoen in 2024. De dekking daarvan zal komen van het ministerie van Justitie en Veiligheid, waaronder het OM ressorteert, dat hiervoor een incidentele bijdrage van 2,4 miljoen zal leveren. Deze bijdrage is afkomstig uit de beleidsbudgetten van de Directie Rechtsbestel van het Directoraat-Generaal Rechtspleging en Rechtshandhaving. Hiervoor is ruimte in het bestedingsplan van de

Directie Rechtsbestel opgenomen; deze gelden zullen per Voorjaarsnota 2024 incidenteel naar het OM worden overgeheveld. De RIEC's hebben in de consultatiereactie gewezen op de extra financiële lasten die voortvloeien uit de wet en dit besluit, bijvoorbeeld in verband met het contactpunt, de rechtmatigheidsadviescommissie, opleidingen en diverse administratieve verplichtingen. In de artikelsgewijze toelichting (in het bijzonder bij de artikelen 1.13, 2.15 en 2.16) wordt op de zorgen van de RIEC's nader ingegaan. Zoals daaruit volgt wordt geen significante kostentoeename voorzien. In aanvulling hierop merk ik op dat de financiële gevolgen beperkt kunnen blijven door de rechtmatigheidsadviescommissie zoveel mogelijk samen te stellen uit reeds bij de deelnemende organisaties werkzame personen met deskundigheid en ervaring op het gebied van de toepasselijke wetgeving inzake gegevensverwerking en de werking van het samenwerkingsverband (artikel 1.14, eerste lid). Daarnaast heeft de VNG gewezen op de impact op de gemeenten die de extra waarborgen (onder andere logging, autorisatie, inrichten van de vertrouwenspersoon¹⁷, rechtmatigheidscommissie en contactpunt) zullen hebben. Ten aanzien van logging en autorisatie geldt dat de samenwerkingsverbanden deze reeds moeten toepassen conform de AVG of de BIO. Wat betreft de instelling van het contactpunt, geldt dat aan artikel 1.2 een vierde lid is toegevoegd, mede om een significante toename van administratieve lasten te voorkomen. Op de (beperkingen op de) rol van het contactpunt wordt ingegaan in de toelichting bij artikel 1.2, eerste en vierde lid en 1.3, eerste lid. De (exacte) omvang van deze voornoemde lasten die zowel de RIEC's als de VNG verwachten, is door hen niet toegelicht.

7. Evaluatie

De wet bevat in artikel 5.1 een evaluatiebepaling die ertoe verplicht binnen vijf jaar na de inwerkingtreding daarvan verslag te doen over de doeltreffendheid en effecten van deze wet. Hierbij zal onder meer worden beoordeeld in hoeverre de knelpunten die de WGS beoogt op te lossen, daadwerkelijk zijn opgelost en in hoeverre de waarborgen ter versterking van de bescherming van persoonsgegevens doeltreffend en effectief zijn gebleken.¹⁸ Daaraan zal de nadere invulling bij het onderhavige besluit van de bepalingen uit de wet onlosmakelijk zijn verbonden. De evaluatie zal daarmee mede inzicht moeten bieden in niet alleen de vraag in hoeverre de bepalingen in het besluit uitvoerbaar en handhaafbaar zijn voor de deelnemers, maar ook of deze voor betrokkenen voldoende begrijpelijk en effectief zijn.

In de evaluatie zal ook de vraag worden meegenomen of het nodig is om regels te herschikken tussen de wet en het besluit, aangezien de evaluatie mede gaat over de vraag of de artikelen in de wet en het besluit voldoende begrijpelijk zijn. Hierop is nader ingegaan in §4b van het nader rapport op het advies van de Afdeling advisering van de Raad van State inzake dit besluit.

¹⁷ Bedoeld zal zijn de verplichting dat één van de functionarissen voor gegevensbescherming van de deelnemende overheidsinstanties optreedt als coördinerend functionaris voor gegevensbescherming voor het samenwerkingsverband (artikel 1.4, tweede lid, WGS). Zoals toegelicht in antwoord 44 van de memorie van antwoord, kan dit bijdragen aan de coördinatie van het toezicht door voornoemde functionarissen.

¹⁸ Aldus ook de nota naar aanleiding van het verslag, antwoord 20 (Kamerstukken II 35 447, 2020/21, nr. 6).

8. Voorhang Eerste en Tweede Kamer

Bij brieven van 4 april 2024 is het ontwerpbesluit toegezonden aan de Eerste en Tweede Kamer (Kamerstukken II 2023/24, 35 447, nr. 28). Beide Kamers hebben niet van de mogelijkheid gebruik gemaakt zich uit te spreken over het ontwerpbesluit. De vaste commissie voor Justitie en Veiligheid van de Eerste Kamer heeft in haar vergaderingen van 9 en 23 april en 14 en 21 mei 2024 geen vragen gesteld over het ontwerpbesluit. De vaste commissie voor Justitie en Veiligheid van de Tweede Kamer heeft in haar procedurevergadering van 24 april 2024 het ontwerpbesluit voor kennisgeving aangenomen.

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, van de wet. Dit verplicht ertoe om bij amvb regels te stellen over de aanwijzing van een deelnemende overheidsinstantie als contactpunt 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, van de wet 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), tenzij wordt overeengekomen dat een andere deelnemende overheidsinstantie besluit op een verzoek indien die daartoe beter in staat is;
- 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 afhan-

deling 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.

In de consultatie hebben de RIEC's opgemerkt dat het onduidelijk is of de bepalingen over het contactpunt juridisch voldoende zijn voor alle in dit kader benodigde juridische bevoegdheden of dat er nog aanvullende mandaatregelingen, machtigingen of AVG-verwerkersovereenkomsten tussen de partners vereist zijn. De VNG heeft in haar consultatiereactie bepleit om in te gaan op mandaatregelingen. In reactie hierop wordt benadrukt dat met de artikelen 1.1 tot en met 1.4 uitdrukkelijk wordt beoogd te voorkomen dat dergelijke regelingen nodig zijn voor de afhandeling van AVG-verzoeken van betrokkenen, de informatieplicht en de meldplicht datalekken.

Het Openbaar Ministerie heeft de suggestie gedaan om een contactpunt ook aan te wijzen voor de uitvoering van bepaalde *andere* verplichtingen van het samenwerkingsverband, zoals dat al is gedaan voor de onder artikel 1.2 tot en met 1.4 BGS genoemde verplichtingen. Een andere optie is – volgens het OM – om per verplichting een verantwoordelijke deelnemer aan te wijzen. Deze suggestie is niet overgenomen, omdat het wenselijk is ruimte te laten voor de samenwerkingsverbanden om dit onderling te regelen. De wet en dit besluit leggen de hoofdlijnen vast. Gelet op de gezamenlijke verwerkingsverantwoordelijkheid (artikel 1.4 WGS) is het uitgangspunt dat de gezamenlijke deelnemers zorgdragen voor de nakoming van hun verplichtingen op grond van de WGS en BGS. Op welke wijze dat wordt gerealiseerd hoeft niet volledig te worden uitgewerkt. Anders dreigt overregulering, temeer omdat diverse plichten voortvloeien uit de AVG en er nu al afspraken bestaan over de wijze van uitvoering.

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 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.¹⁹

Voor de Zorg- en Veiligheidshuizen moeten de gezamenlijke verwerkingsverantwoordelijken – dat wil zeggen de deelnemende overheidsinstanties, bedoeld in artikel 2.27, eerste lid, van de wet – 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 wet, 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 als uitgangspunt 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

¹⁹ 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.

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, is in principe degene die namens de deelnemers van het samenwerkingsverband de besluiten neemt 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 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.

In de consultatie hebben de RIEC's gevraagd of het contactpunt bij een inzageverzoek alle beschikbare informatie moet verzamelen van alle betrokken partners of dat het alleen gaat om de informatie die de RIEC's in dit kader hebben opgeslagen in hun systeem. Hierop wordt geantwoord dat het uitsluitend om dat laatste gaat. Het eerste artikellid bakent de taak van het contactpunt immers expliciet af tot persoonsgegevens die *door het samenwerkingsverband* worden verwerkt.

In de consultatie hebben de gemeente Rotterdam en Zorg- en Veiligheidshuis Rotterdam Rijnmond bepleit te voorzien in een klachtenregeling. In reactie hierop wordt opgemerkt dat burgers het recht hebben bij bestuursorganen te klagen over de wijze waarop zij zich in een concrete

situatie hebben gedragen (artikel 9:1 Awb). Ook kunnen zij bij het contactpunt hun AVG-rechten uitoefenen en daarna in bezwaar en beroep; een klacht is dan niet aan de orde (artikel 9:8 Awb).

Tweede lid

Uit dit lid 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. Naar aanleiding van de consultatiereactie van onder meer het Openbaar Ministerie is deze verplichting tot overleg, voorafgaand aan het nemen van een besluit, meer expliciet in dit artikellid omschreven. De deelnemers die betrokken waren of zijn bij de verwerking van de persoonsgegevens 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 zij de benodigde motivering verstrekken 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.

Op grond van dit artikellid wijst het contactpunt het verzoek af indien of voor zover naar het oordeel van één of meer van de deelnemers die betrokken waren of zijn bij de verwerking van de persoonsgegevens over de betrokkene, een uitzonderingsgrond van toepassing is.

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 (op het recht op gegevenswissing), die niet zien op de zwaarwegende belangen van deelnemers. Daarom is het «vetorecht» uit dit lid daarop niet van toepassing. Het contactpunt kan dan volstaan met overleg.

Derde lid

Het is mogelijk dat de uitzonderingsgrond na verloop van tijd vervalst, 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.

Vierde lid

Dit artikellid bepaalt dat het contactpunt met een andere deelnemende overheidsinstantie kan afspreken dat laatstgenoemde het verzoek afhandelt, indien die daartoe naar hun beider oordeel beter in staat is. In dat geval stuurt het contactpunt het verzoek door aan die overheidsinstantie, die het verzoek daarna afhandelt (tot en met eventueel bezwaar/beroep). Om te voorkomen dat voor de betrokkene onduidelijkheid ontstaat, verplicht dit artikellid het contactpunt om betrokkene te melden dat de andere deelnemende overheidsinstantie het verzoek afhandelt. Dit artikellid is opgenomen naar aanleiding van een daartoe strekkend voorstel van het Openbaar Ministerie.

In de consultatie heeft het OM opgemerkt dat het contactpunt inhoudelijk niet altijd de meest aangewezen deelnemer is om besluiten te nemen op verzoeken van betrokkenen. Het OM heeft bepleit om te regelen dat een contactpunt een verzoek kan overdragen aan een andere deelnemer van het samenwerkingsverband, indien die deelnemer beter in staat is de besluiten te nemen. Naar de verwachting van het OM leidt dit tot beter onderbouwde besluiten en voorkomt dit dat het contactpunt onnodig gegevens ontvangt. Het contactpunt blijft het punt waar een verzoek kan worden ingediend, maar het is mogelijk dat een andere deelnemende overheidsinstantie het verzoek afhandelt, indien deze daartoe beter in staat is.

In de consultatie hebben de RIEC's opgemerkt dat het aanwijzen van één burgemeester als contactpunt een behoorlijke afwijking van de huidige werkwijze is, waarbij per inzageverzoek bekeken wordt welke deelnemer het verzoek afhandelt. Voor de gemeente waarvan de burgemeester als contactpunt wordt aangewezen zal dit een aanzienlijke lastenverzwaring opleveren. Zoals hierboven is toegelicht, is naar aanleiding van de consultatiereacties het onderhavige vierde lid toegevoegd, waardoor het contactpunt met een andere deelnemende overheidsinstantie kan afspreken dat die het verzoek afhandelt, indien die daartoe beter in staat is. Bijgevolg is geen sprake van een behoorlijke afwijking van de huidige werkwijze, noch van een aanzienlijke lastenverzwaring. De RIEC's hebben overigens nu ook al een soort contactpunten, meestal de postbus van de stad met het grootste inwoneraantal in de betreffende RIEC-regio.

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.²⁰ Het onderhavige artikel bepaalt dat de deelnemende overheidsinstantie die optreedt als het contactpunt, zorgdraagt voor de (coördinatie bij de) nakoming van deze informatieplicht. Met dit artikel wordt invulling gegeven aan artikel 1.4, vierde lid, onder a, van de wet, 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.²¹ Het contactpunt kan op deze wijze zijn communicatieve rol relatief lastenluw uitvoeren.

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.

In de consultatie heeft Reclassering Nederland voorgesteld om in het eerste lid de volgende zinsnede achterwege te laten: «mits de betrokken deelnemers aan het contactpunt de benodigde informatie verstrekken ter uitvoering hiervan». Dit voorstel is overgenomen. De zinsnede is overbodig, want de gegevens die het contactpunt nodig heeft om een betrokkene te kunnen informeren – diens identificerende of contactgegevens – volgen al uit de aanmelding door een deelnemer van een signaal, verzoek of casus bij het samenwerkingsverband. Deze gegevens moeten de deelnemers registreren in het systeem van het samenwerkingsverband.²²

In de consultatie hebben de RIEC's, het Openbaar Ministerie en de VNG bepleit om mogelijk te maken dat de deelnemers *per geval* bepalen wie namens het samenwerkingsverband de betrokkene actief informeert over de gegevensverwerking. Het contactpunt heeft er immers niet noodzakelijk zicht op wanneer in een latere fase een uitzondering op de informatieplicht vervalt, terwijl een andere deelnemer (die een interventie overweegt) daarop mogelijk wel zicht heeft.

Dit punt wordt onderkend. Daarom is voor die situaties de verplichting opgenomen dat de betreffende deelnemer een melding moet doen aan het contactpunt zodra de uitzondering niet meer van toepassing is (derde lid). Dit stelt het contactpunt in staat de betrokkene alsnog te informeren. Het is evenwel niet gewenst dat de deelnemers per geval bepalen wie van hen betrokkene informeert. Wanneer een betrokkene wordt geïnformeerd, kan dat aanleiding geven om een AVG-verzoek te doen. Omdat zo'n verzoek bij het contactpunt kan worden gedaan, ligt het in de rede dat het contactpunt tevens degene is die betrokkene informeert. Voor de eenduidigheid naar betrokkenen is het daarom verkieslijk dat het contactpunt altijd degene is die hen informeert.

²⁰ 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.

²¹ Europees Comité voor gegevensbescherming, Richtsnoeren inzake transparantie overeenkomstig AVG, WP260 rev.01, punten 33 en 11.

²² Zie de artikelen 2.5, onderdeel c, 2.8, tweede lid, 2.11, derde lid, 2.16, tweede lid, 2.20, derde lid.

In de consultatie heeft een anonieme functionaris voor gegevensbescherming een aanpassing van dit lid bepleit om de indruk te vermijden dat de gezamenlijke verantwoordelijkheid wordt beperkt. In lijn met dit voorstel is «Alleen het contactpunt is verantwoordelijk» gewijzigd in «Het contactpunt draagt namens de deelnemers aan het samenwerkingsverband zorg voor de nakoming».

Tweede lid

In het tweede lid is de mogelijkheid opgenomen dat één of meer van de deelnemers die betrokken waren of zijn 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. Naar aanleiding van de consultatiereacties van onder meer het Openbaar Ministerie is de verplichting tot overleg tussen het contactpunt en de betrokken deelnemers meer expliciet in dit artikellid omschreven.

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).²³ Bij de vraag of de rechtstreekse 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.²⁴ 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).²⁵

Derde lid

Het is mogelijk dat de uitzonderingsgrond na verloop van tijd verval, 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

²³ Op de relevante excepties is nader ingegaan in paragraaf 3.4 van de memorie van toelichting bij de WGS (Kamerstukken II 2019/20, 35 447, nr. 3).

²⁴ Europees Comité voor gegevensbescherming, Richtsnoeren inzake transparantie overeenkomstig AVG, WP260 rev.01, punt 61.

²⁵ Europees Comité voor gegevensbescherming, Richtsnoeren inzake transparantie overeenkomstig AVG, WP260 rev.01, punt 64.

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 aansprakelijk overeenkomstig artikel 82, vijfde lid, AVG. De melding van een datalek gebeurt in afstemming met de deelnemers die betrokken waren of zijn bij de verwerking van de persoonsgegevens. 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 dat het contactpunt overlegt met de deelnemers die betrokken waren of zijn bij de verwerking van de persoonsgegevens en dat één of meer van deze deelnemers zich kunnen verzetten tegen melding van een datalek *aan een betrokkene* (artikel 34 AVG) indien dat naar hun oordeel noodzakelijk en evenredig is ter waarborging van een zwaarwegend belang als bedoeld in artikel 41 Uitvoeringswet AVG. Op de melding van een datalek *aan de Autoriteit persoonsgegevens* (artikel 33 AVG) is geen uitzondering mogelijk vanwege een zwaarwegend belang. Op grond van artikel 23, eerste lid, AVG, kan alleen artikel 34 vanwege een zwaarwegend belang buiten toepassing kan worden gelaten. In de consultatie hebben de RIEC's en Zorg- en Veiligheidshuis Rotterdam Rijnmond hierop terecht gewezen, waarna dit artikellid in voornoemde zin is aangepast.

In de consultatie hebben onder meer Reclassering Nederland en de RIEC's erop gewezen dat het contactpunt volgens het ontwerpbesluit niet zou hoeven te overleggen met deelnemers die geen gezamenlijke verwerkingsverantwoordelijken zijn (namelijk de private deelnemers aan een Zorg- en Veiligheidshuis), zelfs niet als zij betrokken waren bij de gegevensverwerking. Dit is aangepast, zodat het contactpunt moet overleggen met alle deelnemers die betrokken waren of zijn bij de verwerking van de persoonsgegevens (net als in artikel 1.2 en 1.3). Dat een deelnemer gegevens heeft ingebracht die onderdeel uitmaken van een datalek of anderszins betrokken was bij de verwerking van gegevens die onderdeel uitmaken van het datalek, rechtvaardigt dat het contactpunt met die deelnemer overlegt, ongeacht of die deelnemer behoort tot de gezamenlijke verwerkingsverantwoordelijken.

Artikelen 33, eerste lid, en 34, derde lid, AVG en artikel 42 Uitvoeringswet AVG bevatten enkele andere, meer technische, uitzonderingsgronden die het contactpunt kan toepassen. Daarvoor volstaat overleg met het contactpunt en is regeling van de wijze van besluitvorming niet nodig.

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.²⁶ De rechtmatigheid behelst de vraag of de verstreckende 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 verstreckende 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 maken²⁷ of aan informatie uit publiek toegankelijke bronnen die door de inbrengende deelnemer rechtmatig mag worden verwerkt.²⁸ Het is aan de betreffende deelnemer om te beoordelen of deze gegevens conform artikel 1.5 van de wet ingebracht moeten worden en of sprake is van zwaarwegende redenen die zich tegen verstrekking verzetten. In reactie op de opmerking van de RIEC's uit de consultatie dat een grondslag voor het inbrengen van informatie uit open bronnen door de partners van het RIEC ontbreekt, wordt dan ook geantwoord dat de wet en dit besluit gaan over het gezamenlijk verwerken van gegevens waarover de betrokken deelnemers al beschikken. Dat is iets anders dan het invoeren van nieuwe bevoegdheden tot het vergaren of verzamelen van informatie.

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 van de wet.

²⁶ Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 1.

²⁷ In die zin: Kamerstukken II 2019/20, 35 447, nr. 3, blz. 26.

²⁸ Kamerstukken II 2020/21, 35 447, nr. 6, blz. 51-52 (antwoord 61).

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.

Een concreet voorbeeld van hoe deze toets onder meer gestalte kan krijgen, is beschreven in de RIEC-procesbeschrijving integrale casus-aanpak: «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.»²⁹ 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.»³⁰

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)

²⁹ Voor zover mogelijk binnen hun taken en bevoegdheden.

³⁰ Werkproces integrale casusaanpak door het Regionaal Informatie en Expertise Centrum (RIEC), blz. 4.

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 vernietigen 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, van de wet 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 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.³¹ 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.³² 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 het FEC. Dit lid is niet van toepassing op casusoverleggen (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

³¹ Kamerstukken II 2021/22, 35 447, H, blz. 16.

³² Kamerstukken II 2021/22, 35 447, nr. 21, blz. 8 en 15.

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 2021,³³ en tijdens het wetgevingsoverleg in de Tweede Kamer over de WGS,³⁴ 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, van de wet. Voor andere doeleinden dan de identificatie van de betrokkene is de verwerking van persoonsgegevens over nationaliteit niet toegestaan.

In de internetconsultatie heeft Amnesty International geadviseerd om een verbod op te nemen op de verwerking van persoonsgegevens waaruit ras of etnische afkomst blijkt, in aanvulling op het verbod op verwerking van persoonsgegevens inzake nationaliteit. In reactie hierop wordt opgemerkt dat het voorgestelde verbod al bestaat krachtens artikel 9, eerste lid, van de AVG en artikel 22, eerste lid, Uitvoeringswet AVG. De AVG en de Uitvoeringswet AVG maken hierop slechts onder voorwaarden (beperkt) uitzonderingen mogelijk. Burgers zijn derhalve reeds beschermd tegen discriminatie op grond van hun ras of etnische afkomst. Overigens bevat de WGS geen basis voor de verwerking van persoonsgegevens waaruit ras of etnische afkomst blijkt, ook niet om dit bij amvb te regelen, zoals kennelijk is verondersteld.

Het Openbaar Ministerie heeft in de consultatie voorgesteld om artikel 1.9 te herzien en alsnog dezelfde uitzonderingsmogelijkheden te regelen voor persoonsgegevens inzake nationaliteit als voor bijzondere categorieën persoonsgegevens, te weten artikel 22 en 23 Uitvoeringswet AVG. Volgens het OM wordt de informatie-uitwisseling binnen de samenwerkingsverbanden onnodig belemmerd, bijvoorbeeld bij de aanpak van mensenhandel in RIEC-verband, waar het noodzakelijk kan zijn de nationaliteit te verwerken. In reactie hierop wordt opgemerkt dat het voorbeeld inzake de aanpak van mensenhandel in zoverre wordt ondervangen dat persoonsgegevens over nationaliteit volgens artikel 1.9 wél mogen worden verwerkt als dat voor de identificatie van betrokkene onvermijdelijk is. De noodzaak van nieuwe uitzonderingen is niet dragend onderbouwd, wat wel nodig is gelet op de gevoeligheid van de gegevens.

³³ Kamerstukken 2021/22, 35 447, nr. 21, paragraaf 7.1.

³⁴ Kamerstukken 2020/21, 35 447, nr. 20, blz. 37.

(grondslag: artikel 1.8, eerste lid, WGS)

Met het amendement-Yeşilgöz-Zegerius³⁵ 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.³⁶ Zoals is aangekondigd in de Kamerbrief van 17 december 2021 is het voornemen om bij amvb de gegevensverstrekking tussen de samenwerkingsverbanden nader te clausuleren.³⁷ 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).

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

Eerste lid, onderdeel a (twee samenwerkingsverbanden bevoegd)

Indien twee samenwerkingsverbanden in het concrete geval³⁸ 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.³⁹

³⁵ Kamerstukken 2020/21, 35 447, nr. 14.

³⁶ Namelijk op grond van artikel 1.8, eerste lid, van de wet.

³⁷ Kamerstukken 2021/22, 35 447, nr. 21, bijlage, punt 7.

³⁸ 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.

³⁹ Kamerstukken 2021/22, 35 447, nr. 21, bijlage, punt 7.

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.⁴⁰

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.⁴¹

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 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.⁴² In dat licht is artikel 1.7, achtste lid, van de wet ingevoegd bij amendement.⁴³ 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,

⁴⁰ 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.

⁴¹ Kamerstukken 2021/22, 35 447, nr. 21, bijlage, punt 7.

⁴² Brief aan Tweede Kamer van 25 november 2020, getiteld: «Inbreng VNG en Regioburgemeesters voor WGO Wet Gegevensverwerking door Samenwerkingsverbanden 7 december».

⁴³ Kamerstukken II 2020/21, 35 447, nr. 14

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. Verdere afstemming kan via de reguliere weg tot stand komen. Dat gaat buiten WGS of BGS om. In de consultatie hebben de RIEC's opgemerkt dat samenwerking tussen twee samenwerkingsverbanden soms overleg vergt, bijvoorbeeld als een casus twee RIEC's behelst. In reactie hierop wordt gewezen op artikel 2.20 van de wet, dat de RIEC's een grondslag biedt voor gegevensuitwisseling tussen meerdere RIEC's, voor zover dat noodzakelijk is voor het doel van de bestrijding van de georganiseerde criminaliteit, bedoeld in artikel 2.17 van de wet.

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

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.⁴⁴ 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, van de wet 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

⁴⁴ 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.

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.

In de consultatie hebben Reclassering Nederland, Zorg- en Veiligheidshuis Rotterdam Rijnmond, de Nederlandse GGZ en een anonieme functionaris voor gegevensbescherming opgemerkt dat er geheimhoudingsplichten zijn die in dit lid ontbreken. Voor gegevens die onder andere geheimhoudingsplichten vallen, volstaat dat het eerste lid de gegevensuitwisseling beperkt tot afstemmingsinformatie, en dat de deelnemers een instemmingsrecht hebben inzake de doorverstrekking van de gegevens die zij hadden ingebracht (artikel 1.7, achtste lid, WGS).

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 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 (eerste lid). De minimumeis van een VOG betreft de Zorg- en Veiligheidshuizen en het Financieel Expertisecentrum, aangezien voor iCOV en de RIEC's specifieke eisen gelden:

– 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). Dit sluit aan op het reeds bestaande screeningsbeleid.⁴⁵ Ter verduidelijking is deze specifieke norm voor iCOV in een separaat, tweede artikellid opgenomen; hiertoe heeft de AP in de consultatie geadviseerd.

⁴⁵ 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. Zie BIO Handboek Informatiebeveiliging hoofdstuk 7 en iCOV Screeningsbeleid 2022.

– Bij de RIEC's is sinds 1 juli 2022 een deel van de functies bij de Regeling aanwijzing functies VOG politiegegevens aangewezen voor een VOG Politiegegevens.⁴⁶

Dit artikel is grotendeels een codificatie van de screeningsvereisten die al waren opgenomen in de toepasselijke protocollen en andere documenten, zoals deze luiden voor de komst van de WGS.⁴⁷

In de consultatie heeft het Openbaar Ministerie geadviseerd om te vereisen dat een persoon ten minste in het bezit moet zijn van een VOG «die is toegesneden op het gewenste beschermingsniveau van de gegevens die in de systemen van het betreffende samenwerkingsverband worden verwerkt». Het ligt volgens het OM niet in de rede dat kan worden volstaan met het overleggen van een VOG die de betreffende persoon bij indiensttreding van de deelnemer heeft gekregen. Daarbij wijst het OM erop dat de toets die moet worden aangelegd bij het beoordelen van de VOG-aanvraag kan afwijken, doordat de te autoriseren persoon persoonsgegevens in de systemen van het samenwerkingsverband moet verwerken die meer bescherming verdienen dan de gegevens waar hij bij de reguliere werkzaamheden voor de deelnemer mee werkt. Ook wijst het OM erop dat na indiensttreding bij een deelnemer al vele jaren kunnen zijn verstreken, waardoor een VOG verouderd kan raken.

In het advies van het OM is geen aanleiding gezien om dit artikel aan te passen. Het werk binnen een samenwerkingsverband ligt in het verlengde van het werk voor de betreffende deelnemers. De integriteitsrisico's zijn daarom gelijk aan de integriteitsrisico's bij de reguliere werkzaamheden voor de medewerkers van de deelnemende organisaties van het samenwerkingsverband.

Het is bovendien ongebruikelijk een risicogebied op te nemen in een wettelijke bepaling. De deelnemende organisatie die de VOG aanvraagt geeft vanuit haar rol als werkgever aan welke risicogebieden van toepassing zijn. Dit zijn specifieke functieaspecten waar Justis in de screening rekening mee moet houden.⁴⁸ Van belang is dat de medewerkers die voor een samenwerkingsverband werken, in dienst blijven bij hun deelnemende organisatie (artikel 1.4, derde lid, WGS). Het ligt niet in de rede om voor autorisatie extra vereisten te stellen bovenop de eisen die de deelnemende organisatie stelt.

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, van de wet: zij worden geautoriseerd vanwege het onderhoud of de ondersteuning van de systemen.

⁴⁶ Het gaat om functies waarbij er sprake is van «toegang tot gevoelige informatie bij de uitvoering van wettelijke taken op het terrein van openbare orde en veiligheid of handhaving van de rechtsorde», waarin personen daadwerkelijk toegang hebben tot gevoelige informatie bij de uitvoering van voornoemde wettelijke taken. Per 1 mei 2023 geldt dit ook voor gemeentelijke informatiecoördinatoren en -analisten die beschikken over informatie uit RIEC-casuïstiek. Zie de Regeling van de Minister voor Rechtsbescherming van 3 april 2023, nr. 4565524, tot wijziging van de Regeling aanwijzing functies VOG Politiegegevens, Stcrt. 2023, 10263.

⁴⁷ Bij de Zorg- en Veiligheidshuizen is gangbaar dat de deelnemers voorzien in een vorm van screening die bestaat uit een VOG of een hoger vereiste. Dat volgt al geruime tijd uit artikel 13.3 template privacy protocol. Zo'n privacy protocol betreft onderlinge afspraken over de gegevensverwerking in een Zorg- en Veiligheidshuis.

⁴⁸ Voorbeelden hiervan zijn risicogebieden 11 (bevoegdheid hebben tot het raadplegen en/of bewerken van systemen) en 12 (met gevoelige/vertrouwelijke informatie omgaan).

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 vertrouwensfuncties⁴⁹ 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).⁵⁰ 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 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» (artikel 1.8, vierde lid, van de wet). Vanuit audit-perspectief zijn goede logfiles zeer belangrijk; met de logfiles kunnen handelingen en acties worden herleid.

Als uitwerking van artikel 1.8, vierde lid, van de wet verplicht dit artikel de deelnemers om de logging te laten plaatsvinden in lijn met de Baseline Informatiebeveiliging Overheid (BIO).⁵¹ 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 logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig

⁴⁹ <https://www.aivd.nl/actueel/nieuws/2014/09/08/nieuwe-leidraad-aanwijzing-vertrouwensfuncties>.

⁵⁰ Zie punt 9.2.5.3 van de BIO. Staatscourant 2020 nr. 7857 en <https://www.bio-overheid.nl>.

⁵¹ Zie Staatscourant 2020 nr. 7857 en <https://www.bio-overheid.nl>.

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.⁵² 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 informatiebeveiligingsdienst⁵³ 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)

⁵² 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.

⁵³ 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».

De artikelen 1.13 tot en met 1.15 bevatten de uitwerking van artikel 1.8, zesde lid, van de wet 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 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.⁵⁴

Eerste lid

De taak van de rechtmatigheidsadviescommissies is 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.⁵⁵

In de consultatie hebben de RIEC's gevraagd om de werkzaamheden van de rechtmatigheidsadviescommissie te verduidelijken en om bureaucratie te voorkomen. De VNG merkt op dat een dergelijke commissie een extra vertragende factor kan worden en wenst dubbelingen te voorkomen.

In reactie hierop wordt opgemerkt dat van de rechtmatigheidsadviescommissie niet wordt verwacht om iedere verstrekking van gegevens aan het samenwerkingsverband te beoordelen, wat inderdaad onevenredig zou zijn.⁵⁶ Haar rol is veeleer om te controleren of bepaalde werkwijzen binnen het samenwerkingsverband of de vervaardiging van bepaalde producten door het samenwerkingsverband zodanig zijn ingericht dat deze rechtmatig zijn en dat een «bias» in gegevens zo veel mogelijk wordt

⁵⁴ Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 9.

⁵⁵ Kamerstukken II 2019/20, 35 447, nr. 3, blz. 60.

⁵⁶ Kamerstukken II 2019/20, 35 447, nr. 3, blz. 60.

voorkomen.⁵⁷ De meerwaarde van de rechtmatigheidsadviescommissie kan daarbij juist zijn dat zij duidelijkheid verschaft over de rechtmatigheid, wat niet zozeer vertragend werkt als wel het proces bevordert.

De rechtmatigheidsadviescommissie dient in ieder geval te adviseren over grondslagen en te treffen technische en organisatorische maatregelen; ook brengt zij privacy-issues in beeld en stelt zij mitigerende maatregelen voor.⁵⁸ Verder heeft een rechtmatigheidsadviescommissie tot taak om de rechtmatigheid te toetsen van de verstrekking van een resultaat aan een derde (artikel 1.7, tweede lid, van de wet). Tot slot volgt uit artikel 2.9, tweede lid, van dit besluit dat de rechtmatigheidsadviescommissie van iCOV adviseert over een nieuwe gestandaardiseerde themarapportage als bedoeld in artikel 2.13, onder c, van de wet en over latere wijzigingen in een dergelijke gestandaardiseerde themarapportage.

In de consultatie heeft Amnesty International geadviseerd een verplichte, bindende en transparante mensenrechtentoets vast te leggen. Uit het voorgaande moge blijken dat met de rechtmatigheidsadviescommissie is voorzien in een dergelijke toetsing. Zij dient niet alleen het recht op privacy, maar moet ook aandacht hebben voor het tegengaan van risico's op ongelijke behandeling en discriminatie (artikel 1.14, vierde lid). Wanneer er geautomatiseerde gegevensanalyse plaatsvindt, gelden er bovendien tal van aanvullende waarborgen die bedoeld zijn om discriminatie, fouten en vooroordelen tegen te gaan.⁵⁹ Ook worden er afwegingskaders toegepast voor het zorgvuldige gebruik van algoritmes.⁶⁰ Als iCOV tot een nieuw type gezamenlijke geautomatiseerde gegevensanalyse overgaat, moet iCOV op grond van artikel 35 AVG een gegevensbeschermingseffectbeoordeling uitvoeren en bij hoge risico's moet iCOV de AP raadplegen op grond van artikel 36 AVG.⁶¹ Tot slot wordt aan mensenrechtelijke toetsing bijgedragen door de functionarissen voor gegevensbescherming, de coördinerend functionaris voor gegevensbescherming, periodieke onafhankelijke gegevensbeschermingsaudits en het toezicht door de AP.

Tweede lid

Zoals genoemd in de voornoemde Kamerbrief van 17 december 2021 zijn rechtmatigheidsadviescommissies bevoegd rechtstreeks aan het samenwerkingsverband te adviseren, zonder tussenkomst van leidinggevenden, en worden zij geacht hierin onafhankelijk te opereren.⁶² 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

⁵⁷ Kamerstukken I 2022/23, 35 447, K, vraag 84 en paragraaf 13.

⁵⁸ Kamerstukken II 2019/20, 35 447, nr. 3, blz. 72-73.

⁵⁹ Zie Kamerstukken I 2022/23, 35 447, K, antwoord 37 en artikel 1.9 WGS en artikelen 2.9-2.12 BGS.

⁶⁰ Kamerstukken I 2022/23, 35 447, K, antwoord 40.

⁶¹ Dit is toegelicht in de nota n.a.v. het verslag. Kamerstukken II 2020/21, 35 447, nr. 6, antwoord 85, blz. 71.

⁶² Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 9.

van de deelnemers.⁶³ 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 van de deelnemers aan een samenwerkingsverband hebben op grond van artikel 38, tweede lid, van de AVG een recht op toegang tot de adviezen. Het ligt in de rede dat de rechtmatigheidsadviescommissie hierop anticipeert door aan de coördinerend functionaris voor gegevensbescherming voor het samenwerkingsverband, bedoeld in artikel 1.4, tweede lid, van de wet een afschrift van alle relevante adviezen toe te zenden.⁶⁴ Dit maakt het mogelijk dat de coördinerend FG, samen met FG's van de deelnemers die het advies aangaat, een advies controleert op de vraag of het wettelijk kader goed is gevolgd en of er juiste conclusies worden getrokken over de rechtmatigheid. De coördinerend FG en de FG's van de deelnemers kunnen dit doen indien zij daartoe aanleiding zien gelet op de risico's en de aard en omvang van de verwerking (artikel 39, tweede lid, AVG). Aldus is voorzien in een blik van buiten de rechtmatigheidsadviescommissie, met het oog op de onafhankelijkheid en het gezag van de adviezen van de rechtmatigheidsadviescommissie.

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 en daarbij te motiveren waarom ze afwijken van het advies.

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

⁶³ 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».

⁶⁴ De rechtmatigheidsadviescommissie kan, bijvoorbeeld in het reglement van orde, uitwerken welke soorten adviezen zij aan de coördinerend FG toezendt. Alles toezenden belast de coördinerend FG mogelijk te zwaar.

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.

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. In de consultatie hebben de RIEC's gevraagd of er een maximumtermijn kan worden gesteld aan de reactietermijn voor het geven van een advies door de rechtmatigheidsadviescommissie. Het is niet goed te overzien wat een algemene redelijke termijn zou zijn en het kan uiteenlopen hoe verstrekkend de werkzaamheden zijn. Om vertraging in de advisering te voorkomen bevat het vierde lid een oplossing om tijd te besparen bij onderlinge meningsverschillen, en bevat artikel 1.14, tweede lid, een waarnemingsregeling.

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 en verantwoording. 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, inclusief de motivering voor de afwijking, wordt door de deelnemers gerapporteerd aan de rechtmatigheidsadviescommissie en de coördinerend functionaris voor gegevensbescherming voor het samenwerkingsverband.

Onderdeel van de coördinerende rol van de coördinerend FG is dat deze de gerapporteerde afwijkingen van adviezen van de rechtmatigheidsadviescommissie deelt met de FG's van de andere deelnemers voor zover hen dit aangaat. Dit is nodig om te zorgen dat ook de FG's van de andere deelnemers hun bevoegdheden kunnen uitoefenen, net zoals de coördinerend FG andere relevante informatie met de andere FG's moet delen, zoals adviezen van de rechtmatigheidsadviescommissie en de resultaten van de privacy audits. De rol van de coördinerend FG is immers niet alleen dat deze het toezicht door de FG's van de deelnemers coördineert door waar nodig de onderlinge afstemming te faciliteren, maar ook om relevante informatie te delen met deze FG's.

(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, van de wet. 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. Zoals is toegelicht in §2 van het nader rapport op het advies van de Afdeling advisering van de Raad van State op dit besluit, wordt geen noodzaak gezien om extern voorzitterschap van de rechtmatigheidsadviescommissies dwingend voor te schrijven, maar kan een externe voorzitter wel worden benoemd, mits wordt voldaan aan de deskundigheids- en ervaringsvereisten uit het onderhavige artikellid en mits met de externe voorzitter geen persoonsgegevens of vertrouwelijke operationele informatie wordt gedeeld.

In de consultatie hebben Amnesty International en een oud-functionaris voor gegevensbescherming bepleit om vast te leggen dat de rechtmatigheidsadviescommissies onafhankelijk zijn. Zoals nader is toegelicht in de memorie van antwoord⁶⁵, is voorzien in een stevige positie van de rechtmatigheidsadviescommissie doordat zij rechtstreeks adviseert aan de bestuurders van de deelnemers, zonder tussenkomst van een managementteam van een samenwerkingsverband (artikel 1.13, tweede lid). Een afwijking van een advies moet bovendien gerapporteerd worden aan de coördinerend functionaris voor gegevensbescherming, die zo nodig in actie kan komen (artikel 1.13, zesde lid). Hierin komt de onafhankelijke rol tot uiting. Als zou worden bedoeld dat in het besluit zou moeten worden

⁶⁵ Kamerstukken I 2022/23, 35 447, K, vraag 82.

voorgeschreven dat tot de rechtmatigheidsadviescommissie alleen externe personen kunnen toetreden, dan zou eraan voorbij worden gegaan dat juist bij de deelnemers specialistische kennis en expertise aanwezig is inzake de werking van de samenwerkingsverbanden en de specifiek toepasselijke regelgeving. Als het gaat om formeel onafhankelijk toezicht op de gegevensverwerking, zijn daarvoor beschikbaar de onafhankelijke coördinerend functionaris voor de gegevensbescherming voor het samenwerkingsverband, de onafhankelijke functionarissen voor gegevensbescherming van de deelnemers, de onafhankelijke, periodieke privacy audits en de AP. De periodieke privacy audits moeten worden verricht door onafhankelijke auditors (artikel 1.18, derde lid, van dit besluit). De auditresultaten moeten aan de AP en de coördinerend FG worden gezonden (artikelen 1.10 van de wet en 1.18, vierde lid, van dit besluit).

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 leden 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,⁶⁶ 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 samenwerkings-

⁶⁶ Kamerstukken II 2021/22, 35 447, nr. 21, paragraaf 7.2.

verband.⁶⁷ 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, van de wet 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 lokale en regionale deelnemers worden vertegenwoordigd door personen die benoemd worden door vertegenwoordigende koepelorganisaties of brancheverenigingen van deze deelnemers. Ook in de bestaande werkgroep gegevensdeling zorg en veiligheid worden de lokale en regionale deelnemers vertegenwoordigd door koepelorganisaties en brancheorganisaties. Deze bepaling is daarmee een codificatie van de huidige praktijk, die overigens goed functioneert.

Gelet op de opsomming van de deelnemers van de Zorg- en Veiligheidshuizen in artikel 2.27 van de wet valt hierbij te denken aan gemeenten (VNG), GGD (GGD-GHOR Nederland), reclasseringsinstellingen (Reclassering Nederland⁶⁸), 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.

In de consultatie heeft Zorg- en Veiligheidshuis Rotterdam Rijnmond voorgesteld om met een bepaling in dit besluit te voorzien dat koepelorganisaties of brancheverenigingen in een nader reglement opnemen

⁶⁷ 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).

⁶⁸ In de consultatiereactie van Reclassering Nederland is overigens terecht opgemerkt dat ook valt te denken aan Stichting Verslavingsreclassering GGZ en Stichting Leger des Heils Jeugdbescherming & Reclassering.

hoe zij de vertegenwoordiger aan kunnen wijzen en de ruggespraak hierover met de achterban regelen, evenals wat de status is van de aangewezen vertegenwoordiger en de vaststelling van de opdracht.

Dit advies is niet overgenomen, omdat de wijze waarop de vertegenwoordigers van de branche- en koepelorganisaties worden benoemd, aan hen is, in overleg met de deelnemers. De mogelijkheid tot aanwijzing van vertegenwoordigers uit koepelorganisaties of brancheverenigingen is bedoeld als praktisch alternatief voor deelname door vele honderden lokale en regionale deelnemers, waaronder gemeenten. Deze vertegenwoordigers zijn volwaardige leden van de rechtmatigheidsadviescommissie en moeten beschikken over de relevante deskundigheid en ervaring (artikel 1.14, eerste lid). Hun taak is niet om belangen van de achterban te behartigen, maar om te adviseren over de rechtmatigheid (artikel 1.8, zesde lid, WGS).

De bepaling sluit niet uit dat de rechtmatigheidsadviescommissie bepaalde lokale of regionale deelnemers uitnodigt om in een concreet geval hun expertise in te brengen. Een lokale of regionale deelnemer van het samenwerkingsverband kan zich hiertoe ook op eigen initiatief melden bij de rechtmatigheidsadviescommissie. De leden van de rechtmatigheidsadviescommissie worden geacht de deelnemers te informeren over de agenda. In het reglement van orde, bedoeld in artikel 1.13, vijfde lid, kan de werkwijze zo nodig worden uitgewerkt.

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 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.⁶⁹ 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.

⁶⁹ Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 8.

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 2021.⁷⁰

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.⁷¹ 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. Weliswaar zijn die niet van toepassing op gezamenlijke gegevensverwerkingen in het samenwerkingsverband omdat de wet en dit besluit daarvoor de termijnen al regelen, maar voor de invulling van de noodzaak tot langdurige bewaring kan wel aansluiting worden gezocht bij een bijzondere wet. Zo kunnen op grond van de wet 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 (veelal maximaal 20 jaar), 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. Het voorgaande geldt mutatis mutandis voor gegevens die zijn ingebracht op grond van de Wzd. Dit betekent dat de deelnemers in het Zorg- en Veiligheidshuis bij de beoordeling of hernieuwde verwerking noodzakelijk is op grond van artikel 1.16, tweede en derde lid, voor zover het gaat om Wvggz of Wzd-gegevens aansluiting kunnen zoeken bij de bewaartermijnen uit de Wvggz en Wzd. Verder is van belang dat de bewaartermijn in de wet en dit besluit uitsluitend ziet op de gegevens die in het samen-

⁷⁰ Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 8.

⁷¹ Kamerstukken II 2019/20, 35 447, nr. 3, blz. 128-129.

werkingsverband worden verwerkt. Dit betreft dus niet de fase waarin een deelnemer gegevens voor de eigen taak verwerkt na het resultaat van de gezamenlijke gegevensverwerking van het samenwerkingsverband te hebben ontvangen op grond van artikel 1.7 van de wet.

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 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 levensloopaanpak 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 verantwoor-

dingsplicht uit artikel 5, tweede lid, AVG. Tevens dient betrokkene geïnformeerd te worden over de verlenging van de termijn.

Casussen die na zeven jaar nog steeds voldoen aan de criteria komen vrijwel uitsluitend voor in de categorie waarin 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 weliswaar 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. Indien de bewaartermijn verlengd wordt vanwege het risico op terugval, en er binnen die verlengingsperiode geen sprake is van terugval, dienen de gegevens alsnog vernietigd te worden. Het is dus niet zo dat de bewaartermijn oneindig verlengd kan worden puur vanwege een verondersteld risico op terugval. Op deze regeling is nader ingegaan in §3 van het nader rapport op het advies van de Afdeling advisering van de Raad van State inzake dit besluit.

Artikel 1.17 Opleiding en training ten aanzien van gegevensverwerking

(grondslag: artikel 1.8, negende lid, WGS)

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.⁷² 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. Bij data-ethiek en zorgvuldige omgang met persoonsgegevens komt ook het tegengaan van (onbewuste) discriminatie aan de orde.

In de consultatie heeft de VNG opgemerkt dat een specificatie van het artikel ontbreekt in deze nota van toelichting. Als het doel is dat bepaalde kennis/vaardigheden aanwezig is bij de betreffende medewerkers, kan meer ruimte worden gelaten aan de deelnemers en zou ook rekening moeten worden gehouden met «voorhanden instructies», of «supervisie».

In reactie hierop wordt benadrukt dat dit artikel een zorgplicht betreft die is gericht op passende opleidingen en trainingen. Het gaat erom dat de medewerkers over de noodzakelijke kennis en vaardigheden beschikken. Dat kan mede gestalte krijgen door instructies en goed inwerken, voor zover dat eraan bijdraagt dat de medewerkers beschikken over de noodzakelijke kennis en vaardigheden. De wijze waarop samenwerkingsverbanden precies invulling geven aan deze zorgplicht, leent zich

⁷² Kamerstukken I 2021/22, 35 447, H, blz. 1, 2, 8, 16 en 19.

minder goed voor vastlegging bij algemene maatregel van bestuur. Er moet in de praktijk ruimte blijven voor maatwerk.

Artikel 1.18 Uitwerking auditbepaling

(grondslag: artikel 1.10, vijfde lid, WGS)

Dit artikel is een uitwerking van artikel 1.10, vijfde lid, van de wet, 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, van de wet 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 inwerking-treding 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 van de wet 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. Deze onafhankelijkheid betekent bijvoorbeeld dat de auditor niet in dienst mag zijn bij de deelnemer. Aan de eis van onafhankelijkheid is bijvoorbeeld wel voldaan in het geval van de Auditdienst Rijk.

Ook moet de auditor volgens dit artikellid beschikken over «deskundigheid en 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 Veiligheids-huizen – 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 informatie-beveiligingsaudit.⁷³ 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 wet. Ook zij zijn immers «geautoriseerde personen» in de zin van de wet (artikel 1.8, tweede lid, onder b, WGS).

Hoofdstuk 2. Bepalingen inzake specifieke samenwerkingsverbanden

Paragraaf 2.1 Financieel 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 wet 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.⁷⁴ Daarbij geldt de kanttekening dat de overige deelnemers tot op heden niet deelnemen aan de gezamenlijke verwerking en er derhalve geen 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

⁷³ 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.

⁷⁴ Bron: M. Wesseling / M. de Goede, *Beleid Bestrijding Terrorismefinanciering Effectiviteit en Effecten* (2013-2016), Universiteit van Amsterdam, 2018, blz. 171 en 175.

verwerkingsverantwoordelijken zijn, maar dan uitsluitend voor zover het gaat om gegevensverwerkingen ten behoeve van het Programma Terrorismefinanciering.

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 terrorismefinanciering.

De FEC-deelnemers beogen met het Programma Terrorismefinanciering (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 van de wet. De deelnemers beschikken over voor dit doel relevante (noodzakelijke) informatie en/of interventiemogelijkheden. Het programma richt zich meer concreet op:⁷⁵

- 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 terrorismefinanciering en het verankeren van lessons learned bij betrokken partners.

De samenwerking in het Programma Terrorismefinanciering geschiedt concreet in het FEC Terrorismefinanciering Analyseteam. Dat is belast met de analyse van de tussen deelnemers uitgewisselde informatie op het gebied van bestrijding van terrorismefinanciering ten behoeve van de samenwerking op het gebied van bestrijding van terrorismefinanciering. Het FEC Terrorismefinanciering analyseteam verzamelt, ordent, rangschikt, verrijkt, analyseert en registreert informatie in een signaalendatabase 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 Terrorismefinanciering moet worden onderscheiden van de Taskforce Terrorismefinanciering van het FEC. In het Programma Terrorismefinanciering 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 terrorismefinanciering, waarna interventies kunnen worden afgesproken. Bij het Programma Terrorismefinanciering wordt uitsluitend door overheidsinstanties samengewerkt. Bij de Taskforce Terrorismefinanciering 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)

⁷⁵ 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 terrorismefinanciering (Stcrt. 2015, nr. 18775).

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 terrorismefinanciering. Met het oog op dit doel werken de deelnemers aan het FEC al enige jaren samen met financiële instellingen.

Onderdeel b van 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 publiek-private «taskforces». Zoals in de memorie van toelichting bij de WGS is toegelicht,⁷⁶ 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 wet.

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. De deelnemers worden in dit besluit bestendigd. 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 persoonsge-

⁷⁶ 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.»

gegevens uitgewisseld.⁷⁷ Buiten de taskforces vindt in de zogeheten «projecten» publiek-private samenwerking met de financiële instellingen plaats, zonder persoonsgegevens uit te wisselen.⁷⁸

Publieke partijen: OM, politie, FIU-Nederland en FIOD (artikel 2.2, onderdeel a)

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-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 Terrorismefinanciering

De gegevensverwerking in de Taskforce Terrorismefinanciering 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

⁷⁷ 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.

⁷⁸ 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.

deelnemers: zij zijn op grond van de Wwft verplicht om indien daartoe aanleiding is een Wwft-melding te doen.

De Terrorismefinanciering Taskforce is beschreven in een convenant uit 2019.⁷⁹

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 Ondermijning. De werkwijze van de Serious Crime Taskforce vertoont veel parallellen met de hiervoor beschreven werkwijze van de Taskforce Terrorismefinanciering, 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 2019.⁸⁰

Artikel 2.3 Beperking gegevensverstrekking over kring van personen

(grondslag: artikel 2.4, tweede lid, WGS)

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. De proportionaliteit van het verwerken van deze gegevens moet worden getoetst door de gevolgen voor de persoonlijke levenssfeer van betrokkenen af te wegen tegen het zwaarwegend algemeen belang van het voorkomen en bestrijden van het gebruik van het financiële stelsel voor terrorismefinanciering, financieel-economische criminaliteit en andere ernstige vormen van criminaliteit.

⁷⁹ Staatscourant 2019, 43628 met addendum in Staatscourant 2020, 46050.

⁸⁰ Zie Staatscourant 2019, 43629 met addendum in Staatscourant 2021, 25818.

Om rekening te kunnen houden met constructies waarbij het vermogen verderop in de keten wordt verhuld, maakt dit lid een uitzondering: tot een ruimere verstrekking van gegevens over relaties of contacten kan worden overgegaan, voor zover sprake is van een keten van vermogensverschaffers, leidinggevend, 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.

In de consultatie heeft de AP geadviseerd om te verduidelijken dat de gegevensverstrekking in méér dan drie lijnen vanaf de betrokkene alleen is toegestaan over relaties of contacten die in verband staan met de hiervoor bedoelde keten. Daartoe is, conform het advies van de AP, «indien» vervangen door «voor zover» in dit artikellid.

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.⁸¹

Eerste lid (criteria voor aanmelding signaal of verzoek)

Het is van groot belang dat een bij het FEC ingebracht signaal⁸² 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 voldoende aanwijzingen als startpunt neer te leggen voor alle

⁸¹ Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 1.

⁸² 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».

samenwerkingsverbanden.⁸³ 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.⁸⁴ 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 wet. 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 sanctieregeling, fraude en oplichting, illegaliteit en het niet voldoen aan eisen van integere bedrijfsvoering zoals opgenomen in de Wft en de Wwft.⁸⁵

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

⁸³ Advies van 9 november 2021, Kamerstukken I 2021/22, 35 447, G, blz. 5 en 18–19.

⁸⁴ Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 1.

⁸⁵ Bron: FEC Jaarplan 2021, blz. 6.

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 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.⁸⁶

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».⁸⁷ 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.⁸⁸

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

⁸⁶ Kamerstukken II 2020/21, 35 447, 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.

⁸⁷ Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 4.

⁸⁸ 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, 25 403, nr. 3, p. 73). Deze voorbeelden moeten omwille van de toekomstbestendigheid en flexibiliteit overigens niet uitputtend worden opgevat.

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.

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 het signaal of verzoek te registreren met de vermelding of naar het oordeel van de deelnemers 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.

In de consultatie heeft het Openbaar Ministerie gevraagd of dit betekent dat de toegestane vormen van gegevensverwerking door het FEC niet als geautomatiseerde gegevensanalyse moeten worden aangemerkt. De toegestane gegevensverwerkingen door het FEC betreffen inderdaad geen geautomatiseerde gegevensanalyse.⁸⁹ Geautomatiseerde gegevensanalyse is een analyse van persoonsgegevens waarbij *tijdens* de analyse geen menselijke tussenkomst plaatsvindt, maar nadat de analyse is voltooid menselijke tussenkomst plaatsvindt ter controle van het resultaat op de zorgvuldige totstandkoming, alvorens dit te verstrekken (art. 1.1 en 1.9, tweede lid, WGS).⁹⁰

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

⁸⁹ Zie ook Kamerstukken II 2022/23, 35 447, K, vraag 35.

⁹⁰ Zoals is toegelicht in de nota van wijziging (Kamerstukken II 2020/21, 35 447, nr. 7) is er geen geautomatiseerde gegevensanalyse als een softwarepakket slechts dient als hulpmiddel *terwijl de feitelijke analyse door een natuurlijk persoon geschiedt*, of in het geval van «hit, no-hit»-bevraging (is geen analyse).

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 iCOV-rapportage relaties draagt bij aan onderzoeken in het kader van handel met voorwetenschap, marktmanipulatie, belangenverstrengeling 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 houdt op de cryptomarkt sinds de stapsgewijze inwerkingtreding van Verordening (EU) 2023/1114 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 aanvrager 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 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.

In augustus 2022 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, mensen-smokkel 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 van de aansluiting op iCOV, en de daaruit voortvloeiende mogelijkheid tot het verzoeken om vermogens- en relatierapportages van natuurlijke en rechtspersonen, vooral een meerwaarde 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. De producten van iCOV kunnen eraan 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.⁹¹ Zoals toegelicht in paragraaf 4.2 van de memorie van toelichting bij de wet, 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 bevraagde subject. In de memorie van toelichting is aangegeven dat dit inhoudt dat tot drie stappen vanaf het bevraagde subject de relevante relaties worden weergegeven.⁹² 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, leidinggevenden, 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.

In de consultatie heeft de AP geadviseerd om te verduidelijken dat de gegevensverstrekking in méér dan drie lijnen vanaf de betrokkene alleen is toegestaan over relaties of contacten die in verband staan met de hiervoor bedoelde keten. Daartoe is, conform het advies van de AP, «indien» vervangen door «voor zover» in dit artikellid.

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.⁹³ 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 bevraagde

⁹¹ Zie hierover uitgebreid Kamerstukken II 2019/20, 35 447, nr. 3, blz. 26 en 81.

⁹² Kamerstukken II 2019/20, 35 447, nr. 3, blz. 26.

⁹³ Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 1.

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.

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.⁹⁴ 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.⁹⁵ 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

⁹⁴ Advies van 9 november 2021, Kamerstukken I 2021/22, 35 447, G, blz. 5 en 18–19.

⁹⁵ Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 3.

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 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.⁹⁶ 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 van de wet 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. Met deze personen wordt bedoeld op de natuurlijke of rechtspersonen waarover duidelijke en objectieve aanwijzingen bestaan dat op onrechtmatige wijze financieel gewin is of wordt behaald en hun relevante relaties als bedoeld in artikel 2.12, tweede lid, onder b, WGS.

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

⁹⁶ Vgl. Kamerstukken II 2019/20, 35 447, nr. 3, blz. 82.

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

Volgens de definitie uit artikel 2.13, onder c, van de wet is een iCOV Rapportage Thema (iRT NN)⁹⁷ 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

⁹⁷ 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.

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.⁹⁸

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 en artikel 2.10. 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 dan 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;
- b. witwassen, ernstige fraude en daaraan gerelateerde vormen van financieel-economische criminaliteit, of

⁹⁸ Kamerstukken II 2019/20, 35 447, nr. 3, blz. 27 en 81.

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 (concurrentiebeperkende 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 het samenwerkingsverband tot een nieuw type gezamenlijke geautomatiseerde gegevensanalyse overgaat (iRT NN), dient het een gegevensbeschermingseffectbeoordeling uit te voeren op grond van

artikel 35 AVG.⁹⁹ 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)

ICOV moet bij de selectie van een nieuw thema rekening houden met de wijze waarop het thema inzicht geeft in de problematiek met betrekking tot 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.

⁹⁹ Dit is toegelicht in de nota n.a.v. het verslag. Kamerstukken II 2020/21, 35 447, nr. 6, antwoord 85, blz. 71.

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 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, van de wet 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 wet 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.¹⁰⁰

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 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 voorschrijft dat de evenredigheid van het vaststellen van een nieuw thema wordt getoetst aan de hand van de geschatte ernst, stelselmaticheid, 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

¹⁰⁰ Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 1.

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.¹⁰¹

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 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.

¹⁰¹ Kamerstukken II 2019/20, 35 447, nr. 3, blz. 27.

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 wet om een iRT NN op te stellen, evenals de bevoegdheid uit artikel 2.13, onder d, van de wet 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 de enige vorm van geautomatiseerde gegevensanalyse die wordt toegestaan door de wet en dit besluit.¹⁰²

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.

¹⁰² 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. De WGS 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, 35 447, nr. 7.

In de consultatie heeft het Openbaar Ministerie gevraagd of het aanwijzen van één soort analyse als geautomatiseerde gegevensanalyse betekent dat de overige vormen van gegevensverwerking door iCOV niet als geautomatiseerde gegevensanalyse worden aangemerkt. Dit is een juiste conclusie. Uit artikel 2.12, eerste lid, volgt dat alleen een themarapportage iRT NN wordt opgesteld op basis van een geautomatiseerde gegevensanalyse. De overige vormen van gegevensverwerking door de deelnemers van iCOV betreffen geen geautomatiseerde gegevensanalyse in de zin van de wet (artikel 1.1 van de WGS).

Tweede lid (in acht nemen productbeschrijving)

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)

Deze paragraaf bevat nadere regels over de RIEC's, in aanvulling op paragraaf 2.3 van de WGS. Laatstgenoemde paragraaf beschrijft onder meer het doel, de activiteiten, de deelnemers, onderlinge gegevensuitwisseling tussen RIEC's, en de grondslag voor gegevensverwerking voor activiteiten.

De activiteiten van een RIEC zijn volgens de wet: (a.) het aanwijzen en analyseren van handhavingsknelpunten, (b.) het voeren van casusoverleggen, en (c.) het verrichten van gebiedscans en thematische scans bij misstanden in maatschappelijke sectoren en publieke voorzieningen die vatbaar zijn voor innesteling van georganiseerde criminaliteit (artikel 2.18 WGS).¹⁰³

In de consultatie heeft het Openbaar Ministerie gevraagd of de activiteit «ondermijningsbeeld» – te weten «een bundeling van signalen en fenomenen van criminele aanwezigheid en activiteiten binnen een bepaald geografisch gebied» – ook valt onder hetgeen in artikel 2.18, eerste lid, onderdeel c, van de wet is omschreven. In reactie hierop kan worden bevestigd dat een ondermijningsbeeld daaronder is begrepen, mits het ondermijningsbeeld betrekking heeft op «misstanden in maatschappelijke sectoren en publieke voorzieningen die vatbaar zijn voor innesteling van georganiseerde criminaliteit». De memorie van toelichting noemt als voorbeelden het aanpakken van misstanden in de onroerend goedsector, het tegengaan van mensenhandel en -smokkel, georganiseerde hennepcultuur en andere door de Minister van Justitie en Veiligheid en de regionale stuurgroepen RIEC's te bepalen verschijningsvormen.¹⁰⁴ In het onderhavige besluit worden verschijningsvormen van georganiseerde criminaliteit uitgewerkt (artikel 2.16, onder b).

De activiteiten van de RIEC's mogen overigens geen geautomatiseerde gegevensanalyse in de zin van de wet omvatten, aangezien de mogelijkheid om bij amvb de bevoegdheid tot geautomatiseerde gegevensanalyse te regelen in dit besluit niet is ingevuld. Dit is toegelicht in de memorie van antwoord bij de wet.¹⁰⁵ In de consultatie heeft het Openbaar Ministerie gevraagd of dit betekent dat de toegestane vormen van gegevensverwerking door het RIEC niet als geautomatiseerde gegevensanalyse moeten worden aangemerkt. De toegestane gegevensverwerkingen door het RIEC betreffen inderdaad geen geautomatiseerde gegevensanalyse.¹⁰⁶ Geautomatiseerde gegevensanalyse is een analyse van persoonsgegevens waarbij *tijdens* de analyse geen menselijke tussenkomst plaatsvindt, maar nadat de analyse is voltooid menselijke tussenkomst plaatsvindt ter controle van het resultaat op de zorgvuldige

¹⁰³ Voor de activiteit «Bibob-ondersteuning door RIEC-deelnemers» blijven de bestaande regels gelden, omdat die toereikend zijn voor deze bilaterale gegevensverwerking (Kamerstukken II 2021/21, 35 447, nr. 20, blz. 42).

¹⁰⁴ Kamerstukken II 2019/20, 35 447, nr. 3, blz. 87–88.

¹⁰⁵ Kamerstukken II 2022/23, 35 447, K, vraag 35.

¹⁰⁶ Zie ook Kamerstukken II 2022/23, 35 447, K, vraag 35.

totstandkoming, alvorens dit te verstrekken (art. 1.1 en 1.9, tweede lid, WGS).¹⁰⁷

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 procesbe-

¹⁰⁷ Zoals is toegelicht in de nota van wijziging (Kamerstukken II 2020/21, 35 447, nr. 7) is er geen geautomatiseerde gegevensanalyse als een softwarepakket slechts dient als hulpmiddel terwijl de feitelijke analyse door een natuurlijk persoon geschiedt, of in het geval van «hit, no-hit»-bevraging (is geen analyse).

schrijvingen van de RIEC's uit 2019 worden verwerkt.¹⁰⁸ 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 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 moeten 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.¹⁰⁹ 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

¹⁰⁸ Zie de Procesbeschrijving integrale casusaanpak uit 2019, de Procesbeschrijving Gebiedswijkscan en nulmeting uit 2019 en de Procesbeschrijving Handhavingssknelpunten uit 2019: <https://www.riec.nl/documenten?trefwoord=procesbeschrijving>

¹⁰⁹ Kamerstukken II 2019/20, 35 447, nr. 3, blz. 101–103.

sluit tevens aan bij de memorie van toelichting bij de wet, waarin is benadrukt dat Belastingdienstgegevens pas in de tweede fase mogen worden verwerkt.¹¹⁰

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 toelichting¹¹¹ en de nota naar aanleiding van het verslag¹¹² bij de wet, is het voor het doel van de RIEC's noodzakelijk om bijzondere persoonsgegevens over seksueel gedrag 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 verwerkt (moeten) worden. Het onderhavige artikel verduidelijkt dat het dus uitsluitend gaat om persoonsgegevens met betrekking tot iemands seksueel gedrag 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. In het onderhavige artikel is de verwerking van persoonsgegevens met betrekking tot seksuele gerichtheid uitgesloten. Dit is aangepast conform een toezegging tijdens de plenaire behandeling van de wet in de Eerste Kamer op 11 juni 2024.

In de consultatie hebben de RIEC's opgemerkt dat het onduidelijk is of het fasegewijs proces uit het onderhavige artikel ook van toepassing is op de indiening van een signaal. In reactie hierop wordt opgemerkt dat het fasegewijs proces niet van toepassing is op de indiening van signalen. Dit volgt uit de zinsnede in artikel 2.23, zesde lid, van de wet, waaruit blijkt dat wordt toegekomen aan fase 1 «indien een signaal aanleiding geeft tot gezamenlijke verwerking van gegevens». Dit betekent dat moet worden teruggevallen op artikel 2.23, eerste lid, van de wet: een deelnemer kan een signaal melden, mits dat verband houdt met het doel van het RIEC, en daartoe gegevens verwerken. Op grond van artikel 2.16, tweede lid, van dit besluit moet bij de aanmelding van het signaal worden toegelicht in hoeverre is voldaan aan de criteria. Daarbij kan de deelnemer die het signaal aanmeldt gegevens verwerken die nodig zijn om de deelnemers in staat te stellen om te bepalen of het signaal in overeenstemming is met het doel van de RIEC's. Welke gegevens dat zijn, hangt af van het geval.

In de consultatie heeft de AP inzake de omschrijving van «gegevens omtrent de woonsituatie» opgemerkt dat de zinsnede «hoe de persoon woont, vanuit sociaal-economische invalshoek beschouwd» moet worden geconcretiseerd en dat de zinsnede «en de historie van inschrijvingen op het adres» moet vervallen. Dit advies is overgenomen door de gevraagde

¹¹⁰ Kamerstukken II 2019/20, 35 447, 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 (...).»

¹¹¹ Kamerstukken II 2019/20, 35 447, nr. 3, blz. 97.

¹¹² Kamerstukken II 2020/21, 35 447, nr. 6, blz. 128.

concretisering op te nemen. De zinsnede over de historie van inschrijvingen op het adres is geschrapt. Gegevens omtrent de woonsituatie kunnen volgens artikel 2.22, eerste lid, WGS uitsluitend betrekking hebben op de betrokkene over wie, of rechtspersoon waarover een signaal is aangemeld, dan wel personen uit diens directe kring (artikel 2.22, eerste lid, onderdeel a en b, WGS). Dit betekent dat de WGS niet toestaat dat gegevens omtrent de woonsituatie betrekking zouden hebben op de historie van inschrijvingen op het adres, aangezien die historie derden zou omvatten.

In de definitie van identificerende en contactgegevens is geëxpliciteerd dat de adresgegevens van degene over wie een signaal is aangemeld (dan wel diens directe kring), niet alleen betrekking kunnen hebben op diens huidige adresgegevens, maar ook op diens eerdere adresgegevens. Deze gegevens kunnen noodzakelijk zijn voor het doel van de RIEC's. Dergelijke gegevens worden tot op heden verwerkt overeenkomstig de procesbeschrijvingen van de RIEC's uit 2019, met gebruikmaking van de basisregistratie personen.

Artikel 2.16 Criteria voor behandeling van een signaal

(grondslag: artikel 2.23, negende lid, WGS)

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 2021.¹¹³ 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.¹¹⁴ 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.¹¹⁵

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».¹¹⁶ 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

¹¹³ 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.

¹¹⁴ Advies van 9 november 2021, Kamerstukken I 2021/22, 35 447, G, blz. 5 en 18–19.

¹¹⁵ Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 1.

¹¹⁶ Aldus punt 3.9 van het Privacyprotocol RIEC's-LIEC 2021.

verdiend, dat de grote winsten worden gebruikt om de bovenwereld te ondermijnen en dat de ondermijning dreigt door te werken naar de overheid.¹¹⁷

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 wet, met dien verstande dat «georganiseerde hennepcultuur» is geactualiseerd naar «georganiseerde drugscriminaliteit».¹¹⁸ 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 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.

¹¹⁷ Kamerstukken II 2018/19, 29 911, nr. 223, bijlage, blz. 17.

¹¹⁸ Kamerstukken II 2019/20, 35 447, nr. 3, blz. 84.

In de consultatie hebben de RIEC's en VNG voorgesteld om mogelijk te maken dat, voorafgaand aan de melding van een signaal door een deelnemer, persoonsgegevens gedeeld kunnen worden door het RIEC en die inbrengende deelnemer («verkennde fase») zodat signalen vervolgens conform de vereisten kunnen worden opgebouwd. In reactie hierop wordt opgemerkt dat een deelnemer zelfstandig een signaal kan aanmelden bij het RIEC en dat die deelnemer moet toetsen in hoeverre het signaal voldoet aan de criteria voor het in behandeling nemen van een signaal. Op grond van dit artikellid moet de deelnemer dit toelichten, bijvoorbeeld via het aanmeldformulier. Daarna dienen ook de andere deelnemers te beoordelen of naar hun oordeel is voldaan aan de criteria (artikel 2.23, tweede en derde lid, van de wet). De deelnemers registreren vervolgens in het systeem of naar hun oordeel is voldaan aan de criteria en nemen het signaal al dan niet in behandeling. Als het signaal niet voldoet, kunnen andere deelnemers inzichtelijk maken wat eventueel mist voor het in behandeling nemen van een signaal. Als met de consultatiereactie bedoeld zou zijn dat er in RIEC-verband moet kunnen worden overlegd indien een deelnemer constateert dat hij een signaal niet kan aanmelden omdat het niet voldoet aan de criteria – waarvan het belang door de RIEC's wordt onderschreven – dan zouden deze criteria zinledig zijn als informatiedeling met het RIEC ook mag plaatsvinden als aan die criteria niet is voldaan. Wel is denkbaar dat een deelnemer, voor zover bestaande bevoegdheden tot bilaterale gegevensuitwisseling dat toelaten, met een andere deelnemer overlegt alvorens een signaal aan te melden bij het RIEC.

De RIEC's hebben in de consultatie ook opgemerkt dat signalen vanuit het buitenland slechts zeer beperkt via RIEC-deelnemers in RIEC-samenwerkingsverbanden worden besproken. Zij verzoeken om te onderzoeken of buitenlandse overheidsorganen onder voorwaarden (tijdelijk) kunnen deelnemen aan een RIEC. In reactie hierop wordt opgemerkt dat de RIEC-deelnemers bij wet zijn aangewezen en dat zij krachtens hun eigen bevoegdheden en op grond van artikel 1.2, tweede lid, van de wet bilateraal internationale contacten onderhouden en indien nodig de resultaten daarvan binnen het RIEC inbrengen.

Paragraaf 2.4 Zorg- en Veiligheidshuizen (ZVH)

Artikel 2.17 Definitiebepaling

Artikel 2.26 van de wet 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 gepubli-

ceerd. 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 gesignaleerd 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.¹¹⁹

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.¹²⁰

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.¹²¹

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 wet.¹²²

«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.»*

¹¹⁹ Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 5.

¹²⁰ Kamerstukken II 2019/20, 35 447, nr. 3, blz. 125–126.

¹²¹ Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 1.

¹²² Kamerstukken II 2019/20, 35 447, nr. 3, blz. 106.

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.

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».¹²³ 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.

¹²³ Dit staat in voetnoot 41 van de memorie van toelichting op WGS (Kamerstukken II 2019/20, 35 447, nr. 3, blz. 106).

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 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.¹²⁴ 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.¹²⁵ 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. Zoals Reclassering Nederland in de consultatie terecht heeft opgemerkt, kan een reguliere private deelnemer kenbaar maken dat zij aanleiding ziet om een derde als incidentele deelnemer te betrekken; het is echter alleen aan de reguliere publieke deelnemers om te beslissen over die incidentele deelname. Dit vloeit voort uit de artikelen 2.27 en 2.31, negende lid, van de wet.

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 casusoverleg 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, die een maatschappelijke of politieke relevantie kent en waarbij de overheid betrokken is bij het beleidsterrein waartoe de taak gerekend kan worden.¹²⁶

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 of derden waarvoor betrokkene als huurder verantwoordelijk wordt geacht, in de woning of in de directe woonomgeving ernstige overlast veroorzaakt, of anderszins voor de woonomgeving een risico vormt, of

¹²⁴ Kamerstukken II 2019/20, 35 447, nr. 3, blz. 129.

¹²⁵ Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 6.

¹²⁶ 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.

– 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 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.

In de consultatie hebben de Samenwerkende Zorg- en Veiligheidshuizen bepleit dat ook CJIB/AICE moet kunnen deelnemen, omdat dit ten goede komt aan het plan van aanpak voor de besproken cliënten. Bij het CJIB is het Administratie- en Informatiecentrum voor de Executieketen (AICE) ingericht, dat als ketenregisseur namens de minister verantwoordelijk is voor de tenuitvoerlegging van strafrechtelijke beslissingen. Onder de voorwaarden van het onderhavige artikel lid kan AICE incidenteel deelnemen aan een casusoverleg, indien dat noodzakelijk is.

Verder hebben de Samenwerkende Zorg- en Veiligheidshuizen gevraagd wat de argumentatie is om zorgkantoren en zorgverzekeraars niet op te nemen als deelnemers, en of regionale besturen van Zorg- en Veiligheidshuizen zelf kunnen besluiten om specifieke deelnemers toe te voegen, ook als deze niet in de wet zijn genoemd. In artikel 2.27 van de wet zijn de vaste deelnemers van een Zorg- en Veiligheidshuis uitputtend opgesomd. Hierbij is aan de hand van hun taken onderbouwd waarom deelname noodzakelijk is voor het doel van het Zorg- en Veiligheidshuis. Een Zorg- en Veiligheidshuis kan niet zelfstandig andere vaste deelnemers laten toetreden. Indien een partij niet is genoemd in artikel 2.27 van de wet en deelname incidenteel noodzakelijk blijkt, is dat slechts mogelijk onder de voorwaarden voor incidentele deelname uit het onderhavige artikel. Voor zorgkantoren en zorgverzekeraars is niet gemotiveerd waarom daaraan zou worden voldaan.

Als in de toekomst blijkt dat er een noodzaak is om nieuwe *vaste* deelnemers toe te voegen kan dit overigens worden gerealiseerd via een wijziging van het besluit (op grond van artikel 2.27, vijfde lid, WGS).

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 de wet, 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.

In de consultatie heeft het Openbaar Ministerie geadviseerd om het onderhavige artikel aan te passen om de incidentele deelname van een betrokkene of persoon uit directe kring van betrokkene mogelijk te maken.

Het Openbaar Ministerie doelt erop dat in de consultatieversie van artikel 2.21 stond dat derden «*uitsluitend*» op incidentele basis kunnen deelnemen in de daar genoemde gevallen. Hierdoor zou deelname door een betrokkene of een persoon uit de kring van de betrokkene zijn uitgesloten. Omdat een dergelijke uitsluiting niet is beoogd, is het woord «*uitsluitend*» geschrapt. Zoals hierboven is toegelicht, kan toestemming van de betrokkene volgens de AVG de grondslag vormen voor het verwerken van persoonsgegevens over die persoon; in dit geval bestaat die verwerking uit deelname aan een casusoverleg.

Tweede lid (geheimhoudingsverklaring)

Dit lid bepaalt dat incidentele deelnemers een geheimhoudingsverklaring moeten tekenen. De geheimhoudingsplicht geldt op grond van de artikelen 1.11 en artikel 2.31, tiende lid, van de wet 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.

In de consultatie hebben de Samenwerkende Zorg- en Veiligheidshuizen opgemerkt dat de geheimhoudingsplicht in artikel 1.11 van de wet niet van toepassing is «voor wie reeds uit hoofde van ambt, beroep of wettelijk voorschrift ter zake van die gegevens een geheimhoudingsplicht geldt». Zij vragen of er dan nog een separate geheimhoudingsverklaring benodigd is. Het is inderdaad niet beoogd om hier een doublure te creëren, maar in een dergelijke situatie mag van de derde wel worden verwacht om te verklaren dat hij bij de gegevensverwerking gebonden is aan een bijzonder geheimhoudingsregime uit hoofde van zijn ambt of beroep of een wettelijk voorschrift.

Derde lid (geen autorisatie voor systemen)

Dit lid concretiseert artikel 2.31, negende lid, van de wet, 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, van de wet, 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, van de wet. 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.¹²⁷

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

¹²⁷ Kamerstukken II 2019/20, 35 447, nr. 3, blz. 110 en 131.

een periode van een jaar meerdere malen is aangehouden in verband met overlastgevende 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.

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 wet. 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, van de 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° en 3°, van de wet 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, van de wet 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 casus-overleg).

Hoofdstuk 4. Slotbepalingen

Artikel 4.1 Inwerkingtreding

Dit artikel regelt dat de wet, dit besluit en de wijzigingswet WGS¹²⁸ in werking treden met ingang van 1 maart 2025. Deze datum is enerzijds gekozen vanwege de Aanwijzingen voor de regelgeving, die voorschrijven dat de termijn tussen de publicatiedatum en het tijdstip van inwerkingtreding minimaal drie maanden is, indien een regeling direct relevant is voor medeoverheden (aanwijzing 4.17, vierde lid) en anderzijds vanwege signalen uit de betrokken samenwerkingsverbanden, dat de komende periode noodzakelijk is voor de implementatie van nieuwe waarborgen uit de wet en dit besluit. Het gaat dan onder meer om de aanwijzing van de coördinerend FG's, rechtmatigheidsadviescommissies en contactpunten, het aanpassen van werkprocessen en het voorlichten van de medewerkers over de nieuwe regels.

Met deze inwerkingtredingsdatum wordt afgeweken van de vaste verandermomenten, omdat niet kan worden gewacht tot 1 juli 2025. Deze afwijking is gerechtvaardigd omdat de wet en dit besluit essentieel zijn voor de integrale aanpak van ernstige, ondermijnende vormen van criminaliteit en van complexe problemen op het snijvlak van zorg en veiligheid, waarbij informatiedeling tussen ketenpartners cruciaal is. Het is urgent dat de wet en dit besluit zorgen voor een helder juridisch kader om gegevens gezamenlijk te verwerken voor deze belangrijke gemeenschappelijke doeleinden. Hiermee worden aanmerkelijke ongewenste publieke nadelen voorkomen als bedoeld in aanwijzing 4.17, vijfde lid, aanhef en onder a, van de Aanwijzingen voor de regelgeving.

Voor de artikelen 1.3, vijfde lid, WGS en 1.4, derde lid, eerste volzin, WGS geldt een afwijkende inwerkingtredingsdatum, namelijk 1 juli 2025. Deze bepalingen regelen dat het personeel dat gegevens verwerkt, niet in dienst mag zijn van een aparte rechtspersoon, maar in dienst moet zijn van de deelnemers van het samenwerkingsverband. In sommige Zorg- en Veiligheidshuizen is dit personeel nu in dienst van stichtingen of gemeenschappelijke regelingen met rechtspersoonlijkheid. Zij hebben tot 1 juli nodig voor de aanpassingen in de rechtspersoonlijkheid en om op zorgvuldige wijze ervoor te zorgen dat dit personeel in dienst komt van de deelnemers.

Voor de inwerkingtreding van de artikelen 2.1, 2.2 en 2.6 van dit besluit – die aanvullende deelnemers aan iCOV en het FEC aanwijzen – is een separaat koninklijk besluit nodig, want daarbij geldt de verplichting tot het volgen van een parlementaire nahangprocedure op grond van de artikelen 2.3, derde lid, en 2.11, derde lid, van de wet. Volgens laatstgenoemde artikelen kan het inwerkingtredingsbesluit dat daarop betrekking heeft, niet eerder worden vastgesteld dan vier weken na de start van de nahangprocedure, welke procedure niet eerder kan starten dan na vaststelling van het onderhavige besluit, het BGS. Het streven is dat de artikelen 2.1, 2.2 en 2.6 per 1 maart ingaan.

De Minister van Justitie en Veiligheid,
D.M. van Weel

¹²⁸ Wet van 26 juni 2024 tot wijziging van de Wet gegevensverwerking door samenwerkingsverbanden in verband met het waarborgen van de parlementaire betrokkenheid bij de aanwijzing van andere samenwerkingsverbanden (Stb. 2024, 254).