Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2022–2023

35 447 Regels omtrent gegevensverwerking door samenwerkingsverbanden (Wet gegevensverwerking door samenwerkingsverbanden)

K

MEMORIE VAN ANTWOORD

Ontvangen 20 februari 2023

Met belangstelling heb ik kennisgenomen van het voorlopig verslag van de vaste commissie voor Justitie en Veiligheid. Graag ga ik hieronder, mede namens de Minister voor Rechtsbescherming, in op de gestelde vragen. De antwoorden op de vragen van de bij het verslag betrokken fracties zijn waar nodig gegroepeerd naar thema. In de antwoorden wordt ook verwezen naar het concept-Besluit gegevensverwerking door samenwerkingsverbanden (hierna: concept-BGS). Hiermee wordt uitvoering gegeven aan verplichtingen uit het wetsvoorstel en worden zorgpunten geadresseerd van uw Kamer, de Afdeling advisering van de Raad van State en de Autoriteit Persoonsgegevens. De tekst van het concept-BGS is gelijktijdig met de publicatie van deze memorie van antwoord beschikbaar op www.internetconsultatie.nl/bgs. Tegelijk met de consultatiefase vinden de uitvoeringstoetsen plaats. Zoals toegelicht in antwoord op vraag 31, zal ik na de consultatiefase het gehele ontwerpbesluit in het kader van de voorhangprocedure aan uw Kamer voorleggen.

1. Inleiding

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel Wet Gegevensverwerking door Samenwerkingsverbanden (WGS). De regering heeft met de brief van 17 december 2021[1] de grootste hobbel weggenomen, door de delegatiebepaling buiten werking te zetten en toe te zeggen met een aanpassing te komen. De leden van de VVD-fractie onderschrijven de gekozen oplossing (reparatiewetgeving), omdat de gegevensuitwisseling op dit moment minder waarborgen omvat en geen wettelijke basis heeft. De leden van de VVD-fractie hebben nog wel enkele vragen en aandachtspunten.
De fractieleden van de PvdA en GroenLinks hebben met interesse kennisgenomen van het gewijzigde voorstel. Zij hebben nog enkele vragen.
De leden van de fractie van D66 hebben met belangstelling kennisgenomen van het wetsvoorstel alsmede de onderliggende stukken

[1] Kamerstukken I 2021/22, 35 447, I.

kst-35447-K
ISSN 0921 - 7371
's-Gravenhage 2023

waaronder, nadat het wetsvoorstel als gevolg van amendering was aangepast, de op verzoek van de Eerste Kamer uitgebrachte hernieuwde advisering van het College voor de Rechten van de Mens (brief van 24 juni 2021)[2], de Autoriteit Persoonsgegevens (brief van 9 november 2021)[3] en de Afdeling Advisering van de Raad van State (brief van 18 november 2021)[4] , alsmede de reactie van de regering daarop bij brief van 17 december 2021.
De leden van de PVV-fractie hebben kennisgenomen van het voorstel en hebben nog enkele vragen.
De leden van de ChristenUnie-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel, dat sinds de voorgenomen indiening een aantal forse wijzigingen heeft ondergaan. Deze leden stellen met genoegen vast dat de regering op een aantal punten gevolg heeft gegeven aan de reacties op de consultatie en de adviezen van onder meer de Raad van State. Ook is het wetsvoorstel tijdens de behandeling in de Tweede Kamer nog verder aangepast. Graag stellen deze leden nog de volgende vragen.
De leden van de PvdD-fractie hebben kennisgenomen van het voorstel en hebben enkele vragen hierover. Verzocht wordt dat alle sub-vragen afzonderlijk worden beantwoord.
De leden van de SGP-fractie hebben kennisgenomen van het wetsvoorstel gegevensverwerking door samenwerkingsverbanden. De leden van de SGP-fractie onderschrijven dat het van belang is om gegevensverwerking tussen samenwerkingsverbanden te reguleren. Op dit moment vindt deze gegevensverwerking zonder wettelijke grondslag plaats. In het belang van de bestrijding van ernstige en onder meer ondermijnende criminaliteit dient de gegevensverwerking van samenwerkingsverbanden op een overzichtelijke en rechtsstatelijke manier te worden vormgegeven. De leden van de SGP-fractie hebben nog enkele vragen over het wetsvoorstel.

2. Doelen

Vraag 1 (D66) – brede doelen en noodzakelijkheid, proportionaliteit en subsidiariteit
Allereerst wensen de D66-fractieleden op te merken dat zij doordrongen zijn van het belang van een grotere effectiviteit van de integrale aanpak van «georganiseerde criminaliteit» en de ondermijningsproblematiek, van risico's van inbreuken op de integriteit van het financiële stelsel, van witwas- of fraudeconstructies, van complexe problemen rond personen op het vlak van zorg en veiligheid, en van onder meer (andere) «ernstige vormen van criminaliteit». Zij steunen het principe dat gegevens daarover door samenwerkingsverbanden in beginsel moeten kunnen worden gedeeld en verwerkt. Daarnaast achten de leden van de D66 fractie de vastlegging van waarborgen – in aanvulling op de AVG – voor een goede bescherming van de persoonsgegevens die door deze samenwerkingsverbanden worden verwerkt, noodzakelijk.
Dat gezegd hebbende, vragen de leden van de D66-fractie zich af of de breed geformuleerde doelen in het wetsvoorstel de daar vermelde inbreuken op de grondrechten van het individu (art. 10, recht op eerbiediging van de persoonlijke levenssfeer) rechtvaardigen. Voldoen de maatregelen die voorgesteld worden wel aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit?

---

[2] Kamerstukken I 2021/22, 35 447, D.
[3] Kamerstukken I 2021/22, 35 447, G.
[4] Kamerstukken I 2021/22, 35 447, H.

Zoals de Afdeling advisering in haar voorlichting heeft onderkend, is een zeker abstractieniveau bij de doelomschrijvingen onvermijdelijk. Daarom is een zorgvuldige uitvoeringspraktijk cruciaal om in concrete gevallen telkens te bezien of en op welke wijze aan het doelbindingsbeginsel kan worden voldaan.[5] De gezamenlijke gegevensverwerking door een samenwerkingsverband moet te allen tijde passen binnen de in het wetsvoorstel omschreven doelomschrijvingen. Die doelomschrijvingen vergen mede dat de gezamenlijke gegevensverwerking noodzakelijk is voor de uitoefening van publiekrechtelijke taken en bevoegdheden van de deelnemers.[6] Daarnaast somt het wetsvoorstel op welke categorieën gegevens mogen worden verwerkt en zijn bij amvb nadere preciseringen voorzien van de gegevensverwerkingen, onder meer voor wat betreft de concretisering van het startpunt van de gegevensverwerking in elk samenwerkingsverband.

De eisen die de AVG stelt aan de verwerking van persoonsgegevens gelden onverkort onder de WGS. Bij elke verwerking van persoonsgegevens moeten de deelnemers van een samenwerkingsverband toetsen of de verwerking noodzakelijk is met het oog op het doel waarvoor zij gezamenlijk gegevens mogen verwerken. Elke separate persoonsgegevensverwerking moet voldoen aan de eisen van de AVG, waaronder het beginsel van minimale gegevensverwerking. Onderdeel daarvan is ook dat in ieder geval in het kader van de subsidiariteit en proportionaliteit steeds een afweging zal moeten worden gemaakt welke gegevens kunnen worden gedeeld en of dat noodzakelijk is voor het realiseren van het doel van het samenwerkingsverband, alsook welke deelnemers op welk moment betrokken moeten worden en dus in een voorkomend geval gerechtigd zijn gezamenlijk gegevens te verwerken.

In aanvulling op de AVG bevatten de WGS en het concept-BGS nadere waarborgen voor een goede bescherming van de persoonsgegevens. Te denken valt aan onder meer de onafhankelijke privacy audits, de rechtmatigheidsadviescommissies, de opleidings- en trainingsplicht op het gebied van de gegevensverwerking, en de aanvullende waarborgen bij geautomatiseerde gegevensanalyse. Een volledig overzicht van de waarborgen is opgenomen in het antwoord op vraag 13.

Vraag 2 (D66) – doelen iCOV
De doelen van de samenwerkingsverbanden zijn belangrijk in de opbouw van dit wetsvoorstel, constateren de leden van de D66-fractie. Daarom is het van belang dat die doelen helder, afgebakend en eenduidig worden omschreven. Als voorbeeld nemen zij artikel 2.10 WGS waar het doel van de Infobox Crimineel en Onverklaarbaar Vermogen (ICOV) wordt beschreven.
Wat wordt bedoeld met «met het oog op het in kaart brengen van (...) en het uitoefenen van toezicht op de goede werking van de markt (...)» in artikel 2.10 WGS? Welke markt? Waarom wordt dit doel zo vaag en breed omschreven?

ICOV is een samenwerkingsverband met een breed palet aan deelnemende overheidsorganisaties. Het gaat hierbij om opsporingsdiensten, organisaties met een fiscale taak of een taak op het gebied van invordering, en markttoezichthouders. De diversiteit van organisaties versterkt de ketenaanpak van het op onrechtmatige wijze behalen van financieel gewin. Het samenwerkingsverband heeft volgens artikel 2.10 van het wetsvoorstel als doel «het in kaart brengen van onverklaarbaar of

[5] Kamerstukken I 2021/22, 35 447, H, blz. 10 en 18.
[6] Aldus artikelen 2.2, 2.10, 2.17 en 2.25 in samenhang gelezen met 1.6, eerste lid, van het wetsvoorstel.

crimineel vermogen, het bestrijden van witwas- of fraudeconstructies, het kunnen innen van overheidsvorderingen die oninbaar dreigen te worden en het uitoefenen van toezicht op de goede werking van de markt (...) voor zover dat noodzakelijk is voor de uitoefening van publiekrechtelijke taken en bevoegdheden van de deelnemers».
Deze slotzinsnede vormt een relevante clausulering: de gegevensverwerking moet niet alleen noodzakelijk zijn voor het gemeenschappelijk doel, maar óók noodzakelijk zijn voor de uitoefening van publiekrechtelijke taken en bevoegdheden van de deelnemers (opgesomd in artikel 2.11). Hierin ligt het antwoord besloten op de vraag van de D66-fractie welke markt het betreft: bij de deelnemende markttoezichthouders gaat het dan om het stabiliteitstoezicht en toezicht op trustdienstverleners door De Nederlandsche Bank (DNB) en het mededingingstoezicht, energietoezicht, consumententoezicht en telecomtoezicht door de Autoriteit Consument en Markt (ACM). Markttoezichthouders zijn een cruciale schakel in de aanpak van witwassen en ondermijning omdat juist financiële structuren daarvoor misbruikt worden.
In de artikelen 2.8 en 2.11 van het concept-BGS is een verdere clausulering opgenomen: een verzoek van een deelnemer om een rapportage wordt slechts in behandeling genomen bij duidelijke en objectieve aanwijzingen dat op onrechtmatige wijze financieel gewin is of wordt behaald. Een gegevensverwerking door iCOV moet dus altijd verband houden met het op onrechtmatige wijze behalen van financieel gewin. Daarnaast bevat paragraaf 2.2 van het concept-BGS concrete minimumgrenzen en andere criteria waaraan moet worden voldaan, vooraleer kan worden toegekomen aan gegevensverwerking door iCOV.
Ook voor de andere samenwerkingsverbanden – namelijk het Financieel Expertise Centrum, de Regionale Informatie- en Expertisecentra en de Zorg- en Veiligheidshuizen – bevat het concept-BGS een relevante clausulering in verband met de doeleinden van de samenwerkingsverbanden, met name doordat het startpunt van de gegevensverwerking wordt geconcretiseerd (artikelen 2.4, 2.16 en 2.20 concept-BGS). Eén van de startcriteria is dat altijd sprake moet zijn van duidelijke en objectieve aanwijzingen van risico's in verband met het doel van het samenwerkingsverband.

Vraag 3 (VVD) – doel iCOV inzake innen overheidsvorderingen
ICOV verwerkt gegevens met het oog op het in kaart brengen van onverklaarbaar of crimineel vermogen, het bestrijden van witwas- of fraudeconstructies, het kunnen innen van overheidsvorderingen die oninbaar dreigen te worden en het uitoefenen van toezicht op de goede werking van de markt. Voor deze doelstellingen mag iCOV gegevens verwerken. Niet alle doelstellingen zijn echter even «zwaar». Op welke wijze, vragen de leden van de VVD-fractie, rechtvaardigt het innen van overheidsvorderingen een inbreuk op de privacy?

Volgens artikel 2.10 van het wetsvoorstel is de doelstelling van iCOV mede gericht op «het kunnen innen van overheidsvorderingen die oninbaar dreigen te worden (...) voor zover dat noodzakelijk is voor de uitoefening van publiekrechtelijke taken en bevoegdheden van de deelnemers». De inning van vorderingen is een belangrijke schakel in de aanpak van criminaliteit, want als vorderingen niet geïnd kunnen worden kan criminaliteit alsnog lonend zijn.
Een voorbeeld is de inning van een strafrechtelijke ontnemingsmaatregel van € 20.000 die is opgelegd aan een veroordeelde voor oplichting. Het Centraal Justitieel Incassobureau (CJIB) heeft tot taak deze vordering te innen. De veroordeelde stelt de vordering niet te kunnen betalen. Het CJIB kan als deelnemer aan iCOV een aanvraag doen om een iCOV Rapportage Vermogen en Inkomsten (iRVI). Hiermee kan het CJIB controleren of er onvermelde vermogenscomponenten zijn op basis waarvan het CJIB toch

een hoger bedrag zou kunnen invorderen. Uit de iRVI kan bijvoorbeeld blijken dat de veroordeelde in de jaren ervoor een forse erfenis heeft gehad. De veroordeelde stelt te zijn «vergeten» om dit te melden en dat de erfenis in beheer is bij een notaris, die maandelijks een deel uitkeert. Door de iCOV-rapportage kan het CJIB het maandelijks in te vorderen bedrag verhogen en kan de ontnemingsmaatregel in korte tijd worden geïnd.
De doelstelling van het innen van overheidsvorderingen is niet onbeperkt. Het gaat niet om willekeurig welke overheidsvordering. Het gaat om overheidsvorderingen die oninbaar dreigen te worden. In artikel 2.8 van het concept-BGS is daarnaast opgenomen dat alleen aan gegevensverwerking voor dit doel kan worden toegekomen als sprake is van duidelijke en objectieve aanwijzingen dat op onrechtmatige wijze financieel gewin is of wordt behaald. Dit kan volgens voornoemd artikel bovendien alleen bij overheidsvorderingen van ten minste € 5.000 vanwege een onherroepelijke boete, ontnemingsmaatregel of schadevergoedingsmaatregel. Daarnaast moet worden voldaan aan de andere vereisten van een verzoek om een rapportage, waaronder een proportionaliteitstoets. Aldus wordt gewaarborgd dat deze gegevensverwerking voldoende zwaarwegend is om een inbreuk op de privacy te rechtvaardigen. Overigens sluit de formulering van artikel 2.10 WGS aan bij de doelen uit het iCOV-convenant waarvoor deelnemers nu bilateraal gegevens kunnen uitwisselen.[7]

Vraag 4 (D66) – reikwijdte doel RIEC's
Ook de beschrijving van het doel van de RIEC's, het samenwerkingsverband dat zich vooral met het strafrechtelijk deel zal bezighouden en dat uit een enorm groot aantal partijen kan bestaan, is uiterst ruim geformuleerd. Artikel 2.17 WGS stelt dat uitsluitend gegevens verwerkt mogen worden voor zover noodzakelijk voor de uitoefening van de wettelijke taken en bevoegdheden op het terrein van handhaving «in het belang van de bestrijding van de georganiseerde criminaliteit». De leden van de D66-fractie constateren dat het begrip «georganiseerde criminaliteit» onbepaald is en niet nader is gedefinieerd in de begripsbepalingen van artikel 1.1 van dit wetsvoorstel. Waarom niet? Wat met «georganiseerde criminaliteit» wordt bedoeld hangt er van af aan wie je het vraagt (en is bovendien aan verandering onderhevig). De gedachte dat daarmee een beperking wordt aangebracht en dat alleen de zwaarst mogelijke vormen van criminaliteit hieronder zouden vallen is in ieder geval niet juist; zo gauw er sprake is van zelfs maar een minimaal gestructureerde samenwerking tussen meerdere personen die zich een korte periode bezig houden met strafbare feiten kan van georganiseerde criminaliteit worden gesproken. Zo zal het in de praktijk ook vrijwel zeker worden uitgelegd. Is daarmee de toepassingssfeer van die RIEC's niet te groot, zo vragen de leden van de D66-fractie. Waarom heeft de regering niet als minimumdrempel een bepaalde wettelijke strafbedreiging bij het begrip «georganiseerde criminaliteit» opgenomen, bijvoorbeeld een verband dat zich bezig houdt met misdrijven waar een gevangenisstraf van vier jaar of meer op staat?

Het begrip georganiseerde criminaliteit is een breed begrip.[8] De regering onderkent dat het startpunt van de gegevensverwerking voldoende precies en duidelijk moet zijn. In artikel 2.16 van het concept-BGS worden daarom nadere criteria gesteld waar een signaal aan moet voldoen om in

[7] Artikel 2, Convenant iCOV 2018, Stcrt. 2019, 11302.
[8] In punt 3.9 van het Privacyprotocol RIEC's-LIEC 2021 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».

behandeling te kunnen worden genomen door een RIEC, zoals het vereiste dat in het concrete geval een gezamenlijke aanpak met meerdere deelnemers van het RIEC nodig is. Verder is één van die criteria dat het signaal moet zijn gerelateerd aan de aldaar opgesomde verschijningsvormen van georganiseerde criminaliteit, namelijk mensenhandel en -smokkel, georganiseerde drugscriminaliteit, fraude of misbruik in de vastgoedsector, dan wel witwassen en daaraan gerelateerde vormen van financieel-economische criminaliteit. De opgesomde verschijningsvormen zijn afkomstig uit artikel 2 van het RIEC-convenant en zijn genoemd in de memorie van toelichting op de WGS.[9] 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. Daarnaast bevat artikel 2.16 van het concept-BGS de mogelijkheid dat een RIEC-stuurgroep of de Minister van Justitie en Veiligheid, na toetsing van de evenredigheid, aanvullende verschijningsvormen van georganiseerde criminaliteit benoemt. Dit moet dan worden bekengemaakt door plaatsing op internet. 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.
Overigens zullen de deelnemers van een RIEC bij elke casus in het kader van de subsidiariteit en proportionaliteit steeds een afweging moeten maken welke gegevens kunnen worden gedeeld en of dat noodzakelijk is voor het realiseren van het doel van het samenwerkingsverband alsmede welke deelnemers op welk moment betrokken moeten worden en dus in een concreet geval gerechtigd zijn gezamenlijk gegevens te verwerken. Artikel 2.23, derde lid, van het wetsvoorstel bevat hiertoe criteria aan de hand waarvan een signaal in een concreet geval moet worden getoetst, zoals het type en gewicht van het signaal, het aantal signalen en de aard en omvang daarvan.

Vraag 5 (PvdD) – welbepaaldheid doelen FEC en iCOV
Op bladzijde 16 van het advies van de Autoriteit Persoonsgegevens wordt ingegaan op de vraag of de artikelen 2.2, tweede lid en 2.10 WGS voldoen aan de eis van «welbepaaldheid».[10] De Autoriteit Persoonsgegevens oordeelt van niet en beroept zich daarbij op de uitspraak van het Europese Hof van Justitie in de zaak Digital Rights Ireland en op het bindend advies van het Hof van Justitie Europese Unie over de Passenger Name Record (PNR)-overeenkomst tussen de EU en Canada.
Deelt de regering de conclusie van de Autoriteit Persoonsgegevens? Zo nee, op welke juridische redenering wordt die ontkennende beantwoording gegrond?

In het aangehaalde onderdeel van het advies adviseert de AP om de wettelijke doelen van de samenwerkingsverbanden aan te scherpen. Voor zover het gaat om de welbepaaldheid van de doelstelling van iCOV wordt verwezen naar het antwoord op *vraag 2 (D66) – doelen iCOV*.
Voor zover het gaat om de welbepaaldheid van de doelstelling van het FEC, bakent het concept-BGS de gegevensverwerking in het FEC af tot (onderdelen van) specifieke doelen, passend binnen de doelstelling van het FEC uit artikel 2.2 WGS. Daarbij is conform het advies van de AP de term «andere ernstige vormen van criminaliteit» gedefinieerd, zoals is aangekondigd in punt 4 van de bijlage bij de brief van 17 december 2021 (Reactie op afzonderlijke aanbevelingen advies AP).[11] Ook regelt het

[9] Kamerstukken II 2019/20, 35 447, nr. 3, blz. 84.
[10] Kamerstukken I 2021/22, 35 447, G, p. 16.
[11] Kamerstukken II 2021/22, 35 447, nr. 21, blz. 12–13.

concept-BGS een beperking van de kring van personen waarover gegevens worden verwerkt (artikel 2.3), criteria voor de behandeling van een signaal of verzoek in het FEC (artikel 2.4) en nadere aanvullende waarborgen (artikel 2.5). Aldus wordt de welbepaaldheid bevorderd.

3. Adviezen

Vraag 6 (GroenLinks/PvdA) – appreciatie van de adviezen
De Eerste Kamer heeft de Autoriteit Persoonsgegevens, het College voor de Rechten van de Mens en de Raad van State gevraagd om (nader) advies uit te brengen over het gewijzigde voorstel van wet. De leden van de fracties van GroenLinks en PvdA hebben naar aanleiding van die adviezen een aantal specifieke vragen, maar zouden de regering om te beginnen willen vragen een appreciatie van de in de adviezen genoemde punten van zorg en kritiek te geven. Ook vernemen de leden graag of de geuite zorgen aanleiding zijn geweest voor de regering om de wet te heroverwegen of aan te passen? En op welke wijze is de nieuwe Staatssecretaris voor Digitalisering bij dit wetsvoorstel betrokken?

Het overgrote deel van de aanbevelingen uit de adviezen van de AP en het College voor de Rechten van de Mens en de voorlichting van de Afdeling advisering van de Raad van State neem ik over. In de brief van 17 december 2021[12] van de toenmalige Minister van Justitie en Veiligheid is een appreciatie gegeven van de aanbevelingen uit de adviezen van de AP en het College voor de Rechten van de Mens en van de voorlichting van de Afdeling advisering. In het concept-BGS heb ik deze Kamerbrief als uitgangspunt genomen. Schematisch weergegeven ziet de opvolging van de aanbevelingen van de AP eruit als weergegeven in onderstaande tabel. De nummering van de aanbevelingen loopt hierin synchroon met de appreciatie van de aanbevelingen in de Kamerbrief van 17 december 2021:

Aanbeveling AP	**Verwerkt in concept-BGS?**
1. Startpunt van de gegevensverwerking verduidelijken.	Ja, artikelen 2.4, 2.8, 2.11, 2.16 en 2.20.
2. Schrappen van de doelstellingen van iCOV inzake het innen van overheidsvorderingen die oninbaar dreigen te worden en het uitoefenen van toezicht op een goede werking van de markt.	Nee, wel wordt in het concept-BGS de gegevensverwerking door iCOV beperkt tot onrechtmatig financieel gewin (artikelen 2.8, 2.10 en 2.11).
3. Ondergrens inzake crimineel en onverklaarbaar vermogen bij iCOV.	Ja, artikel 2.8.
4. Preciseren doelstelling FEC inzake «andere ernstige vormen van criminaliteit».	Ja, artikel 2.4, derde lid.
5. Gegevensverzameling Zorg- en Veiligheidshuizen beperken tot directe omgeving.	Ja, artikel 2.19.
6. Uitdrukkelijke criteria voor incidentele deelname aan Zorg- en Veiligheidshuizen.	Ja, artikel 2.21.
7. Schrappen van mogelijkheid gegevensdeling tussen samenwerkingsverbanden.	Nee, wel wordt dit nader geclausuleerd in het concept-BGS (artikel 1.10).
8. Preciseren bewaartermijn.	Ja, artikel 1.16.
9. Toets door onafhankelijke bestuurlijke autoriteit bij verstrekking aan derden.	Ja, artikel 1.13, tweede lid (onafhankelijke rol). Zie ook vraag 82.
10. Duidelijke regeling over uitzonderingen op rechten betrokkene en transparantie.	Ja, art. 1.3 en 1.8, tweede lid (en art. 14 AVG en 1.9, derde lid, WGS).

[12] Kamerstukken II 2021/22, 35 447, nr. 21.

Aanbeveling AP	Verwerkt in concept-BGS?
11. Verstrekkingsplicht wijzigen in bevoegdheid.	Nee, wel hebben de deelnemers enige beoordelingsruimte bij het bepalen welke gegevens noodzakelijk zijn voor het samenwerkingsverband, en kunnen zij wegens zwaarwegende redenen afzien van verstrekking.[1]

[1] Zie punt 11, Kamerstukken II 2021/22, 35 447, nr. 21.

In de adviezen zie ik op één punt aanleiding tot aanpassing van het wetsvoorstel, namelijk om de mogelijkheid om bij amvb nieuwe samenwerkingsverbanden te regelen, te beperken tot tijdelijke spoedsituaties. Dit licht ik toe in hoofdstuk 11 van deze memorie van antwoord dat hier specifiek aan is gewijd. Dit is eerder aangekondigd in §5.1 van de brief van 17 december 2021 van de toenmalige Minister van Justitie en Veiligheid.[13] De Staatssecretaris voor Digitalisering heeft bij de totstandkoming van het voorliggende wetsvoorstel geen betrokkenheid.

Vraag 7 (PvdD) – aanbevelingen AP en de amvb
De regering ziet in de kritiek van de Autoriteit Persoonsgegevens aanleiding om in het Besluit gegevensverwerking door samenwerkingsverbanden een tiental punten nader te regelen.
De leden van de PvdD-fractie vragen of de regering alle aanbevelingen van de Autoriteit Persoonsgegevens overgenomen? Zo nee, welke niet en waarom niet? De aanpassingen die de regering voorstelt, betreffen voorschriften in een AMvB en niet in een formele wet. Wordt daarmee voldoende voorkomen dat het stelsel in rechte zal standhouden indien een rechter over de rechtmatigheid moet oordelen van de inbreuken op grondrechten of op de Algemene Plaatselijke Verordening (APV) en andere relevante regelgeving? Wordt de inwerkingtreding van de WGS uitgesteld totdat de AMvB tot stand is gebracht? Zo nee, bestaat er dan een reële kans dat de rechter in die periode de WGS of de uitvoering daarvan onrechtmatig acht, nu de regering heeft aangegeven – gelet op de zwaarwegende juridische kritiek van de Autoriteit Persoonsgegevens – dat alsnog in de AMvB nadere waarborgen zullen moeten worden geregeld?

Verwezen wordt naar het antwoord op de vorige vraag. Ook in de bijlage bij de brief van 17 december 2021 is de toenmalige Minister ingegaan op de aanbevelingen van de AP. De nadere uitwerking in het concept-BGS is nodig voor een goede werking van de wet en regelt de onderwerpen waarvan de WGS verplicht dat deze bij amvb worden uitgewerkt. De voorwaarden en waarborgen uit het wetsvoorstel en de amvb zijn nodig om de gegevensverwerkingen juridisch houdbaar te laten zijn in het licht van de AVG en artikel 8 EVRM. Het is dan ook om meerdere redenen vereist om de wet en de amvb tegelijkertijd in werking te laten treden. Uit artikel 10 Grondwet kan niet worden afgeleid dat iedere afzonderlijke inbreuk op het grondrecht van de persoonlijke levenssfeer bij formele wet moet zijn voorzien. De term «bij of krachtens de wet» laat toe dat lagere regelgeving beperkingen stelt. Ook op grond van het EVRM is een formele wet niet vereist waar het gaat om de voorwaarde dat een inmenging in het privéleven bij wet moet zijn voorzien. Ten slotte bepaalt ook de AVG niet op welk (wets)niveau de verwerkingsgrondslag van de publieke taak moet zijn neergelegd, omdat de verordening uitgaat van een materieel

[13] Kamerstukken II 2021/22, 35 447, nr. 21, blz. 4.

wetsbegrip.[14] Dit betekent dat de gegevensverwerking niet in een formele wet hoeft te worden geregeld, maar dat dit ook mogelijk is door middel van nationale, lagere regelgeving, mits de formele wet daarvoor grondslagen biedt. Het concept-BGS is die lagere regelgeving, waarvoor de WGS de vereiste grondslagen biedt.

Vraag 8 (GroenLinks/PvdA) – transparantie
In zijn advies van 9 november stelt de Autoriteit Persoonsgegevens dat het wetsvoorstel niet bepaalde fundamentele beginselen zoals het transparantiebeginsel in acht neemt. Het is volgens de Autoriteit daarmee te lastig voor burgers om te weten te komen welke informatie over hen bekend is en wordt uitgewisseld. Het corrigeren van mogelijk onjuiste informatie wordt hiermee vrijwel onmogelijk. Zonder transparantie is effectieve rechtsbescherming van burgers niet mogelijk en de Autoriteit Persoonsgegevens waarschuwt zelfs voor «kafkaëske toestanden voor grote aantallen mensen». Ook het College voor de Rechten van de Mens heeft in haar advies aan de Eerste Kamer dit probleem benoemd. De leden van GroenLinks- en de PvdA-fracties maken zich hier zorgen om. Inmiddels is het mede door de toeslagenaffaire duidelijk geworden wat voor verschrikkelijke gevolgen het voor iemand kan hebben als zij op basis van onjuiste aannames als fraudeur of verdachte zonder het te weten op een lijst worden gezet waar ze bovendien niet meer vanaf kunnen komen. Wat zijn de mechanismes die de regering in stelling heeft gebracht om transparantie jegens burgers te garanderen? Waar zijn deze verankerd? Zijn deze voldoende toegankelijk voor burgers? Ook als hierbij het doenvermogen wordt betrokken?

Artikel 5, eerste lid, van de AVG verplicht ertoe om persoonsgegevens te verwerken op een wijze die transparant is (transparantiebeginsel). De AVG, het wetsvoorstel en het concept-BGS kennen verschillende mechanismen om deze transparantie jegens burgers te waarborgen. Allereerst vergroot het wetsvoorstel, samen met de onderliggende amvb, de voorzienbaarheid en daarmee transparantie door de verwerkingen door de samenwerkingsverbanden een duidelijk wettelijk kader te geven. Ten aanzien van de verwerking van persoonsgegevens door de samenwerkingsverbanden is de AVG leidend, en daarin is transparantie het uitgangspunt: artikel 14 van de AVG verplicht de deelnemers van het samenwerkingsverband, als gezamenlijke verwerkingsverantwoordelijken, in beginsel om betrokkenen te informeren over onder andere het feit dat gegevens over betrokkene worden verwerkt en voor welke doeleinden. Dit kan middels individuele berichtgeving of door middel van een privacystatement op de website van de deelnemers en de website van het samenwerkingsverband. Een verdere uitwerking hiervan is vastgelegd in artikel 1.3 van het concept-BGS. De algemene uitzonderingen uit de AVG en de Uitvoeringswet AVG gelden ook voor wat betreft de verwerkingen die plaatsvinden in de samenwerkingsverbanden onder de WGS. Een relevante uitzondering doet zich onder meer voor als het verstrekken van de informatie de doeleinden van de gegevensverwerking zou doorkruisen of bij de doorkruising van opsporings- en toezichtbelangen. Indien deze uitzondering vervalt, bijvoorbeeld na afronding van een gezamenlijk project, moet de informatieplicht alsnog worden nagekomen. In de WGS zijn geen aanvullende uitzonderingsgronden opgenomen.
De transparantie wordt, los van de informatieplicht, ook geborgd doordat het wetsvoorstel samenwerkingsverbanden verplicht om jaarverslagen te

[14] Overwegingen 41 en 45 bij de AVG. Zie ook Afdeling Bestuursrechtspraak Raad van State, 30 juni 2021 (ECLI:NL:RVS:2021:1420): «Die wetgeving moet duidelijk en nauwkeurig zijn en de toepassing daarvan moet voorspelbaar zijn voor degenen op wie deze van toepassing is. Uit deze overwegingen volgt niet dat de noodzaak voor de verwerking moet voortvloeien uit een wet in formele zin».

publiceren met daarin een verantwoording van de effectiviteit en bruikbaarheid van de gegevensverwerking.
Bij geautomatiseerde gegevensanalyse – die bij iCOV aan de orde kan zijn – moet een samenwerkingsverband op eigen initiatief aan het publiek op toegankelijke wijze uitleg geven over gehanteerde patronen, indicatoren en andere onderliggende logica (artikel 1.9, derde lid, WGS). Bij iCOV kan een dergelijke geautomatiseerde gegevensanalyse dus pas plaatsvinden als deze uitleg is gepubliceerd op de website van het samenwerkingsverband.
Verder is voorzien in de aanwijzing van een contactpunt voor elk samenwerkingsverband, waar betrokkenen op toegankelijke wijze hun recht op inzage van hun persoonsgegevens kunnen uitoefenen, evenals hun andere rechten op grond van de AVG, zoals het recht op correctie. In het kader van transparantie en rechtszekerheid richting burgers is het van belang dat er één contactpunt komt dat de behandeling van verzoeken van betrokkenen coördineert en afhandelt. Dit is uitgewerkt in artikel 1.1 van het concept-BGS. Daarin is ook bepaald dat op de website van het samenwerkingsverband de naam en contactgegevens van het contactpunt moeten worden vermeld.

Vraag 9 (D66) – punten van zorg Raad van State
In de brief van 18 november 2021 van de Afdeling Advisering van de Raad van State formuleert de Afdeling op pagina 2 vier bedenkingen tegen het wetsvoorstel.[15] Zou de regering die puntsgewijs kunnen becommentariëren? De leden van de D66-fractie constateren dat het antwoord dat de regering de Eerste Kamer bij brief van 17 december 2021 stuurde, niet alle punten van zorg die de Raad van State heeft geformuleerd, adresseert.

De Afdeling advisering ziet in het wetsvoorstel een belangrijke verbetering in vergelijking met de huidige praktijk.[16] Zij noemt evenwel vier aandachtspunten, die ik hierbij achtereenvolgens van een nadere reactie voorzie, in aansluiting op de brief van 17 december 2021 van de toenmalige Minister van Justitie en Veiligheid:[17]

1. De Afdeling advisering vraagt allereerst aandacht voor de delegatiegrondslagen die het wetsvoorstel bevat met het oog op de introductie van nieuwe samenwerkingsverbanden (artikelen 3.1 en 3.2 WGS). Tegen die achtergrond behoeft het voorliggende wetsvoorstel in elk geval op termijn aanpassing. De Afdeling advisering suggereert om het wetsvoorstel aan te nemen onder de voorwaarde dat op termijn een separaat wetsvoorstel wordt ingediend waarmee de mogelijkheid om bij amvb nieuwe samenwerkingsverbanden te regelen, wordt beperkt tot tijdelijke spoedsituaties (aldus §4a van de voorlichting).
   Reactie:
   Ik neem deze suggestie over, conform het voornemen van mijn ambtsvoorganger.[18] Dit licht ik toe in het hieraan gewijde hoofdstuk 11 van deze memorie van antwoord.
2. Ten tweede stelt de Afdeling advisering dat bij de voorgenomen amvb en in de uitvoering moet worden bezien of en zo ja, op welke wijze aan het doelbindingsbeginsel kan worden voldaan. Wat betreft de Zorg- en Veiligheidshuizen stelt de Afdeling advisering dat nader dient te worden beargumenteerd wat hun plaats binnen de WGS is.
   Reactie:
   Ik onderschrijf in dit verband de stelling van de Afdeling advisering dat een zeker abstractieniveau bij de doelomschrijvingen onvermijdelijk is en dat een zorgvuldige uitvoeringspraktijk cruciaal is omdat in

[15] Kamerstukken I 2021/22, 35 447, H, p. 2.
[16] Kamerstukken I 2021/22, 35 447, H, blz. 1 en 7.
[17] Met name §5.1, 5.2 en 7.1 tot en met 7.3, Kamerstukken II 2021/22, 35 447, nr. 21.
[18] §5.1, Kamerstukken II 2021/22, 35 447, nr. 21.

concrete gevallen telkens zal moeten worden bezien of en op welke wijze aan het doelbindingsbeginsel kan worden voldaan. Daarnaast somt het wetsvoorstel op welke categorieën gegevens mogen worden verwerkt en zijn in het concept-BGS nadere preciseringen voorzien van de gegevensverwerkingen.
De Zorg- en Veiligheidshuizen passen binnen het doel van de WGS. Zorg- en Veiligheidshuizen spelen een belangrijke rol bij het voorkomen van de escalatie van sociale en zorgproblematiek tot het niveau dat jeugdigen en kwetsbare personen afglijden naar onder meer (georganiseerde) criminaliteit, of ernstige gewelddelicten veroorzaken. Dit is nader toegelicht in §5.2 van de Kamerbrief van 17 december 2021.

3. De Afdeling advisering benadrukt, ook waar het gaat om de naleving van artikel 1 van de Grondwet en andere gelijke behandeling- en non-discriminatieregimes, het belang van een zorgvuldige uitvoeringspraktijk, in het bijzonder bij geautomatiseerde gegevensanalyse.
Reactie:
Om de naleving van artikel 1 van de Grondwet en andere gelijke behandeling- en non-discriminatieregimes nog beter te verzekeren, zullen diverse waarborgen worden getroffen. Deze worden opgesomd in antwoord op *vraag 37 (D66) – waarborgen en voorzorgsmaatregelen bij geautomatiseerde gegevensanalyse.* Daarin wordt – onder veel meer – ingegaan op de rol van de rechtmatigheidsadviescommissies bij het tegengaan van risico's op ongelijke behandeling en discriminatie, de verplichte opleiding van medewerkers, het niet-verwerken van gegevens over nationaliteit en de waarborgen bij geautomatiseerde gegevensanalyse, die bedoeld zijn om discriminatie, fouten en vooroordelen tegen te gaan in algoritmen die bij een geautomatiseerde analyse worden gebruikt.
4. De Afdeling advisering stelt dat het voor een zorgvuldige uitvoering in de praktijk van belang is dat wordt geïnvesteerd in professionaliteit en (juridische) deskundigheid op de werkvloer, evenals in een cultuur waarin kan en mag worden afgeweken van algoritmische uitkomsten. Daarnaast zijn afwegingskaders van belang om te bevorderen dat algoritmen zorgvuldig en met respect voor relevante grondrechten tot stand worden gebracht. Ook dienen relevante derde partijen, zoals belangenorganisaties, te worden betrokken bij het ontwerp van algoritmen die een samenwerkingsverband hanteert. Tot slot wijst de Afdeling advisering op het belang van een zorgvuldige evaluatie en terugkoppeling als het gaat om de resultaten van de toepassing van algoritmen.
Reactie:
Ik onderken het belang van de adequate en zorgvuldige uitvoering van de WGS en de daaruit voortvloeiende nadere regelgeving. Daarom wil ik verschillende maatregelen nemen, onder meer op het vlak van opleidingseisen, rechtmatigheidsadviescommissies en privacy audits. Dit laat onverlet dat de samenwerkingsverbanden reeds veel benodigde kennis en expertise hebben opgebouwd. In het antwoord op *vraag 56 (D66) – kwaliteit van de uitvoeringspraktijk* licht ik naar aanleiding van deze aanbeveling van de Afdeling advisering de voorgenomen maatregelen toe ten behoeve van de professionaliteit en (juridische) deskundigheid binnen de samenwerkingsverbanden. Tevens onderken ik – zoals mijn ambtsvoorganger ook heeft gedaan[19] – dat geïnvesteerd moet worden in professionaliteit en (juridische) deskundigheid op de werkvloer, evenals in een cultuur waarin kan en mag worden afgeweken van algoritmische uitkomsten. In het antwoord op *vraag 40 (VVD) – expertise inzake algoritmen en tegengaan ongewenste profilering* beschrijf ik op welke wijze gevolg

[19] Kamerstukken II 2021/22, 35 447, nr. 21, paragraaf 7.3.

wordt gegeven aan de aanbevelingen die de Afdeling advisering in haar voorlichting heeft gedaan ten behoeve van een zorgvuldig gebruik van algoritmen. Dit geschiedt onder meer door middel van afwegingskaders voor het zorgvuldige gebruik van algoritmes.
De Afdeling advisering heeft in haar voorlichting terecht gesteld dat het aangewezen is om relevante derde partijen, zoals belangenorganisaties, te betrekken bij het ontwerp van algoritmen die een samenwerkingsverband hanteert. Ik licht dit toe in antwoord op *vraag 41 (PvdA/GroenLinks) – betrekken van externe partijen bij algoritmen.*
Tot slot onderken ik, met de Afdeling advisering, het belang dat een zorgvuldige evaluatie en terugkoppeling plaatsvindt als het gaat om de resultaten van de toepassing van algoritmen. In antwoord op *vraag 38 (PvdA/GroenLinks) – evaluatie en toezicht geautomatiseerde gegevensanalyse* zijn de diverse terugkoppelings- en evaluatiemechanismen opgesomd, waartoe het wetsvoorstel verplicht.

Vraag 10 (PvdD) – verenigbaarheid met de Grondwet en verdragsbepalingen
De Autoriteit Persoonsgegevens, de Raad van State en het College voor de Rechten van de Mens hebben kritiek op of twijfel over de vraag of het voorstel voldoet aan de eisen die voortvloeien uit de AVG en uit artikel 10 Grondwet en vergelijkbare verdragsbepalingen. Als deze kritiek of twijfel gegrond is, impliceert dit dan dat als het voorstel wordt aangenomen en uitgevoerd, de kans reëel is dat een rechter bepalingen van de WGS of van uitvoeringsmaatregelen onverbindend zal oordelen? Zo nee, op welke juridische redenering wordt die ontkennende beantwoording gegrond, zo vragen de leden van de fractie van PvdD.

Met het wetsvoorstel is een evenwichtig kader gecreëerd dat in overeenstemming is met de AVG, de Grondwet en internationale regelgeving, waarbij mogelijkheden voor gegevensverwerking gepaard gaan met een groot aantal waarborgen ter bescherming van de grondrechten van burgers. Dat deze waarborgen in belangrijke mate worden uitgewerkt bij amvb, is niet in strijd met artikel 10 van de Grondwet. Op grond daarvan is de wetgever immers bevoegd tot delegatie en kan het recht op eerbiediging van de persoonlijke levenssfeer worden beperkt bij of krachtens de wet, wat betekent dat delegatie van beperkingsbevoegdheid naar het niveau van algemene maatregel van bestuur geoorloofd is. Het tweede lid draagt de wetgever op regels te stellen inzake de vastlegging en verstrekking van persoonsgegevens en gezien het gebruik van het woord «regels» is de wetgever ook volgens deze bepaling bevoegd tot delegatie. Overigens wil de regering benadrukken dat de eisen die het geldende gegevensbeschermingsrecht stelt aan de verwerking van persoonsgegevens, onverkort blijven gelden voor de deelnemers van een samenwerkingsverband. Bij alle bevoegdheden tot persoonsgegevensverwerking die de deelnemers van een samenwerkingsverband krijgen op grond van dit wetsvoorstel, moet bij de uitoefening telkens door de deelnemers worden getoetst of de persoonsgegevensverwerking noodzakelijk is met het oog op het doel waarmee zij gezamenlijk gegevens mogen verwerken. Elke separate persoonsgegevensverwerking moet daarnaast voldoen aan de eisen van de AVG.
De Afdeling advisering van de Raad van State heeft in haar voorlichting gesteld dat het wetsvoorstel in beginsel voldoet aan artikel 10 van de Grondwet. Wel rijst volgens de Afdeling advisering de vraag of het wetsvoorstel, in het licht van artikel 10 van de Grondwet een adequate wettelijke grondslag biedt voor de beoogde (vergaande) verwerking door en verstrekking van gegevens aan nieuwe samenwerkingsverbanden die op grond van artikelen 3.1 en 3.2 WGS bij amvb worden aangewezen. De Afdeling advisering heeft gesteld dat daarom die mogelijkheid moet worden beperkt tot tijdelijke spoedsituaties, waarbij de wezenlijke

elementen uiteindelijk alsnog op het niveau van de formele wet worden vastgelegd. De Afdeling advisering heeft als alternatief gesuggereerd om het wetsvoorstel aan te nemen onder de voorwaarde dat een separaat daartoe strekkend reparatiewetsvoorstel op termijn wordt ingediend.[20] In §5.1 van zijn brief van 17 december 2021 heeft de toenmalige Minister van Justitie en Veiligheid geschreven dat hij bereid is om toe te zeggen dat de artikelen 3.1 tot en met 3.3, die de mogelijkheid regelen om nieuwe samenwerkingsverbanden bij amvb te regelen, niet in werking zullen treden, en dat een wetsvoorstel wordt ingediend waarmee die artikelen worden aangepast.[21] Ik ben hiertoe eveneens bereid. Hierop wordt nader ingegaan in §11 van deze memorie van antwoord.

Vraag 11 (CU) – grondrechtelijke aspecten
De leden van de ChristenUnie-fractie stellen met voldoening vast dat het aangepaste wetsvoorstel in de beoordeling van de Raad van State nu in beginsel voldoet aan de eisen van art. 10 van de Grondwet, doordat de belangrijkste beperkingen op de betrokken grondrechten nu in hoofdzaak worden geregeld op het niveau van een formele wet. Dat laat echter onverlet dat grondrechten niet alleen in de Grondwet zijn gecodificeerd. Hoe taxeert de regering de houdbaarheid van dit wetsvoorstel in internationaal grond- en mensenrechtelijk verband?

Op een en ander is ingegaan in het antwoord op de vorige vraag en de memorie van toelichting, in paragraaf 7 («Grondrechtelijke aspecten»).[22]

4. Delen van gegevens en rechtsbescherming

4.1 Rechtsbescherming

Vraag 12 (VVD) – rechten van burgers
Op welke wijze is de rechtsbescherming van burgers voldoende gewaarborgd, zo vragen de leden van de VVD-fractie? Hoe en bij wie kan je verifiëren welke gegevens worden uitgewisseld? Is dit voldoende duidelijk voor burgers? Is duidelijk welke gevolgen de gegevensuitwisseling en verwerking heeft voor de betreffende persoon? Kunnen burgers onjuiste gegevens tijdig en op een eenvoudige manier corrigeren? Zo ja op welke wijze?

Op de verwerking van persoonsgegevens die plaatsvinden onder de gezamenlijke verwerkingsverantwoordelijkheid van deelnemers op grond van de WGS zijn onverkort de rechten en plichten uit de AVG van toepassing. Een betrokkene kan een beroep doen op de rechten die de AVG hem al geeft, zoals het recht op inzage, het recht op rectificatie, het recht op gegevenswissing en het recht op beperking van de verwerking (artikelen 15–18 AVG). Zo kan een betrokkene onder meer verifiëren welke categorieën persoonsgegevens over hem worden uitgewisseld en voor welke doeleinden (artikel 15, eerste lid, onder a en b, AVG).
Ook voor samenwerkingsverbanden die zijn opgenomen in de WGS geldt de informatieverplichting op grond van artikel 14 AVG, die verplicht om betrokkenen bepaalde informatie te verschaffen over de verwerking van hen betreffende persoonsgegevens. Zo raken burgers op de hoogte van het feit dat gegevens over hen worden verwerkt en worden zij ook in staat gesteld om hun rechten te kunnen uitoefenen.
Per samenwerkingsverband zal een contactpunt ingericht worden waar burgers terecht kunnen om hun rechten op grond van de AVG uit te oefenen, zoals hun inzage- en correctierecht. Het contactpunt coördineert

[20] Kamerstukken I 2021/22, 35 447, H, blz. 7 en 9–10.
[21] Kamerstukken II 2021/22, 35 447, nr. 21, blz. 4.
[22] Kamerstukken II 2019/20, 35 447, nr. 3, blz. 35 e.v.

dergelijke verzoeken. In artikel 1.1 van het concept-BGS is per samenwerkingsverband uitgewerkt welke deelnemer het contactpunt vormt. Wie het contactpunt is, moet tevens bekend worden gemaakt op de website van het samenwerkingsverband.
Burgers kunnen bij het contactpunt ook verzoeken om onjuiste gegevens te rectificeren. Dit moet gebeuren door de deelnemende partij die de betreffende gegevens heeft ingebracht. Het contactpunt zal correctieverzoeken coördineren.
Op de verplichtingen en rechten uit de AVG gelden de uitzonderingen uit de AVG en de Uitvoeringswet AVG, zoals beschreven in de memorie van toelichting.[23] Het wetsvoorstel voegt daar geen uitzonderingen aan toe.

Vraag 13 (GroenLinks/PvdA) – herhaling voorkomen van de toeslagenaffaire
Hoe ziet de regering dit wetsvoorstel in het licht van de toeslagenaffaire en het rapport «Ongekend Onrecht», zo vragen de leden van de fracties van GroenLinks en PvdA. Is de regering bereid te wachten op de uitkomst van de parlementaire enquête over dit onderwerp? Zo nee, hoe borgt de regering dat de hierin te maken analyse en aanbevelingen ook zullen gelden voor de hier aan orde zijnde wet? En hoe garandeert de regering dat tot die tijd niet dezelfde schadelijke mechanismes en structuren hun werk doen? Is in de onderhavige wet (wel) geborgd dat onschuldige burgers geen slachtoffer worden van onterechte verdenkingen, disproportionele maatregelen, discriminerende profilering of andere zeer ongewenste (bij)effecten van de wet?

De WGS is er bij uitstek op gericht om gegevensverwerkingen – in dit geval door samenwerkingsverbanden – in goede en rechtmatige banen te leiden. De WGS en het BGS bevatten een reeks belangrijke waarborgen om de bescherming van persoonsgegevens te versterken. Deze waarborgen – weergegeven in het onderstaande schema – hebben grote toegevoegde waarde. Ze vormen een concretisering en aanvulling op de waarborgen uit de AVG. De waarborgen moeten worden gecontroleerd door de inzet van de rechtmatigheidsadviescommissies en de onafhankelijke, periodieke privacy audits. Gegevensverwerking is bovendien uitsluitend toegestaan na duidelijke en objectieve aanwijzingen van risico's in verband met het doel van het samenwerkingsverband. Door naleving van deze kaders, in combinatie met de bepalingen van de AVG, is geborgd dat een herhaling van situaties als bij de toeslagenaffaire wordt voorkomen.
Gelet op de uitgebreide waarborgen in het wetsvoorstel en de amvb wordt geen aanleiding gezien om te wachten op de uitkomst van de parlementaire enquête. Het is van belang om op korte termijn recht te doen aan het belang om de waarborgen te versterken en om de gegevensverwerkingen binnen de in het wetsvoorstel opgenomen samenwerkingsverbanden van een helder wettelijk kader te voorzien. De urgentie bestaat eruit dat het wetsvoorstel de slagkracht van de overheid verbetert bij de aanpak van enerzijds ernstige, ondermijnende vormen van criminaliteit en anderzijds van complexe problemen op het snijvlak van zorg en veiligheid. De urgentie van die aanpak wordt breed gedeeld. Bij de Zorg- en Veiligheidshuizen gaat het bijvoorbeeld om jongeren die geronseld worden door criminele netwerken en langzaam het criminele circuit in worden getrokken. Een Zorg- en Veiligheidshuis biedt dan een persoonsgerichte aanpak op maat om een jongere uit het criminele circuit te trekken en op het rechte spoor te brengen door de samenwerking tussen strafrecht, sociaal domein en zorg te organiseren.
Op dit moment ervaren de samenwerkingsverbanden onduidelijkheid over de bestaande juridische mogelijkheden, wat leidt tot handelingsver-

[23] Kamerstukken II 2019/20, 35 447, nr. 3, blz. 18.

legenheid waar die niet zou hoeven te bestaan. Onder de huidige wetgeving verschilt het bijvoorbeeld per deelnemer of en in welke mate een deelnemer gegevens met het samenwerkingsverband mag delen of van het samenwerkingsverband mag ontvangen. De consequentie hiervan is dat de deelnemers aan een samenwerkingsverband, zelfs als zij ieder voor zich de fragmenten hebben die nodig zijn om de complexe puzzel van de criminaliteitsbestrijding op te lossen, die puzzeldelen nu niet volledig bij elkaar mogen leggen.
Het wetsvoorstel maakt een einde aan deze versnippering van informatie door te zorgen voor heldere juridische grondslagen voor gezamenlijke gegevensverwerking. Dat voorkomt dat samenwerkingsverbanden in een grijs gebied moeten opereren waarvan de grenzen niet altijd helder zijn. Die helderheid stelt de samenwerkingsverbanden in staat effectiever te functioneren. Die duidelijkheid biedt het wetsvoorstel ook inzake de toepasselijke waarborgen en de begrenzing van de gegevensdeling. Ook volgens de Afdeling advisering van de Raad van State – aldus haar advies uit 2019 – is deze rechtszekerheid nodig om als samenwerkingsverband effectief te kunnen functioneren.[24] Zoals de Afdeling advisering van de Raad van State bovendien in haar voorlichting over de WGS terecht opmerkt, is gegevensverwerking onmiskenbaar een belangrijk instrument om ernstige en ondermijnende criminaliteit tegen te gaan: «In die zin vormt niet alleen bescherming van persoonsgegevens, maar ook effectieve misdaadbestrijding rechtsstatelijk handelen.» De Afdeling advisering ziet in het wetsvoorstel een belangrijke verbetering in vergelijking met de huidige praktijk.[25] Randvoorwaardelijk en daarmee eveneens urgent, is volgens de Afdeling advisering wel de adequate en zorgvuldige uitvoering van de WGS en de daaruit voortvloeiende nadere regelgeving. De maatregelen die daarom worden getroffen, worden toegelicht in het antwoord op *vraag 56 (D66) – kwaliteit van de uitvoeringspraktijk*.

Overzicht waarborgen WGS	**Toepasselijke artikelen**
Toezicht en rechtmatigheid	
Rechtmatigheidsadviescommissies voor de structurele beoordeling van nieuwe en gewijzigde verwerkingen en met aandacht voor het tegengaan van discriminatierisico's	Art. 1.8, zesde lid, WGS en art. 1.13, 1.14, 1.15 concept-BGS
Onafhankelijke privacy audits voor rechtmatigheidscontrole, waarvan de resultaten aan de AP moeten worden gezonden	Art. 1.10 WGS en art. 1.18 concept-BGS
Coördinerend functionaris gegevensbescherming	Art. 1.4, tweede lid, WGS
Uitsluitend verstrekking van rechtmatig verwerkte gegevens	Art. 1.5 concept-BGS
Onafhankelijk toezicht en handhaving door de AP i.v.m. naleving WGS, BGS en AVG (o.a. corrigerende maatregelen, bestuursdwang, dwangsom of bestuurlijke boetes)	Art. 6, derde lid, 15, 16, 18 Uitvoeringswet AVG, art. 58 en 83 AVG, art. 5:32 Awb
Dataminimalisatie en opslagbeperking	
Limitatieve opsomming welke categorieën gegevens de deelnemers gezamenlijk mogen verwerken	Art. 2.4, 2.12, 2.22, 2.30 WGS en art. 2.15 concept-BGS
Termijn voor vernietiging of anonimisering van de verwerkte persoonsgegevens: 5 jaar, met beperkte uitzondering	Art. 1.8, zevende lid, WGS en art. 1.16 concept-BGS
Geen gegevens over nationaliteit, met beperkte uitzondering	Art. 1.9 concept-BGS
Doelbinding	
Omschrijving doeleinden samenwerkingsverbanden, telkens met koppeling aan noodzaak voor de taken van deelnemers	Art. 2.2, 2.10, 2.17, 2.25 WGS
Passende organisatorische maatregelen voor doelbinding	Art. 1.8, vijfde lid, WGS

[24] Kamerstukken II 2019/20, 35 447, nr. 4, blz. 7.
[25] Kamerstukken I 2021/22, 35 447, H, blz. 1 en 7.

Overzicht waarborgen WGS	Toepasselijke artikelen
Gegevensverwerking uitsluitend toegestaan na duidelijke en objectieve aanwijzingen van risico's in verband met het doel van het samenwerkingsverband	Art. 2.4, 2.8, 2.11, 2.16 en 2.20 concept-BGS
Verstrekking resultaten mag alleen voor verenigbaar doel	Art. 1.7 WGS
Kwaliteit en juistheid	
Plicht tot opleidingen en trainingen over gegevensverwerking	Art. 1.17 concept-BGS
Verplichting om zorg te dragen voor juiste persoonsgegevens	Art. 5, eerste lid, onder a, AVG
Verplichting voor deelnemer om de bij een signaal, verzoek of casus te verstrekken gegevens vooraf te toetsen op juistheid en kwaliteit	Artikel 1.6 concept-BGS
Verantwoordelijkheidsverdeling voor correctie onjuistheden en terugmeldingsplicht van onjuistheden aan de bronhouder	Art. 1.7 concept-BGS
Verplichting tot toetsen feitelijke juistheid en kwaliteit van gegevens die bij het resultaat worden verstrekt	Art. 1.8, eerste lid, concept-BGS
Motiveringsplicht op basis van welke informatie sturingsinformatie of een interventieadvies tot stand komt	Art. 1.8, tweede lid, concept-BGS
Verplichting om de resultaten periodiek te evalueren op bruikbaarheid en effectiviteit	Art. 1.7, vierde en vijfde lid, WGS
Integriteit en vertrouwelijkheid	
Verplichting tot adequaat beveiligingsniveau	Art. 32 AVG
Vereisten aan de screening van medewerkers	Art. 1.8, derde lid, WGS en art. 1.11 concept-BGS
Binding aan Baseline Informatiebeveiliging Overheid (BIO)	Art. 1.8, achtste lid, WGS
Limitatieve omschrijving van degenen die autorisaties krijgen tot de systemen	Art. 1.8, tweede lid, WGS
Plicht tot periodieke beoordeling van de autorisaties	Art. 1.8, achtste lid, WGS en §9.2.5, 9.2.5.2 en 9.2.5.3 BIO
Verplichting tot logging, zodat controleerbaar is of de gegevensverwerking rechtmatig is, onder meer in de audits.	Art. 1.8, vierde lid, WGS en art. 1.12 concept-BGS
Geheimhoudingsplicht	Art. 1.11 WGS
Aanwijzing contactpunt voor nakoming meldplicht datalekken	Art. 1.3 concept-BGS
Transparantie	
Informeren betrokkene over gegevensverwerking	Art. 14 AVG
Een contactpunt dat betrokkenen informeert	Art. 1.3 concept-BGS
Jaarverslag van het samenwerkingsverband, met daarin een verantwoording van de effectiviteit en bruikbaarheid van de gegevensverwerking	Art. 1.12 WGS
Rechtsbescherming	
Aanwijzing van een contactpunt binnen het samenwerkingsverband waar betrokkenen hun rechten op grond van hoofdstuk III AVG kunnen uitoefenen, zoals verzoeken om inzage, correctie of gegevenswissing	Art. 1.4, vierde lid, WGS en art. 1.2 concept-BGS
Mogelijkheid bezwaar/beroep tegen besluit van contactpunt op AVG-verzoek (doeltreffende voorziening in rechte)	Art. 1.2 concept-BGS, art. 34 Uitvoeringswet AVG, hfd. 8 Awb en art. 79 AVG
Mogelijkheid van een klacht bij de AP (handhavingsverzoek)	Art. 77 AVG
Aanvullende waarborgen bij geautomatiseerde gegevensanalyse	
Plicht tot adequate, uniforme technische en organisatorische maatregelen voor de kwaliteit, juistheid en volledigheid	Art. 1.9, eerste lid, WGS
Verplichting tot menselijke tussenkomst vóórdat een resultaat van de analyse wordt verstrekt, waarbij het wordt getoetst op zorgvuldigheid van wijze van totstandkoming	Art. 1.9, tweede lid, WGS
Verplichting tot uitleg over gehanteerde patronen, indicatoren of andere onderliggende logica	Art. 1.9, derde lid, WGS
Verplichting tot pseudonimisering	Art. 1.9, vijfde lid, WGS en art. 2.12 concept-BGS
Verbod op algoritmes waarvan de uitkomsten niet navolgbaar en controleerbaar zijn	Art. 1.9, zesde lid, WGS
Nadere waarborgen geautomatiseerde gegevensanalyse iCOV	Art. 2.9 – 2.12 concept-BGS

Vraag 14 (PVV) – herhaling voorkomen van de toeslagenaffaire
Op welke manier is bij dit wetsvoorstel lering getrokken uit het afschuwelijke debacle van de toeslagenaffaire, waarbij de levens van veel mensen zijn verwoest, zo vragen de leden van de fractie van PVV.

Verwezen wordt naar het antwoord op de vorige vraag.

Vraag 15 (D66) – rechtsbescherming
Kan de regering aangeven welke mogelijkheden burgers hebben om tegen de verwerking van hun persoonsgegevens door de samenwerkingsverbanden in het geweer te komen? Het gaat hierbij veelal om informatie over burgers waarvan ze zelf niet eens weten dat die bestaat, laat staan dat deze data worden uitgewisseld en gecombineerd met data van andere organisaties. Dat kan het voor de burgers heel moeilijk maken om een beslissing die daar uit voorkomt aan te vechten. Over het antwoord op deze vraag is het wetsvoorstel volgens de leden van de D66-fractie niet helder.

Zoals is geantwoord op *vraag 12 (VVD) – rechten van burgers*, zijn op het wetsvoorstel onverkort de rechten en plichten uit de AVG van toepassing, zo ook de informatieverplichting op grond van artikel 14 AVG. Op grond hiervan raken burgers op de hoogte van de verwerking van persoonsgegevens en worden zij ook in staat gesteld om hun rechten te kunnen uitoefenen. Zoals in de amvb nader wordt uitgewerkt, is het contactpunt verantwoordelijk voor de nakoming van de informatieplicht en voor het nemen van besluiten op verzoeken van betrokkenen tot uitoefening van hun rechten op grond van de AVG. Het contactpunt moet voorafgaand aan het nemen van een besluit overleggen met de andere gezamenlijke verwerkingsverantwoordelijken, in ieder geval met degenen die de persoonsgegevens hebben verstrekt of als resultaat hebben ontvangen. Indien een betrokkene het niet eens is met het besluit op zijn verzoek, dan kan diegene terecht bij het contactpunt voor bezwaar en vervolgens bij de bestuursrechter voor beroep. Immers, de schriftelijke beslissing van een bestuursorgaan (het contactpunt) op een dergelijk verzoek is een besluit in de zin van de Algemene wet bestuursrecht volgens artikel 34 van de Uitvoeringswet AVG. Dit betekent dat bestuursrechtelijke rechtsbescherming openstaat.
Daarnaast geldt dat wanneer een deelnemer na de gezamenlijke gegevensverwerking beslist om een interventie te plegen, daartegen de gebruikelijke rechtsbescherming bestaat die van toepassing is bij besluiten of strafrechtelijke handhaving. Voor de goede orde wordt opgemerkt dat de beslissingen over een interventie niet genomen worden door het samenwerkingsverband, maar pas in de interventiefase door een individuele deelnemer, die voorafgaand aan de interventie ook nog zelfstandig feitenonderzoek moet doen. De informatie vanuit het samenwerkingsverband kan slechts als aanleiding dienen.

Vraag 16 (CU) – rechtsbescherming
Een wezenlijk onderdeel wat deze leden betreft is de rechtsbescherming. Hoe krijgt die in concreto vorm en inhoud?

Verwezen wordt naar het antwoord op vraag 15 (D66) over rechtsbescherming.

Vraag 17 (PvdD) – rechtsbescherming
In hoeverre is het voor een individuele burger mogelijk om te verifiëren welke gegevens er over hem of haar worden uitgewisseld, waar deze informatie terechtkomt en welke gevolgen dat kan hebben voor die persoon? Zo ja, op welke wijze? Zo nee, behoren uit een oogpunt van bescherming van grondrechten dan niet alsnog voorzieningen in de wet te worden opgenomen die de mogelijkheid wel creëren? In artikel 1.9 WGS, eerste lid is een zorgplicht opgenomen. Kan een burger daaraan een aanspraak ontlenen? Zo nee, verdraagt zich het ontbreken van waarborgen en aanspraken voor de burger op dit punt zich met het grondrecht op bescherming van persoonsgegevens?

Verwezen wordt naar het antwoord op vraag 15 (D66) over rechtsbescherming.

Vraag 18 (PvdA/GroenLinks) – overleg met de rechtspraak over rechtsbescherming
Is er met de voor deze wet relevante onderdelen van de rechtspraak overleg geweest over de vraag wat er nodig is om de rechtsbescherming op een volwaardige wijze vorm te geven?

Het wetsvoorstel stond open voor (internet)consultatie van 6 juli tot 20 september 2018. De reactie van de Nederlandse Vereniging voor Rechtspraak (NVvR) is vanzelfsprekend bij het uiteindelijke wetsvoorstel betrokken. Nader overleg heeft niet plaatsgehad. In de consultatie op het concept-BGS staat ook voor de NVvR de mogelijkheid open om te reageren.

4.2 Verwerkte categorieën persoonsgegevens

Vraag 19 (PvdD) – soorten gegevens die worden verwerkt door de RIEC's
In paragraaf 3.1 van zijn advies verwijst de Autoriteit Persoonsgegevens naar de ernst van de inbreuk op het privéleven door op te sommen welke persoonsgegevens de RIEC's mogen verwerken. De Autoriteit Persoonsgegevens stelt: «Eigenlijk is er nauwelijks een gegeven te bedenken dat er niet onder valt. Het gaat daarbij bovendien niet alleen om de gegevens van de betrokkene zelf, maar ook van mensen in een directe kring van de betrokkene.» [26]
Kloppen deze twee constateringen van de Autoriteit Persoonsgegevens, zo vragen de leden van de PvdD-fractie. Kan de regering vijf tot tien andere persoonsgegevens noemen waarvoor dan geldt dat zij niet onder de bijna twintig in artikel 2.22, eerste lid WGS genoemde gegevens vallen en dus niet door RIEC's zouden mogen worden verwerkt?

Voorbeelden van persoonsgegevens die niet door de RIEC's mogen worden verwerkt zijn arbeidsgegevens, onderwijsgegevens, gegevens over gezondheid, zorgverzekeringsgegevens, persoonsgegevens waaruit ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische gegevens en biometrische gegevens.
Voor de categorieën persoonsgegevens die volgens artikel 2.22, eerste lid, WGS wel mogen worden verwerkt door de RIEC's geeft artikel 2.15 van het concept-BGS een concretisering. De leverende deelnemers moeten in het concrete geval afwegen welke persoonsgegevens precies noodzakelijk zijn om beschikbaar te stellen om een goede invulling te kunnen geven aan de doelstelling van de RIEC's. 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.

Vraag 20 (D66) – verwerking bijzondere persoonsgegevens in RIEC inzake mensenhandel
Op pagina 37 van het wetgevingsoverleg in de Tweede Kamer stipuleert de regering: «Er worden geen gegevens verwerkt over nationaliteit, ras of etnische afkomst.» [27] De leden van de fractie van D66 begrijpen in dat licht niet waarom artikel 2.21 lid 1 WGS dan de bevoegdheid geeft persoonsgegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid te verwerken.

---

[26] Kamerstukken I 2021/22, 35 447, G, p. 11.
[27] Kamerstukken II 2020/21, 35 447, nr. 20, p. 37.

Wat is hiervan de logica? Dezelfde vraag over artikel 2.22 lid 1 onder 2 WGS. De regering zegt op pagina 29 van het wetgevingsoverleg dat het samenwerkingsverband Regionale Informatie- en Expertisecentra (RIEC) die gegevens mag verwerken als het gaat om mensenhandel en gedwongen prostitutie.[28] Dit begrijpen de D66-fractieleden niet. Geen gegevens over nationaliteit, maar wel over seksuele gerichtheid bij mensenhandel?

Volgens artikel 2.17 van het wetsvoorstel houdt de gegevensverwerking in een RIEC verband met de bestrijding van georganiseerde criminaliteit. Een van deze vormen van criminaliteit is mensenhandel. Zoals gesteld in de memorie van toelichting[29] en de nota naar aanleiding van het verslag[30] bij de WGS, is het voor het doel van de RIEC's noodzakelijk om bijzondere persoonsgegevens over seksueel gedrag of seksuele gerichtheid te kunnen verwerken. Daarbij is erop gewezen dat bij de aanpak van mensenhandel in RIEC-verband namelijk ook onderzoeken plaatsvinden naar illegale prostitutie en uitbuiting, waarbij gegevens over seksueel gedrag en seksuele gerichtheid verwerkt (moeten) worden. Artikel 2.15 van het concept-BGS verduidelijkt dat het uitsluitend gaat om persoonsgegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid wanneer de verwerking noodzakelijk is voor onderzoeken in het kader van bestrijding van mensenhandel, illegale prostitutie en uitbuiting, in aanvulling op de verwerking van persoonsgegevens van strafrechtelijke aard. Hiermee wordt deze gegevenscategorie uit artikel 2.21 WGS scherper afgebakend en in overeenstemming gebracht met datgene wat volgens artikel 23, onder c, van de Uitvoeringswet AVG reeds is toegestaan.

Wat betreft de verwerking van nationaliteit: zoals aangegeven in de Kamerbrief van 17 december 2021,[31] en tijdens het wetgevingsoverleg in de Tweede Kamer over de WGS,[32] 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 artikel 1.9 van het concept-BGS wordt hetzelfde geregeld voor persoonsgegevens inzake nationaliteit. Dit betekent dat de samenwerkingsverbanden geen persoonsgegevens over nationaliteit mogen verwerken, tenzij dit voor de identificatie van betrokkene onvermijdelijk is. Dit is relevant voor de reikwijdte van de term «identificerende gegevens» in de artikelen 2.4, eerste lid, onder a, 2.12, eerste lid, onder a, 2.22, eerste lid, onder a, en 2.30, eerste lid, onder a, WGS. Voor andere doeleinden dan de identificatie van de betrokkene is de verwerking van persoonsgegevens over nationaliteit niet toegestaan.

Vraag 21 (PvdD) – geen onrechtmatige gegevens
Waarom is niet in artikel 1.5 WGS geregeld dat verstrekking van gegevens die niet rechtmatig zijn verkregen, verboden is, zo vragen de leden van de PvdD-fractie.

---

[28] Kamerstukken II 2020/21, 35 477, nr. 20. p. 29.
[29] Kamerstukken II 2019/20, 35 447, nr. 3, blz. 97.
[30] Kamerstukken II 2020/21, 35 447, nr. 6, blz. 128.
[31] Kamerstukken 2021/22, 35 447, nr. 21, paragraaf 7.1.
[32] Kamerstukken 2020/21, 35 447, nr. 20, blz. 37.

Gegevensverstrekkingen door de deelnemers aan een samenwerkingsverband in de zin van de WGS moeten voldoen aan het gegevensbeschermingsrecht. Een van de vereisten daarin is dat de verwerking rechtmatig is. Dit volgt uit artikel 5, eerste lid, onder a, AVG, artikelen 3, derde lid, en 39c, tweede lid, Wet justitiële en strafvorderlijke gegevens en artikel 3, tweede lid, Wet politiegegevens. Een verstrekking aan het samenwerkingsverband van onrechtmatig verwerkte gegevens voldoet niet aan die norm en is dus reeds vanwege het gegevensbeschermingsrecht niet toegestaan. Dit is buiten twijfel gesteld in artikel 1.5 van het concept-BGS.

Vraag 22 (CU) – gekleurde datasets en correctie van onjuiste gegevens
Onder meer het College voor de Rechten van de Mens waarschuwt voor het gebruik van zogenoemde «gekleurde datasets». Kan de regering de leden van de ChristenUnie-fractie aangeven hoe daar in de bestaande praktijk mee wordt omgegaan en hoe bij de uitvoering van dit wetsvoorstel voorkomen kan worden dat dergelijke gekleurde datasets tot onwenselijke resultaten gaan leiden? Tot slot vernemen de leden van de ChristenUnie fractie graag hoe controle en zo nodig correctie van onjuiste gegevens vorm krijgen.

Artikel 1.6 van het concept-BGS bevat waarborgen voor de kwaliteit van een aangemeld signaal, verzoek of casus. Artikel 1.7 bevat waarborgen ten behoeve van de correctie van onjuistheden tijdens gezamenlijke gegevensverwerking. Artikel 1.8 van het concept-BGS bevat regels over de kwaliteit en navolgbaarheid van de resultaten.
Artikel 1.9 van het wetsvoorstel bevat waarborgen om fouten en vooroordelen tegen te gaan in gezamenlijke geautomatiseerde gegevensanalyse. Het betreft in de eerste plaats de verplichting voor de deelnemers om voor adequate en uniforme technische en organisatorische maatregelen zorg te dragen die de kwaliteit van de gezamenlijke geautomatiseerde gegevensanalyse en de juistheid en de volledigheid van de te verwerken gegevens bevorderen. In de tweede plaats de verplichting om een resultaat van een gezamenlijke geautomatiseerde gegevensanalyse uitsluitend aan een deelnemer of derde te verstrekken na menselijke tussenkomst waarbij wordt beoordeeld of het resultaat op zorgvuldige wijze tot stand is gekomen. Verder speelt in het kader van de te betrachten zorgvuldigheid bij iCOV het Kwaliteitskader Big Data[33] een rol, dat is opgesteld door de politie en het OM. Dit wordt gebruikt voor het toetsen van big data toepassingen aan onder andere rechtmatigheid en ethiek. Hierin komen onder meer terug de richtlijnen voor het toepassen van algoritmes door de overheid uit de brief van 8 oktober 2019.[34] Het kwaliteitskader ziet op de ontwikkeling en toepassing van algoritmes en data-analysemethoden in de opsporing.

4.3 Opslagbeperking

Vraag 23 (PVV) – motivering maximale bewaartermijn
De leden van de PVV-fractie lezen op pagina 2 van de brief van 17 december 2021 het volgende: «Zo moeten er periodieke onafhankelijke privacy audits worden gehouden, waarvan de resultaten aan de Autoriteit Persoonsgegevens moeten worden gezonden. Ook valt onder meer te denken aan de verplichte rechtmatigheidsadviescommissies, de loggingsplicht, de maximale bewaartermijn van vijf jaar, de jaarverslagleggingsplicht, de beperking op het aantal autorisaties, en nadere criteria op met

[33] Kamerstukken II 2019/20, 29 628, nr. 948, bijlage «Kwaliteitskader Big data».
[34] Kamerstukken II 2018/19, 29 628, 641.

name het gebied van betrouwbaarheid en kwaliteit van de signalen.» [35] *Waarom is gekozen voor een maximale bewaartermijn van vijf jaar?*

Volgens artikel 1.8, zevende lid, WGS moeten persoonsgegevens die door het samenwerkingsverband worden verwerkt, worden vernietigd of geanonimiseerd zodra zij niet langer noodzakelijk zijn voor het doel van het samenwerkingsverband en moeten de persoonsgegevens in ieder geval uiterlijk vijf jaar na de datum van eerste verwerking worden verwijderd uit de systemen van het samenwerkingsverband of worden geanonimiseerd. De RIEC's kennen nu al een termijn van 5 jaar[36] en binnen het FEC gelden, afhankelijk van het soort informatie, termijnen van 2 of 5 jaar.[37] Binnen iCOV werden de rapportages voorheen maximaal 8 jaar bewaard, nu vijf jaar.[38] Met de voorgestelde termijn van ten hoogste vijf jaar is een balans gevonden tussen enerzijds het optimale gebruik van reeds verzamelde gegevens en anderzijds de proportionaliteit. Gegevens kunnen tot 5 jaar nog steeds relevant zijn voor het doel van het samenwerkingsverband. Daarna is de kans gering dat zij nog een zinvolle rol vervullen. Dat de termijn *maximaal* 5 jaar is, betekent dat al eerder dient over te worden gegaan tot verwijdering wanneer de verwerking reeds eerder niet meer noodzakelijk is.

Vraag 24 (D66) – uitzonderingen op maximale bewaartermijn
Een ander voorbeeld is het belangrijke onderdeel van de bewaartermijn van de verkregen gegevens. Artikel 1.8 lid 7 WGS stelt daarover dat gegevens na uiterlijk vijf jaar worden verwijderd, tenzij een wettelijk voorschrift daaraan in de weg staat, tenzij noodzakelijk voor een rechtsvordering of, in bijzondere gevallen,....»voor zover dat (bewaren) noodzakelijk is voor het doel van het samenwerkingsverband.» Betekent dit niet gewoon dat de privacy-gevoelige gegevens van burgers gewoon altijd bewaard kunnen worden (en verwerkt), zo vragen de leden van de D66-fractie.

Voor het antwoord op deze vraag wordt verwezen naar het antwoord op *vraag 26 (PvdD) – uitzonderingen op maximale bewaartermijn*. Zoals hieruit blijkt, zijn in artikel 1.16 van het concept-BGS de bijzondere gevallen gepreciseerd en kan hernieuwde verwerking zich alleen voordoen bij de Zorg- en Veiligheidshuizen.

Vraag 25 (D66) – uitzonderingen op maximale bewaartermijn
Volgens artikel 1.8 onder 7 WGS worden de gegevens na verloop van tijd vernietigd of uit de systemen gehaald. Zijn er echt geen uitzonderingen op deze regel, zo vragen de leden van de fractie van D66. Bijvoorbeeld wanneer wetenschappelijk onderzoek wordt gedaan naar een bepaald persoon, groep of fenomeen en een lange terugkijkperiode van belang is.

Artikel 5, eerste lid, onder b, AVG biedt de mogelijkheid om ten behoeve van wetenschappelijk onderzoek en statistiek persoonsgegevens te verwerken. De verwerking vindt dan niet plaats op grond van de WGS en valt buiten de reikwijdte van de bewaartermijn uit de WGS. Deze mogelijkheid uit de AVG houdt in dat verwerking van gegevens voor wetenschappelijke en statistische doeleinden als niet onverenigbaar wordt beschouwd met het oorspronkelijke doel waarvoor de desbetreffende gegevens zijn verzameld. Ook geldt bij verwerking van persoonsgegevens ten behoeve van wetenschappelijk onderzoek of statistiek niet het verbod

---

[35] Kamerstukken II 2021/22, 35 447, nr. 21, p. 2.
[36] Zie artikel 17, tweede lid, Privacyprotocol RIEC's-LIEC 2021.
[37] Zie Bijlage B bij het Informatieprotocol FEC 2019, blz. 9.
[38] Zie iCOV privacy statement, https://icov.nl/wp-content/uploads/2021/03/PrivacyStatementiCOVnieuw.pdf

om bijzondere categorieën van persoonsgegevens te verwerken, mits is voldaan aan de voorwaarden van artikel 24 Uitvoeringswet AVG.[39] Hetzelfde geldt met betrekking tot de verwerking van strafrechtelijke gegevens.[40] Mocht de maximale bewaartermijn worden overschreden, dan hoeven volgens artikel 1.8, zevende lid, van het wetsvoorstel de persoonsgegevens niet te worden vernietigd indien zij worden geanonimiseerd.

Vraag 26 (PvdD) – uitzonderingen op maximale bewaartermijn
De slotzin van het zevende lid [van artikel 1.8 WGS] *spreekt over «persoonsgegevens die worden bewaard». Moet hieruit worden afgeleid dat persoonsgegevens die voor verwerking door een samenwerkingsverband zijn aangeboden door een deelnemer langer dan vijf jaar mogen worden bewaard? Wat wordt met «bijzondere gevallen» bedoeld? Kan de regering daar voorbeelden van geven? Levert een situatie dat een deelnemer of een samenwerkingsverband het nodig vindt om eerder verwerkte gegevens samen met nieuwe gegevens te verwerken omdat de verwachting bestaat dat resultaten worden verkregen die in het belang zijn van het samenwerkingsverband, een «bijzonder geval op»?*

De bijzondere gevallen waarin hernieuwde verwerking mogelijk is zullen worden geregeld in het BGS.[41] Verwezen wordt naar artikel 1.16 van het concept-BGS. De bijzondere gevallen zijn daarin beperkt tot de Zorg- en Veiligheidshuizen, voor zover daarbij sprake is van – kort samengevat – complexe problematiek waarbij lange tijd ondersteuning nodig is om tot een duurzame oplossing te komen, of waarbij een groot risico bestaat op terugval waardoor weer zou worden voldaan aan de criteria voor het in behandeling nemen van een casus. Te denken valt aan personen bij wie sprake is van chronische psychische 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. In de toelichting op artikel 1.16 is een uitgebreide motivering opgenomen.
In het door de leden van de PvdD-fractie geschetste voorbeeld is geen sprake van een bijzonder geval waarin hernieuwde gegevensverwerking gerechtvaardigd is. Dit voorbeeld valt niet onder de uitputtend opgesomde categorieën bijzondere gevallen uit artikel 1.16 van het concept-BGS.

4.4 Gegevensdeling met private partijen of derden

Vraag 27 (D66) – deelname private partijen
Daar komt bij dat de beperkingen die wél in de wet zelf zijn opgenomen ook bepaald niet robuust kunnen worden genoemd. Deze bevatten regelmatig nogal vage formuleringen, constateren de leden van de D66-fractie. Zie bijvoorbeeld artikel 1.3 lid 3 WGS, waarin ten aanzien van het aanwijzen van een private partij als deelnemer staat opgenomen dat dit kan «indien het doel van het samenwerkingsverband redelijkerwijs niet kan worden bereikt zonder deelname van deze private partij (...)». Zal dat in de praktijk niet gewoon betekenen dat een private partij in feite altijd

---

[39] Zie artikel 9, tweede lid, onder j, AVG en artikel 24 UAVG.

[40] Zie daarover artikel 32, onder f, UAVG. Zie voorts artikel 33, eerste lid, onder a, UAVG, op grond waarvan het verbod van verwerking van strafrechtelijke persoonsgegevens niet geldt, indien de verwerkingsverantwoordelijke de gegevens heeft verkregen krachtens de Wpg of de Wjsg. Dat geldt ook voor verkrijging van gegevens die op grond van artikel 22 Wpg, artikel 15 Wjsg of artikel 39g Wjsg voor wetenschappelijk onderzoek en statistiek zijn verstrekt.

[41] Dit is ook aangekondigd in de brief van Minister van JenV van 17 december 2021 aan de Tweede en Eerste Kamer in reactie op de aanbeveling van de AP: Kamerstukken II 2021/22, 35 447, nr. 21, bijlage, punt 8.

kan worden toegevoegd als dat vanuit de publieke deelnemers van het samenwerkingsverband nodig, wenselijk of gewoon handig wordt gevonden? Nog los van de vraag wie hierop gaat toezien (daarover hieronder meer) is het immers vrijwel onmogelijk om achteraf te gaan bewijzen dat het doel redelijkerwijs wél had kunnen worden bereikt zónder deelneming van de private partij. Graag een reactie van de regering.

Artikel 1.3, derde lid, WGS is een *randvoorwaarde* voor aanwijzing van private partijen als deelnemer, maar biedt geen *grondslag* voor samenwerkingsverbanden om zelf private partijen toe te voegen. De deelnemers aan de samenwerkingsverbanden zijn de bij of krachtens de WGS aangewezen overheidsinstanties, overheidsorganen en private partijen, aldus artikel 1.3, eerste lid, WGS. Indien (al dan niet private) deelnemers worden toegevoegd bij amvb, moet zowel een voorhangprocedure als een bijzondere nahangprocedure worden gevolgd, als gevolg van het amendement-Kuiken[42] en het amendement-Van Nispen[43]. Dit is opgenomen in de artikelen 2.3, 2.11, 2.19 en 2.27 WGS. Dit bewerkstelligt dat uw Kamer tweemaal de kans krijgt om zich uit te spreken over de aanwijzing van nieuwe (al dan niet private) deelnemers bij amvb, en een dergelijke aanwijzing kan tegenhouden. In het concept-BGS worden alleen bij het FEC private deelnemers toegevoegd (artikel 2.2), om te zorgen dat de private partijen die nu al in het FEC participeren dat kunnen blijven doen. Dit betreft bij ministeriële regeling aan te wijzen banken, waarmee publiek-private samenwerking nodig is ten behoeve van 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. Voor een nadere toelichting op de beperkingen voor deelname van private partijen wordt verwezen naar het antwoord uit deze memorie van antwoord op *vraag 29 (SGP) – gegevens delen met private partijen* en naar het antwoord op vraag 69 van de D66-fractie in de nota naar aanleiding van het verslag.[44]

Vraag 28 (D66) – verstrekkingen aan derde partijen
Volgens o.a. artikel 1.7 WGS kunnen verwerkte gegevens aan een derde worden verstrekt. Dit kunnen dus zeer persoonlijke en gevoelige gegevens zijn. Graag verzoeken de leden van de D66-fractie de regering per samenwerkingsveld een paar voorbeelden van zulke derden te noemen die voor een dergelijke gegevensoverdracht in aanmerking kunnen komen.

Het voorgestelde artikel 1.7 stelt de eis dat de resultaten van de gezamenlijke verwerking uitsluitend aan deelnemers of derden worden verstrekt voor doelen die verenigbaar zijn met de doelen van het desbetreffende samenwerkingsverband. Voor wat betreft de toetsing van de vraag of het doel van de ontvanger verenigbaar is met het doel van het samenwerkingsverband, kan worden aangesloten bij de criteria die artikel 6, vierde lid, onder a tot en met e, AVG, geeft voor de afweging of er sprake is van verdere verwerking voor een verenigbaar doel. Dit betekent dat verstrekking aan een derde afhangt van onder meer het verband tussen het doel van het samenwerkingsverband en het doel van de derde, de

[42] Kamerstukken II 2020/21, 35 447, nr. 18 (amendement-Kuiken over een voorhangprocedure voor de aanwijzing bij amvb van nieuwe deelnemers aan de samenwerkingsverbanden).
[43] Kamerstukken II 2020/21, 35 447, nr. 11 (amendement-Van Nispen over een mogelijkheid voor het parlement om een uitbreiding van een samenwerkingsverband vooraf goed of af te keuren).
[44] Kamerstukken II 2020/21, 35 447, nr. 6, antwoord 69, blz. 55–57.

gevoeligheid van de persoonsgegevens, de mogelijke gevolgen voor de betrokkenen en het bestaan van passende waarborgen.
Verstrekking aan een derde is uitsluitend mogelijk na toetsing van de verstrekking door de rechtmatigheidsadviescommissie en op voorwaarde dat geen deelnemer bezwaar heeft tegen verstrekking (artikel 1.7, tweede lid, aanhef, WGS). De verstrekking van bijzondere categorieën persoonsgegevens en persoonsgegevens van strafrechtelijke aard aan derden, vindt alleen plaats na instemming van de deelnemer die deze gegevens aan het samenwerkingsverband heeft verstrekt (artikel 1.7, derde lid, WGS). Deze bepalingen voorkomen dat persoonsgegevens in strijd met het doel van het desbetreffende samenwerkingsverband worden verwerkt, vrijgegeven of te breed verspreid raken.

Deze voornoemde voorwaarden maken het lastig om in zijn algemeenheid voorbeelden te geven, omdat de afweging of verstrekking aan een derde mag, sterk zal afhangen van de concrete omstandigheden van het geval. Het gaat hierdoor hooguit om verstrekkingen op incidentele basis.
ICOV kent momenteel geen verstrekkingen aan derden. Zoals opgemerkt in de memorie van toelichting, staat het huidige juridische kader waarbinnen iCOV werkt, niet toe dat er informatie wordt gedeeld met derden, terwijl dat juist noodzakelijk kan zijn om een integraal beeld van een casus of problematiek te verkrijgen.[45]
Bij FEC zijn verstrekkingen mogelijk onder voornoemde voorwaarden uit artikel 1.7 WGS en artikel 6, vierde lid, AVG. Hierbij valt te denken aan een incidentele verstrekking aan een gemeente in het kader van het FEC Programma Buitenlandse Financiering wanneer een interventie door die gemeente passender is dan interventie door een deelnemer aan het FEC, bijvoorbeeld door een vergunning te weigeren.[46]
Voor de RIEC's geldt hetzelfde; er wordt nu in beginsel geen informatie met derden gedeeld, maar onder de WGS kan dit – afhankelijk van het geval – incidenteel denkbaar zijn met bijvoorbeeld (lucht)havenbedrijven, DNB of Royal Flora Holland (tegengaan van meeliften door de illegale economie).
Bij de Zorg- en Veiligheidshuizen kunnen derden op incidentele basis deelnemen aan casusoverleggen. Het gaat dan om partijen die actief zijn op uiteenlopende gebieden zoals huisvesting, zorg, maatschappelijke opvang, jeugdhulp, crisisopvang, woonbegeleiding, beschermd wonen, begeleiding bij geestelijke of licht verstandelijke beperkingenproblematiek, maatschappelijk werk, slachtofferzorg en huisartsenzorg, alsmede curatoren, bewindvoerders of mentoren (zie nader artikel 2.21 van het concept-BGS).

Vraag 29 (SGP) – gegevens delen met private partijen
De leden van de SGP-fractie lezen dat het wetsvoorstel mogelijkheden biedt om de resultaten van gegevensverwerking te delen met derden, waaronder private partijen. De leden van de SGP-fractie lezen dat als waarborg is opgenomen dat de verstrekking vooraf door een in te stellen rechtmatigheidsadviescommissie moet zijn getoetst en dat verstrekking noodzakelijk moet zijn voor de behartiging van de gerechtvaardigde belangen of uitvoering van wettelijke verplichtingen van deze private derde. De leden van de SGP-fractie constateren dat behartiging van de gerechtvaardigde belangen een vrij algemene term is die private partijen

[45] Kamerstukken II 2019/20, 35 447, nr. 3, blz. 83.
[46] Dit is sinds 2019 structureel onderdeel van het FEC Programma Terrorismefinanciering. De activiteiten van het Programma Buitenlandse Financiering zijn gericht op het in kaart brengen van de (van origine) buitenlandse financiering van non-profit instellingen waarvan één of meerdere betrokken partijen direct of indirect in verband kunnen worden gebracht met terrorisme of de financiering daarvan.

ruim in kunnen vullen. Is de regering voornemens nadere kaders te geven ter invulling van deze gerechtvaardigde belangen?

Het gaat hierbij om de behartiging van gerechtvaardigde belangen in de zin van artikel 6, eerste lid, onder f, van de AVG. Een belangrijke randvoorwaarde is dat de resultaten van de gegevensverwerking door het samenwerkingsverband uitsluitend mogen worden gebruikt voor doeleinden die verenigbaar zijn met het doel van het samenwerkingsverband (artikel 1.7 WGS, tweede lid, aanhef en onder b). Zoals toegelicht in de nota naar aanleiding van het verslag, is hiervan doorgaans uitsluitend sprake indien de private partij een publiek belang behartigt, bijvoorbeeld door publiek-private samenwerking om criminaliteit aan te pakken.[47] Daarbij is opgemerkt dat commerciële doeleinden daarentegen onverenigbaar zijn met de doeleinden van de samenwerkingsverbanden die worden aangewezen bij of krachtens dit wetsvoorstel.[48] Voor wat betreft de toetsing van de vraag of het doel van de gegevensverwerking door de private deelnemer verenigbaar is met het doel van het samenwerkingsverband, kan worden aangesloten bij de criteria die artikel 6, vierde lid, onder a tot en met e, AVG, geeft voor de afweging of er sprake is van verdere verwerking voor een verenigbaar doel.
Overigens volgt uit artikel 1.7, zesde lid, van de WGS dat resultaten van gegevensverwerking voor zover deze gegevens mede gebaseerd zijn op gegevens van de Belastingdienst (met uitzondering van de FIOD) alleen aan private partijen kunnen worden verstrekt indien dat noodzakelijk is voor het uitvoeren van een wettelijke verplichting of de vervulling van een publiekrechtelijke taak van de ontvanger en op voorwaarde dat sprake is van verenigbaarheid met het doel van het samenwerkingsverband. Verstrekking van een resultaat voor de behartiging van de gerechtvaardigde belangen van private partijen is daardoor uitgesloten. Zoals is toegelicht in de nota naar aanleiding van het verslag, wegen de belangen van private partijen niet op tegen het belang van belastingplichtigen om hun belastinggegevens geheim te houden. Zou de Belastingdienst belastinggegevens breed verspreiden onder private partijen, dan is denkbaar dat belastingplichtigen minder bereid zijn om hun belastingaangifte volledig en correct in te vullen.[49]

Vraag 30 (D66) – signaal van derde en uitsluiten van u-bochtconstructie
Stel dat het wetsvoorstel in werking is getreden. Zou het dan kunnen gebeuren dat een derde behoefte heeft aan gegevens over een bepaald persoon of organisatie, maar zelf die gegevens niet mag vergaren. Kan die derde dan een signaal aan een deelnemer van een samenwerkingsverband geven? En als langs die weg de deelnemer van het samenwerkingsverband de gegevens verwerkt en binnen dat verband deelt, dat de gegevens dan vervolgens aan de derde/signaalgever worden verstrekt? Is zo'n u-bocht constructie mogelijk, zo vragen de D66-fractieleden. Zo ja, hoe kwalificeert de regering dit? Zo nee, hoe wordt dit door de wettelijke regeling voorkomen?

Zoals de Minister van Justitie in de brief van 17 december 2021 schreef zal, in aanvulling op de bovengenoemde waarborgen, bij algemene maatregel van bestuur worden geregeld dat samenwerkingsverbanden zoveel mogelijk moeten motiveren op basis van welke informatie de uitkomst tot stand is gekomen. Bij amvb worden mede daarom nadere regels gesteld over de criteria om een bepaald signaal voor te dragen, waaronder over de aard, de eisen van kwaliteit en betrouwbaarheid

[47] Kamerstukken II 2020/21, 35 447, nr. 6, antwoord 159, blz. 124–125.
[48] Kamerstukken II 2020/21, 35 447, nr. 6, antwoord 60, blz. 51.
[49] Kamerstukken II 2020/21, 35 447, nr. 6, antwoord 67, blz. 55.

waaraan moet zijn voldaan. Zoals uit de startcriteria uit het concept-BGS blijkt, kan alleen een signaal, verzoek of aangemelde casus van een deelnemer de aanleiding zijn voor gezamenlijke gegevensverwerking. Hierbij moet aan diverse materiële criteria worden getoetst, waaronder in het bijzonder de vraag of de gezamenlijke gegevensverwerking past binnen het doel van het samenwerkingsverband. Verder is relevant dat de deelnemers uitsluitend rechtmatig verwerkte gegevens aan het samenwerkingsverband mogen verstrekken (artikel 1.5 van het concept-BGS). Een signaal van een derde mag alleen door een deelnemer in een samenwerkingsverband worden ingebracht indien dat noodzakelijk is voor het doel van het samenwerkingsverband met het oog op de *eigen* wettelijke taken en bevoegdheden van de deelnemers. Wanneer dat niet het geval is, is er geen verwerkingsgrondslag, zodat ook niet kan worden toegekomen aan doorverstrekking van het signaal aan het samenwerkingsverband. Als het signaal wel verstrekt wordt aan en verwerkt in het samenwerkingsverband, kan het resultaat van die verwerking pas verstrekt worden aan de derde partij als de verwerking van het resultaat overeenkomt met de taak of doelstelling van de derde partij en als alle deelnemers aan het samenwerkingsverband toestemming hebben gegeven voor de doorverstrekking van de gegevens (artikel 1.7, tweede lid). Hiermee is de genoemde u-bocht constructie uitgesloten als de verwerking uitsluitend ten behoeve van de derde zou plaatsvinden.

4.5 Besluit gegevensverwerking door samenwerkingsverbanden

Vraag 31 (D66) – toezending van concept-BGS aan Eerste Kamer
De Raad van State geeft in haar brief van 18 november 2021 twee opties, een novelle of het aannemen onder bepaalde voorwaarden. De leden van de D66-fractie opteren voor een derde mogelijkheid te weten de voorwaarde dat het Besluit gegevensverwerking door samenwerkingsverbanden dat volgens de brief van de regering van 17 december 2021) in voorbereiding is aan de Eerste Kamer wordt toegezonden opdat de inhoud daarvan bij de beraadslaging kan worden betrokken.[50] Ook eventuele andere AMvB's die het gewijzigd voorstel van wet van de benodigde concretisering, invulling of aanvulling zouden moeten voorzien, zouden aan de Eerste Kamer moeten worden verstrekt. Alleen dan wordt inzichtelijk wat de totale regeling is. Alleen dan is er daadwerkelijk enig zicht op de reikwijdte, omvang, richting en het toepassingsbereik van dit wetsvoorstel en op belangrijke vragen over wie daarmee in de praktijk aan het werk zullen gaan, aan welke regels zij gebonden zullen zijn, en wie toezicht op die regels gaat houden. Alleen dan kan de Eerste Kamer een geïnformeerde beslissing nemen over de vraag of dit wetsvoorstel in de uitvoeringspraktijk een niet alleen werkbaar maar ook rechtsstatelijk verantwoord instrument zal zijn, in plaats van een carte blanche waarmee de uitvoerende macht alle kanten op kan en het van de goedertierenheid van de daarbij betrokken personen gaat afhangen of er wel of niet grote ongelukken gaan gebeuren. Graag verzoeken de D66-leden een reactie van de regering op dit voorstel.

De tekst van het concept-BGS is gelijktijdig met de publicatie van deze memorie van antwoord in internetconsultatie gebracht en is nu dus te raadplegen. Tegelijk met de consultatiefase vinden de uitvoeringstoetsen plaats. Na de consultatiefase zal ik het gehele concept-BGS aan uw Kamer toezenden in het kader van de voorhangprocedure opdat optimaal inzicht wordt geboden in de uitwerking van de waarborgen en de concretisering van de regels over de gegevensverwerkingen. Dat betekent dat bij de voorhangprocedure niet alleen de bepalingen uit het concept-BGS aan uw

[50] Kamerstukken II 2021/22, 35 447, nr. 21, p. 6.

Kamer zullen worden voorgelegd waarvan het wetsvoorstel dat voorschrijft, maar ook de overige bepalingen.
Er zijn geen andere amvb's die bij het wetsvoorstel behoren.

Vraag 32 (D66) – nadere normering bij amvb van waarborgen
In het debat in de Tweede Kamer met de regering over dit wetsvoorstel is al opgemerkt dat in de tekst van het wetsvoorstel 68 keer naar op te stellen AMvB's wordt verwezen. Dus op al die onderdelen wordt in de wettekst opgenomen dat op een later moment nadere invulling kan worden gegeven aan alles dat nu nog niet sluitend is gemaakt, waarbij, zo constateren de leden van de D66-fractie, vaak wordt opgenomen dat bij of zelfs krachtens AMvB nadere voorwaarden kunnen worden gesteld, nadere invulling kan worden gegeven, reikwijdte kan worden uitgebreid, waarborgen kunnen worden gewijzigd et cetera. Uit het oogpunt van rechtszekerheid en transparantie achten deze leden dit bezwaarlijk. Pregnant voorbeeld is art. 1.8 WGS waar nota bene die waarborgen geregeld worden en waarin niet minder dan vier keer staat opgenomen dat bij of krachtens algemene maatregel van bestuur (in het tweede geval dus wellicht ook middels een ministeriële regeling of een andere in een AMvB gedelegeerde bevoegdheid) nadere regels zullen worden gesteld over, kort gezegd, de vraag wat die waarborgen dan zouden inhouden. De facto is daarmee in deze fase volgens de leden van de D66-fractie onduidelijk waar die waarborgen nou daadwerkelijk uit bestaan. Ook de bijzondere waarborgen die ten aanzien van geautomatiseerde gegevensanalyse staan opgenomen (art. 1.9) moeten bij of krachtens AMvB nog nader worden ingevuld. Bij of krachtens AMvB kunnen de deelnemers aan het Financieel Expertise Centrum (FEC) worden uitgebreid met private partijen (artikel 2.3 lid 1 sub h WGS), kunnen de categorieën van gegevens die worden verzameld en geanalyseerd worden aangevuld of van nadere regels worden voorzien (artikel 2.4 lid 2 WGS) en moeten nog nadere regels worden gesteld voor zowel de activiteiten van het FEC als het signalenoverleg (artikelen 2.5 lid 2 en 2.6 lid 2 WGS). Bij de andere samenwerkingsverbanden (ICOV, RIEC's en Zorg- en Veiligheidshuizen (ZVH)) gebeurt hetzelfde. Hoe werkbaar is dit allemaal nog en hoe inzichtelijk voor de burger die de wet wil en moet kennen?

Allereerst is van belang dát de waarborgen nu vastgelegd worden, zodat duidelijk is voor de deelnemers aan de samenwerkingsverbanden en de burger, waar de samenwerkingsverbanden aan moeten voldoen. Dat veel van de waarborgen bij amvb worden uitgewerkt, doet daaraan niet af. Artikel 10 van de Grondwet staat de wetgever ook toe om regels met betrekking tot de beperking van het recht op eerbiediging van de persoonlijke levenssfeer bij of krachtens de wet te stellen. De hoofdelementen van de gezamenlijke gegevensverwerking voor de samenwerkingsverbanden zijn opgenomen in de formele wet: het doel van het samenwerkingsverband, welke partijen deelnemen met het oog op de opgesomde taken en bevoegdheden, de activiteiten die zij verrichten, welke gegevens zij daarbij onder welke randvoorwaarden mogen verwerken, en welke waarborgen voor de gezamenlijke gegevensverwerking gelden. De Afdeling advisering stelt in haar voorlichting dat het gewijzigde voorstel nu wel diverse wezenlijke elementen en begrenzingen van de wettelijke regeling op het niveau van de formele wet bevat, als het gaat om de in het wetsvoorstel zelf geregelde samenwerkingsverbanden. Volgens de Afdeling advisering doet daaraan niet af dat bepaalde aspecten bij amvb nader geregeld worden, want de grondwetgever heeft in artikel 10, eerste lid, van de Grondwet delegatie toegestaan.[51] Gelet op de behoefte uit de praktijk aan flexibiliteit acht ik het wenselijk om

[51] Kamerstukken II 2021/22, 35 447, H, blz. 9.

bepaalde aspecten bij amvb nader te regelen.[52] Het gaat dan bijvoorbeeld om de regels over de criteria waaraan het startpunt (een signaal, verzoek of casus) van de gegevensverwerking moet voldoen.
De werkbaarheid en inzichtelijkheid worden bevorderd doordat er sprake is van slechts één amvb, te weten het concept-BGS. Deze kent dezelfde indeling en volgorde als de WGS. In de toelichting wordt telkens de samenhang met de betreffende artikelen uit de WGS vermeld. Uiteraard is van belang dat er passende opleidingen en trainingen plaatsvinden zodat elke deelnemer de waarborgen in de amvb kent. Daartoe verplicht artikel 1.17 van het concept-BGS. Een nadere uitwerking in de amvb zorgt ervoor dat er flexibel ingespeeld kan worden op ontwikkelingen op het gebied van informatieverwerking, data-analyse en waarborgen rondom dataverwerkingen. De ontwikkelingen op deze gebieden gaan snel.
De tekst van het concept-BGS is gelijktijdig met de publicatie van deze memorie van antwoord in internetconsultatie gebracht en is nu dus te raadplegen.

Vraag 33 (PvdD) – nahangprocedure amvb onder WGS
De AMvB die de regering voorstelt, gaat in zijn visie de belangrijke waarborgen omvatten die vereist zijn in het kader van bescherming van grondrechten. Waarom is de nahangprocedure niet op die AMvB van toepassing verklaard?

Voor het antwoord op deze vraag wordt verwezen naar het antwoord op vraag 31 van D66 over toezending van concept-BGS aan Eerste Kamer.

Vraag 34 (SGP) – aanwijzing nieuwe deelnemers via alternatieve voorhangprocedure
De leden van de SGP-fractie lezen dat artikel 10 van de Grondwet bepaalt dat het recht op eerbiediging van de persoonlijke levenssfeer door de formele wetgever mag worden beperkt, dat de wetgever die bevoegdheid mag delegeren aan lagere wetgevers en dat derhalve nadere delegatie bij AMvB mogelijk is. De leden van de SGP-fractie lezen in het advies van de Afdeling Advisering van de Raad van State dat dit geen carte blanche voor de wetgever is om verdere beperkingen bij AMvB te regelen. Het wetsvoorstel is zodanig gewijzigd dat de Afdeling haar waardering uitspreekt voor de wijziging. De leden van de SGP-fractie lezen dat het huidige voorstel alsnog een voorhangprocedure introduceert voor de aanwijzing van nieuwe deelnemers aan de samenwerkingsverbanden bij AMvB. De leden van de SGP-fractie vragen de regering of ingeval van spoed, deelname aan een samenwerkingsverband met terugwerkende kracht in voorhangprocedure gebracht kan worden om misdaadbestrijding niet in de weg te zitten.

Indien deelnemers worden toegevoegd bij amvb, moet zowel een voorhangprocedure als een bijzondere nahangprocedure worden gevolgd.[53] De voorhangprocedure werd opgenomen in het wetsvoorstel door het amendement-Kuiken[54] en de bijzondere nahangprocedure door het amendement-Van Nispen[55]. Het resultaat is dat een amvb die deelnemers toevoegt in twee verschillende fasen moet worden voorgelegd aan het parlement: voorafgaand aan aanbieding aan de

---

[52] Zie voor een nadere toelichting Kamerstukken II 2020/21, 35 447, nr. 6, antwoord 29, blz. 26–27.
[53] Dit is opgenomen in de artikelen 2.3, tweede en derde lid, 2.11, tweede en derde lid, 2.19, derde lid, en 2.27, vijfde lid, WGS.
[54] Kamerstukken II 2020/21, 35 447, nr. 18 (amendement-Kuiken over een voorhangprocedure voor de aanwijzing bij amvb van nieuwe deelnemers aan de samenwerkingsverbanden).
[55] Kamerstukken II 2020/21, 35 447, nr. 11 (amendement-Van Nispen over een mogelijkheid voor het parlement om een uitbreiding van een samenwerkingsverband vooraf goed of af te keuren). De toenmalige Minister heeft een appreciatie aan de Tweede Kamer gezonden (Kamerstukken II 2020/21, 35 447, nr. 19).

Afdeling advisering van de Raad van State en voorafgaand aan de inwerkingtreding. Er is niet gekozen voor een lichtere vorm van parlementaire betrokkenheid.
Na inwerkingtreding van een amvb een voor- of nahangprocedure niet meer mogelijk. Daarom is het niet mogelijk dat deelname aan een samenwerkingsverband met terugwerkende kracht in voorhangprocedure wordt gebracht.

5. Profilering / geautomatiseerde gegevensanalyse[56]

Vraag 35 (GroenLinks/PvdA) – welke geautomatiseerde gegevensanalyse

Welke geautomatiseerde gegevensanalyse gaat er op basis van deze wet plaatsvinden?

Geautomatiseerde gegevensanalyse is volgens artikel 1.1 WGS een analyse van persoonsgegevens waarbij *tijdens* de analyse geen menselijke tussenkomst plaatsvindt.[57] De gegevensanalyse wordt dus daadwerkelijk door een geautomatiseerd systeem uitgevoerd. Het wetsvoorstel vereist wel dat er menselijke tussenkomst plaatsvindt in de fase *nadat* de analyse is voltooid maar *voordat* de resultaten worden verstrekt aan de deelnemer van het samenwerkingsverband. Daarbij moet gecontroleerd worden op zorgvuldige totstandkoming van de analyse (artikel 1.9, tweede lid, WGS).
Welke vormen van geautomatiseerde gegevensanalyse mogelijk zijn, kan verschillen per samenwerkingsverband en wordt in de amvb nader uitgewerkt.
Alleen aan iCOV geeft het wetsvoorstel de bevoegdheid tot gezamenlijke geautomatiseerde gegevensanalyse (artikel 2.13). Deze bevoegdheid is uitgewerkt in artikel 2.9 tot en met 2.12 van het concept-BGS. Het gaat dan om de geautomatiseerde gegevensanalyse van gegevensbestanden ten behoeve van een iCOV themarapportage, waarbij de analyse van de data door middel van (beschrijvende) algoritmen plaatsvindt en niet alleen door menselijke duiding. De iCOV themarapportage 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. Hierbij wordt ook uitgelegd hoe de resultaten tot stand zijn gekomen. Voordat de rapportage verstrekt wordt, wordt de rapportage door meerdere medewerkers gecontroleerd.
De WGS biedt voor FEC en de RIEC's de mogelijkheid om bij amvb de bevoegdheid tot geautomatiseerde gegevensanalyse te regelen. Voor FEC en de RIEC's is deze mogelijkheid niet ingevuld in het concept-BGS.[58]

Vraag 36 (GroenLinks/PvdA) – besluitvorming en toezicht op algoritmen

Wie gaat bepalen welke algoritmen gebruikt gaan worden, en hoe wordt hier toezicht op gehouden?

---

[56] In het voorlopig verslag is deze paragraaf getiteld «profilering». Omdat het wetsvoorstel niet de term «profilering» hanteert, maar «geautomatiseerde gegevensanalyse», is de benaming van deze paragraaf aangepast. De begrippen zijn geen synoniemen, maar vertonen overlap. Hierop is ingegaan in de nota naar aanleiding van het verslag (Kamerstukken II 2020/21, 35 447, nr. 6, antwoord 80, blz. 67).

[57] Voor nadere toelichting zij verwezen naar de nota van wijziging, Kamerstukken II 2020/21, 35 447, nr. 7.

[58] Zoals toegelicht in de nota van wijziging (Kamerstukken II 2020/21, 35 447, nr. 7), is deze mogelijkheid in de WGS opgenomen om, gelet op de toekomstbestendigheid, niet bij voorbaat de deur dicht te houden voor innovatieve technologische ontwikkelingen, wanneer die noodzakelijk blijken om de verwachte toename aan data in de toekomst effectief te kunnen verwerken, bijvoorbeeld bij uitbreiding van (internationale) samenwerking of de ontwikkeling van efficiëntere analysemethodiek.

Voordat bij iCOV sprake kan zijn van geautomatiseerde gegevensanalyse, moeten algoritmes door de rechtmatigheidsadviescommissie worden getoetst aan onder meer navolgbaarheid en controleerbaarheid. Verder moet de procedure worden doorlopen uit de artikelen 2.9 en 2.10 van het concept-BGS, waarin onder meer is voorzien in een specifieke procedure voor de vaststelling van indicatoren en in andere specifieke waarborgen. Voor de verantwoording van de operationalisatie van de indicatoren wordt het Kwaliteitskader Big Data[59] van het Openbaar Ministerie en de Politie gebruikt of een vergelijkbaar door de rechtmatigheidsadviescommissie goedgekeurd format.
De Autoriteit Persoonsgegevens heeft onder alle omstandigheden de bevoegdheid om te onderzoeken of de door samenwerkingsverbanden gebruikte algoritmen functioneren in overeenstemming met het gegevensbeschermingsrecht. Zij toetst daarbij op basis van de beginselen van rechtmatigheid, transparantie en behoorlijkheid, zoals vastgelegd in de AVG. Verder kijkt zij naar de wijze waarop de in de AVG vastgelegde verantwoordingsplicht wordt uitgevoerd. De Autoriteit Persoonsgegevens heeft een en ander uitgewerkt in een specifiek kader voor het toezicht op artificiële intelligentie en algoritmes.[60]
Verder is een samenwerkingsverband verplicht om de AP ingevolge artikel 36 AVG voorafgaand aan een voorgenomen verwerking van persoonsgegevens te raadplegen wanneer de uitkomst van de gegevensbeschermingseffectbeoordeling een hoog risico laat zien wanneer het samenwerkingsverband geen maatregelen neemt om het risico te beperken.[61]
Voordat een samenwerkingsverband tot een nieuw type gezamenlijke geautomatiseerde gegevensanalyse overgaat, dient het een gegevensbeschermingseffectbeoordeling uit te voeren op grond van artikel 35 AVG.[62]
Voorts heeft het kabinet extra middelen beschikbaar gesteld voor de functie van een algoritmetoezichthouder die is ondergebracht bij de Autoriteit Persoonsgegevens.

Vraag 37 (D66) – waarborgen en voorzorgsmaatregelen bij geautomatiseerde gegevensanalyse
In dat licht zou de D66-fractie willen benadrukken dat bepaalde groepen in de samenleving harder getroffen kunnen worden door de nadelige effecten van dit wetsvoorstel. Mensen in kwetsbare posities komen meer in aanraking met overheidsinstanties dan mensen die zichzelf goed kunnen redden. Automatische risicoselectie op basis van (zelflerende) algoritmes speelt hier een rol. De D66-fractie is bezorgd over het risico dat de samenwerkingsverbanden de geautomatiseerde gegevensanalyse zoals (risico)profilering niet correct gebruiken. Zijn er voldoende waarborgen en voorzorgsmaatregelen opgenomen in het voorliggende wetsvoorstel om de ingrijpende gevolgen van deze risicoprofielen te voorkomen. Is voldoende afgedekt dat de deelnemers aan de samenwerkingsverbanden de analyse niet vooral richten op bepaalde wijken of personen van een bepaalde afkomst? Is het wetsvoorstel discriminatieproof?

Geautomatiseerde gegevensanalyse is alleen aan de orde bij iCOV.
Zoals de toenmalige Minister van Justitie en Veiligheid schreef in de brief van 17 december 2021, zal gevolg worden gegeven aan de aanbevelingen van de Afdeling advisering over een zorgvuldig gebruik van algoritmes,

[59] Kamerstukken II 2019/20, 29 628, nr. 948, bijlage «Kwaliteitskader Big data».
[60] https://autoriteitpersoonsgegevens.nl/nl/nieuws/toezicht-op-algoritmes.
[61] Op dit preventieve toezicht door de AP is nader ingegaan in de nota n.a.v. het verslag, Kamerstukken II 2020/21, 35 447, nr. 6, antwoord 39, blz. 33–34) en §3.5 van de memorie van toelichting.
[62] Dit is toegelicht in de nota n.a.v. het verslag. Kamerstukken II 2020/21, 35 447, nr. 6, antwoord 85, blz. 71.

een fenomeen dat in algemene zin ook de aandacht heeft en waartoe de nodige stappen zijn gezet, die ook hun toepassing zullen hebben op gegevensverwerkingen onder de WGS. Zoals de Minister terecht vaststelde in de voornoemde brief, geldt het discriminatieverbod voor elk overheidsonderdeel. Dat betekent dat ook onder de WGS geen ongerechtvaardigd onderscheid mag worden gemaakt. Daarnaast is een verwerking waar discriminatie aan ten grondslag ligt, strijdig met de normen van het gegevensbeschermingsrecht. De AVG, WGS en het concept-BGS bevatten daar bovenop extra waarborgen om discriminatie tegen te gaan.

Voordat een samenwerkingsverband tot een nieuw type gezamenlijke geautomatiseerde gegevensanalyse overgaat, dient het een gegevensbeschermingseffectbeoordeling uit te voeren op grond van artikel 35 AVG.[63]

Op grond van artikel 9, eerste lid, AVG mogen geen gegevens worden verwerkt over ras of etnische afkomst. Artikel 1.9 concept-BGS voegt daaraan toe dat ook geen gegevens over nationaliteit mogen worden verwerkt, tenzij dit voor de identificatie van betrokkene onvermijdelijk is. In artikel 1.14 van het concept-BGS is uitgewerkt dat de leden van de rechtmatigheidsadviescommissie, waarin deskundigen advies uitbrengen over de rechtmatigheid van gegevensverwerkingen door het samenwerkingsverband, er zorg voor dienen te dragen dat in de rechtmatigheidsadviescommissie aandacht is voor het tegengaan van risico's op ongelijke behandeling en discriminatie. Bovendien is in artikel 1.17 van het concept-BGS uitgewerkt dat medewerkers die ingezet worden in het samenwerkingsverband opleidingen krijgen ter bevordering van hun kennis en vaardigheden op het gebied van een zorgvuldige omgang met persoonsgegevens en data-ethiek. Het tegengaan van (onbewuste) discriminatie komt bij deze beide onderdelen aan de orde.

Verder zijn in dit kader van belang de aanvullende waarborgen bij geautomatiseerde gegevensanalyses (artikel 1.9 WGS). Deze waarborgen zijn mede bedoeld om – in lijn met overweging 71 bij de AVG – discriminatie, fouten en vooroordelen tegen te gaan in algoritmen die bij een geautomatiseerde analyse worden gebruikt:

- Artikel 1.9, eerste lid, verplicht de deelnemers om voor adequate en uniforme technische en organisatorische maatregelen zorg te dragen die de kwaliteit van de gezamenlijke geautomatiseerde gegevensanalyse en de juistheid en de volledigheid van de te verwerken gegevens bevorderen. De deelnemers moeten de gehanteerde methode dus toetsen op feitelijke juistheid en kwaliteit. Wat de kwaliteit van de gegevens zelf betreft, volgt hieruit dat iCOV gegevens alleen mag gebruiken als deze van voldoende kwaliteit zijn. ICOV geeft hieraan invulling door uitgebreid te toetsen of de data van voldoende kwaliteit zijn en of zij geschikt zijn om betrouwbaar te koppelen met data van andere deelnemers, alvorens de gegevens voor rapportages te gebruiken.[64]
- Artikel 1.9, tweede lid, regelt de verplichting om een resultaat van een gezamenlijke geautomatiseerde gegevensanalyse uitsluitend aan een deelnemer of derde te verstrekken na menselijke tussenkomst, waarbij wordt beoordeeld of het resultaat op zorgvuldige wijze tot stand is gekomen.
- Artikel 1.9, derde lid bevat de verplichting tot uitleg op toegankelijke wijze aan het publiek over de gehanteerde patronen, indicatoren en andere onderliggende logica.

---

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

[64] Zie nota n.a.v. het verslag, Kamerstukken II 2020/21, 35 447, nr. 6, antwoord 85, blz. 72 (alinea beginnend met «iCOV beoordeelt de data...»).

- Artikel 1.9, zesde lid, regelt een verbod op algoritmen waarvan de uitkomsten niet navolgbaar en controleerbaar zijn. De analyse moet dus op zodanige wijze plaatsvinden dat de uitkomsten navolgbaar en controleerbaar zijn.

Bij de toegestane geautomatiseerde gegevensanalyse – namelijk bij iCOV – bevatten artikel 2.9 tot en met 2.12 van het concept-BGS bovendien de volgende aanvullende waarborgen:
– Vooraf moet advies worden gevraagd aan de rechtmatigheidsadviescommissie over onder meer de gehanteerde indicatoren, verwerkingsmethode en gegevens. Dit geschiedt aan de hand van een door deelnemers van iCOV op te stellen productbeschrijving. Daarin moeten zij het thema, de indicatoren en de methode beschrijven en verantwoorden.
– Er mogen uitsluitend gevalideerde indicatoren worden gebruikt. Ze moeten zijn gecontroleerd op geldigheid en juistheid, rekening houdend met vertekening (*bias*), navolgbaarheid, betrouwbaarheid en representativiteit van de gegevens; de deelnemers dienen er zorg voor te dragen dat de indicatoren objectief en nauwkeurig zijn.
– Er moet voldoende aanleiding zijn voor de geautomatiseerde gegevensanalyse, bestaande uit duidelijke en objectieve aanwijzingen inzake onrechtmatig financieel gewin.
– De deelnemers dienen te zorgen voor een representatieve onderzoeksgroep en moeten aandacht hebben voor het risico van vooringenomenheid.
– De gehanteerde methode moet uitlegbaar, navolgbaar en controleerbaar zijn.
– Over de toepassing van deze waarborgen moet periodiek worden gerapporteerd aan de rechtmatigheidsadviescommissie.

Tot slot valt te wijzen op het Kwaliteitskader Big data,[65] dat iCOV gebruikt bij de ontwikkeling van een nieuw type themarapportage. Hierin zijn uitdrukkelijk vragen geformuleerd om het risico van discriminatie in de indicatoren en gebruikte data te voorkomen.

Vraag 38 (PvdA/GroenLinks) – evaluatie en toezicht geautomatiseerde gegevensanalyse
Hoe faciliteert de regering een zorgvuldige evaluatie en terugkoppeling van resultaten om hiermee te voorkomen dat het leerproces van zelflerende algoritmen wordt gevoed met «biased» data? Is de regering van plan het toezicht op de rechtmatige toepassing van kunstmatige intelligentie en bovenstaande door de Raad van State voorgestelde waarborgen te evalueren en de Kamer hierover te informeren? Zo ja, is dit een periodiek terugkerende evaluatie? Zo nee, is de regering bereid een dergelijke evaluatie toe te zeggen en/of een verantwoording op dit onderwerp te verplichten voor het jaarverslag van de betrokken samenwerkingsverbanden?

Voor zover de WGS en de amvb een grondslag bieden voor geautomatiseerde gegevensanalyse – namelijk alleen bij de themarapportages van iCOV – is geen sprake van zelflerende algoritmen of kunstmatige intelligentie, aangezien de mens moet specificeren welke indicatoren worden gebruikt, hoe deze worden toegepast op de data en hoe deze vervolgens weergegeven worden in een rapportage. De algoritmes die iCOV gebruikt zijn beschrijvend van aard. Met andere woorden: iCOV stelt vooraf gedefinieerde ofwel gestandaardiseerde vragen aan de data die een navolgbaar en controleerbaar resultaat opleveren. De gebruikte indicatoren worden door de mens gespecificeerd op basis van weten-

[65] Kamerstukken II 2019/20, 29 628, nr. 948, bijlage «Kwaliteitskader Big data».

schappelijk onderzoek, expertsessies en/of statistische validatie. De mens beslist hoe de indicatoren worden geoperationaliseerd in de data en hoe zij worden weergegeven in de rapportage. Dit volgt uit de artikelen 2.9, tweede lid, en 2.10 van het concept-BGS en artikel 1.9, tweede lid, van het wetsvoorstel (verplichting tot menselijke tussenkomst).

Kenmerkend voor niet-zelflerende algoritmen is dat de mens zelf specificeert hoe de computer moet werken. Artikel 1.9, zesde lid, WGS verbiedt om algoritmes te hanteren waarvan de uitkomsten niet navolgbaar en controleerbaar zijn. Door onder andere kunstmatige intelligentie volgen zelflerende algoritmes geen vooraf bepaalde set van regels maar maken ze gebruik van zelflerende statistische technieken. Daardoor zijn de beslissingen die een zelflerend algoritme maakt voor de mens haast ondoorgrondelijk. Wanneer gebruik is gemaakt van zelflerende algoritmes is de toets hoe de uitkomsten tot stand zijn gekomen nagenoeg onmogelijk.

Er is evenmin sprake van kunstmatige intelligentie, zoals is toegelicht in §10 van deze memorie van antwoord. De vraag wordt daarom zo geïnterpreteerd dat wordt gevraagd naar de evaluatiemechanismen van geautomatiseerde gegevensanalyse.

Het wetsvoorstel voorziet in diverse terugkoppelings- en evaluatiemechanismen van de gegevensverwerkingen:
– De ontvangers van resultaten van de gegevensverwerking van het samenwerkingsverband zijn verplicht ten minste jaarlijks terug te koppelen wat de effectiviteit en bruikbaarheid van die resultaten was (artikel 1.7, vierde lid, wetsvoorstel).
– De deelnemers van een samenwerkingsverband moeten een periodieke evaluatie op basis van deze terugkoppeling uitvoeren (artikel 1.7, vijfde lid, wetsvoorstel).
– In onafhankelijke privacy audits moet periodiek worden onderzocht of men voldoet aan de AVG en de WGS; de resultaten gaan in afschrift naar de AP (artikel 1.10 wetsvoorstel).
– Er moet een jaarverslag worden gepubliceerd met een terugkoppeling over de bruikbaarheid van de resultaten die partijen van het samenwerkingsverband hebben ontvangen (artikel 1.12 wetsvoorstel).
– Een evaluatie van de doeltreffendheid en effecten van de wet in de praktijk moet binnen vijf jaar plaatsvinden (artikel 5.1 wetsvoorstel).
– De indicatoren worden opgesteld op basis van wetenschappelijke kennis, statistische validatie en expertkennis (artikel 2.10 concept-BGS).
– De rechtmatigheidsadviescommissie geeft verplicht advies aan de deelnemers over onder meer de indicatoren en verwerkingsmethode (artikel 2.9, tweede lid, concept-BGS).

Vraag 39 (PvdA/GroenLinks) – afwijken van algoritmische uitkomsten
Hoe stimuleert de regering het creëren en behouden van een cultuur waarin kan en mag worden afgeweken van algoritmische uitkomsten bij geautomatiseerde gegevensanalyse om discriminatoire behandeling van persoonsgegevens te corrigeren?

Dit wordt gestimuleerd door naleving van de waarborgen, toegelicht in antwoord op *vraag 37 (D66) – waarborgen en voorzorgsmaatregelen bij geautomatiseerde gegevensanalyse* en in antwoord op de navolgende vraag.

Vraag 40 (VVD) – expertise inzake algoritmen en tegengaan ongewenste profilering

Een zorgvuldige uitvoeringspraktijk is van belang om risico's op het gebied van discriminatie en ongelijke behandeling te voorkomen. Menselijk handelen is daarbij cruciaal. Immers mensen stellen datasets samen en richten algoritmen in. De leden van de fractie van VVD vragen de regering welke waarborgen er zijn voor het creëren van expertise enerzijds en een cultuur anderzijds waarmee ongewenste profilering wordt tegengegaan?

Graag sluit ik mij aan bij de slotalinea van de brief van 17 december 2021 aan uw Kamer, waarin de toenmalige Minister van Justitie en Veiligheid schreef dat geïnvesteerd moet worden in professionaliteit en (juridische) deskundigheid op de werkvloer, evenals in een cultuur waarin kan en mag worden afgeweken van algoritmische uitkomsten. Voor wat betreft de kwaliteit van de uitvoeringspraktijk in algemene zin verwijs ik naar *vraag 56 (D66) – kwaliteit van de uitvoeringspraktijk*. Hierna ga ik specifiek in op de expertise en cultuur ten aanzien van algoritmen, om ongewenste profilering tegen te gaan.

Er zal gevolg worden gegeven aan de aanbevelingen die de Afdeling advisering in haar voorlichting heeft gedaan ten behoeve van een zorgvuldig gebruik van algoritmes. Naast het investeren in professionaliteit en (juridische) deskundigheid op de werkvloer en een cultuur waarin kan en mag worden afgeweken van algoritmische uitkomsten, heeft de Afdeling advisering benadrukt dat afwegingskaders van belang zijn om te bevorderen dat algoritmen zorgvuldig en met respect voor relevante grondrechten tot stand worden gebracht.[66] In zijn algemeenheid heeft het kabinet, net als het vorige, veel aandacht voor het zorgvuldige gebruik van algoritmes. Er zijn afwegingskaders en hulpmiddelen ontwikkeld, die bouwstenen vormen van het op te stellen implementatiekader «inzet van algoritmen». De inzet van het kabinet is om binnen deze instrumenten prioritering aan te brengen en deze te stroomlijnen, zodat in alle fasen van de levenscyclus van algoritmische toepassingen praktische handvatten worden geboden.[67] Enkele van deze afwegingskaders zijn:

– Het Kwaliteitskader Big Data, dat is opgesteld door de politie en het OM.[68] Dit wordt gebruikt voor het toetsen van big data toepassingen aan onder andere rechtmatigheid en ethiek.
– De Handreiking AI-systeemprincipes voor non-discriminatie, getiteld «*non-discriminatie by design*».[69] Dit is een praktische handreiking waarin stap voor stap wordt uitgelegd hoe organisaties kunnen voorkomen dat hun algoritmes discrimineren. In de handreiking is een vertaalslag gemaakt van essentiële juridische kaders naar operationele ontwerpprincipes. De handreiking is opgesteld in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties door een team van onderzoekers van de universiteiten van Tilburg en Eindhoven, Vrije Universiteit Brussel en het College voor de Rechten van de Mens. De handreiking geeft tien regels waarmee volgens de opstellers misstanden zoals bij de kindertoeslagen kunnen worden voorkomen.
– Het Impact Assessment voor Mensenrechten bij de inzet van Algoritmen (IAMA).[70] Dit impact assessment kan een organisatie gebruiken om in de gehele levenscyclus van algoritmische systemen de risico's

---

[66] Kamerstukken I 35 447, H, blz. 2, 15 en 19.
[67] Dit is gemeld in de beantwoording van vragen van de vaste commissie voor Digitale Zaken van de Tweede Kamer over het rapport Algoritmes getoetst; De inzet van 9 algoritmes bij de rijksoverheid». Zie het antwoord op vraag 32 uit Kamerstukken II 2022/23, 26 643, nr. 923.
[68] Kamerstukken II 2019/20, 29 628, nr. 948, bijlage «Kwaliteitskader Big data».
[69] Zie https://www.tilburguniversity.edu/nl/over/schools/law/departementen/tilt/onderzoek/handreiking of Kamerstukken II 2020/21, 26 643, nr. 765, bijlage.
[70] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2021/02/25/impact-assessment-mensenrechten-en-algoritmes/IAMA.pdf.

voor mensenrechten in kaart te brengen. Het IAMA is in opdracht van het vorige kabinet door de Universiteit Utrecht ontwikkeld.
– De richtlijnen voor het toepassen van algoritmes door de overheid uit de brief van 8 oktober 2019.[71]

Tot slot onderken ik, met de Afdeling advisering van de Raad van State,[72] het belang dat een zorgvuldige evaluatie en terugkoppeling plaatsvindt als het gaat om de resultaten van de toepassing van algoritmen. In antwoord op de *Vraag 38 (PvdA/GroenLinks) – evaluatie en toezicht geautomatiseerde gegevensanalyse* zijn de diverse terugkoppelings- en evaluatiemechanismen opgesomd, waartoe het wetsvoorstel verplicht.

Vraag 41 (PvdA/GroenLinks) – betrekken van externe partijen bij algoritmen
Welke risico's omvat het betrekken van relevante derde partijen, zoals belangenorganisaties, bij het ontwerp van algoritmen met als doel om onrechtmatige werkingen te voorkomen en het maatschappelijk draagvlak voor het gebruik van algoritmen te vergroten? Hoe waarborgt de regering en/of het betrokken samenwerkingsverband de transparantie en objectiviteit (in de zin van «non-biased») van het algoritme wanneer een externe partij deze (mede) ontwerpt?

De Afdeling advisering van de Raad van State heeft in haar voorlichting terecht gesteld dat het aangewezen is om relevante derde partijen, zoals belangenorganisaties, te betrekken bij het ontwerp van algoritmen die een samenwerkingsverband hanteert, omdat daarmee onrechtmatige verwerkingen kunnen worden voorkomen en tevens het maatschappelijk draagvlak voor het gebruik van algoritmen kan worden vergroot.[73] Het wetsvoorstel laat ruimte om derde partijen te betrekken bij het ontwerp van algoritmen. Uiteraard mogen daarbij geen persoonsgegevens toegankelijk worden voor deze derden en van belang is dat het inzichtelijk blijft hoe de algoritmen werken.

De transparantie wordt gewaarborgd doordat de samenwerkingsverbanden uitleg moeten geven over gehanteerde patronen, indicatoren en andere onderliggende logica bij geautomatiseerde gegevensanalyse (artikel 1.9, derde lid, WGS). Bovendien verplicht artikel 14 van de AVG de deelnemers in beginsel om betrokkene te informeren over onder andere het feit dat gegevens over betrokkene worden verwerkt en voor welke doeleinden. Verder moeten samenwerkingsverbanden jaarverslagen publiceren met daarin een verantwoording van de effectiviteit en bruikbaarheid van de gegevensverwerking (artikel 1.12 WGS).

De objectiviteit wordt gewaarborgd doordat het startpunt van de gegevensverwerking moet bestaan uit objectieve en duidelijke aanwijzingen (art. 2.11 concept-BGS) en door de aanvullende waarborgen, die zijn opgenomen in de artikelen 2.10 tot en met 2.12 van het concept-BGS. Deze zijn toegelicht in antwoord op *vraag 37 (D66) – waarborgen en voorzorgsmaatregelen bij geautomatiseerde gegevensanalyse*.
In het kader van de objectiviteit bij een geautomatiseerde gegevensanalyse is bovendien van belang dat de onderzoeksvragen voor een iCOV-themarapportage in verhouding moeten staan met het thema en de indicatoren van de themarapportage. De verantwoording van het thema, de indicatoren, en de methode van verwerking worden voor toetsing voorgelegd aan de rechtmatigheidsadviescommissie (artikel 2.9, tweede lid, concept-BGS). De indicatoren moeten objectief en nauwkeurig zijn,

[71] Kamerstukken II 2018/19, 29 628, 641.
[72] Kamerstukken I 35 447, H, blz. 17.
[73] Kamerstukken I 2021/022, 35 447, H, blz. 15–16.

zijn gecontroleerd op geldigheid en juistheid en zijn gebaseerd op wetenschappelijke literatuur, statistische validatie en kennis van experts (artikel 2.10 concept-BGS).

6. Digitale technieken

Vraag 42 (VVD) – gebruikte software

De Raad van State publiceerde in mei 2021 «Aanbevelingen voor digitalisering en wetgeving».[74] Een aantal aanbevelingen is relevant bij het beoordelen van dit wetsvoorstel, zoals dat de digitale techniek betrokken dient te worden bij het ontwerpen van wet- en regelgeving. Is dit bij het voorliggende wetsvoorstel gebeurd, vragen de leden van de VVD-fractie. Is er inzicht in het specificatieproces van de software die samenwerkingsverbanden gebruiken (dit is het proces van omzetting van de wet- en regelgeving in een code). En zijn de samenwerkingsverbanden in voldoende mate in staat om softwarematige gegevens en voorspellingen te doorgronden en in hun afweging te betrekken, zonder daar onevenredig veel gewicht aan toe te kennen? Is deze informatie voldoende toegankelijk voor burgers?

In haar voornoemde aanbevelingen omschrijft de Afdeling advisering van de Raad van State «specificatieproces» als «het proces van omzetting van wet- en regelgeving in code». Voor iCOV zijn er in dit opzicht enige gevolgen denkbaar. ICOV is betrokken bij zowel het wetsvoorstel als het concept-BGS, zodat er inderdaad inzicht is in het specificatieproces van de software. De gevolgen van het wetsvoorstel zijn bijvoorbeeld dat nieuwe voorwaarden voor de aanvragen van iCOV-rapportages zullen worden toegevoegd aan de aanvraagpagina voor rapportages. Een deel van de voorwaarden en verplichtingen is reeds staande praktijk, zoals het aangeven uit welke databronnen een iCOV-rapportage afkomstig is. Op het concept-BGS, waarin diverse waarborgen worden geconcretiseerd, zullen uitvoeringstoetsen worden verricht. Daarin kan ook de verhouding tot de softwaresystemen aan de orde komen.
Het doorgronden van voorspellingen is niet aan de orde, want iCOV gebruikt iCOV geen voorspellende algoritmes, aangezien ze niet een verwachting of waarschijnlijkheid afgeven van een toekomstige gebeurtenis. Het gaat om beschrijvende algoritmes, die antwoord geven op specifieke feitelijke vragen. Bijvoorbeeld: is een rechtspersoon een erkende hypotheeknemer?

Samenwerkingsverbanden voeren zelf de gegevensverwerkingen uit en moeten in staat zijn om deze te doorgronden en te kunnen uitleggen. De WGS en het concept-BGS staan thans alleen voor iCOV gezamenlijke geautomatiseerde gegevensanalyse toe. Alvorens algoritmes bij iCOV in gebruik worden genomen, worden deze getoetst aan de hand van richtlijnen en voorgelegd aan de rechtmatigheidsadviescommissie.[75] Transparantie, validatie en controleerbaarheid van het algoritme zijn voor iCOV van groot belang. Op deze aspecten vindt dan ook een grondige toetsing plaats. Uit artikel 1.9, derde lid, WGS volgt dat het samenwerkingsverband in staat moet zijn (en verplicht is) om bij gezamenlijke geautomatiseerde gegevensanalyse op toegankelijke wijze uitleg te geven over de gehanteerde patronen en indicatoren of andere onderliggende logica. Artikel 1.9, zesde lid, WGS, verbiedt om algoritmes te hanteren waarvan de uitkomsten niet navolgbaar en controleerbaar zijn. Artikel 2.12 van het concept-BGS bepaalt dat de gehanteerde methodiek uitlegbaar,

---

[74] Raad van State, «Digitalisering. Wetgeving en bestuursrechtspraak», Den Haag, mei 2021.
[75] Zie het Kwaliteitskader Big Data dat wordt geïmplementeerd in de iCOV processen: https://www.rijksoverheid.nl/documenten/rapporten/2020/05/29/tk-bijlage-2-kwaliteitskader-big-data.

navolgbaar en controleerbaar moet zijn. Artikel 1.8 van het concept-BGS verplicht bovendien om bij de verstrekking van resultaten zoveel mogelijk te motiveren op basis van welke informatie het resultaat tot stand is gekomen, tenzij het resultaat is gebaseerd op een casusoverleg of signalenoverleg. ICOV heeft een leeswijzer bij zijn rapportages en bij een themarapportage of iCOV Rapportage Relaties wordt ook nog mondeling toelichting gegeven.
Na ontvangst van een resultaat zal er altijd eigenstandig nader onderzoek verricht moeten worden naar aanleiding van ontvangen resultaten, conform de wettelijke taken en bevoegdheden van de ontvanger.

Vraag 43 (VVD) – informatiebeveiliging
Worden de informatiesystemen beveiligd en gecertificeerd, zo vragen de leden van de fractie van VVD.

Volgens artikel 1.8, achtste lid, van het wetsvoorstel mogen persoonsgegevens alleen worden verwerkt in systemen met een adequaat beveiligingsniveau. De informatiebeveiliging moet volgens die bepaling ten minste voldoen aan de richtlijnen van de Minister van BZK: de Baseline Informatiebeveiliging Overheid (BIO). Op grond daarvan moeten er regelmatig beveiligingsaudits worden gedaan indien sprake is van basisbeveiligingsniveau 2, waarvan hier sprake is.[76] Bij iCOV worden de gegevens verwerkt in een hoog beveiligde omgeving en is sprake van basisbeveiligingsniveau 3.
Ook bevat de BIO richtlijnen voor het uitvoeren van beveiligingsupdates en het uitvoeren van controles van de veiligheid van autorisaties. In artikel 1.8, tweede lid, van het wetsvoorstel is ook geborgd dat alleen personen die geautoriseerd zijn toegang hebben tot de systemen waarin persoonsgegevens zijn opgenomen. De AP houdt toezicht op de naleving van alle waarborgen in het wetsvoorstel, dus ook de waarborg van een adequaat beveiligingsniveau.

7. Toezicht en handhaving

Vraag 44 (VVD) – toezicht
De Raad van State wijst erop dat er duidelijke voorwaarden moeten worden afgesproken waaronder zo groot mogelijke transparantie en voldoende mate van menselijk toezicht; hoe is dat toezicht geregeld bij deze samenwerkingsverbanden? Het betreft het toezicht op de zaken die de gegevensverwerking betreffen, maar ook of de verantwoordingseisen, zoals bijvoorbeeld de jaarverslaglegging (artikel 1.12 WGS), de rapportage over de effectiviteit van de gegevensverwerking (artikel 1.7 WGS), de verplichting om een contactpersoon aan te wijzen (artikel 1.4 WGS), etc. worden nageleefd?

Het toezicht op de gegevensverwerking bij de samenwerkingsverbanden in de zin van de WGS is op verschillende manieren geborgd:
– De in te stellen rechtmatigheidsadviescommissie zal ingevolge het voorgestelde artikel 1.8, zesde lid, van het wetsvoorstel tot taak krijgen de rechtmatigheid van de verwerking van persoonsgegevens in het samenwerkingsverband structureel te beoordelen bij nieuwe verwerkingen en wijziging in verwerkingen en om voorstellen aan het samenwerkingsverband te doen om onrechtmatigheden op te lossen. In het concept-BGS is voorzien dat een rechtmatigheidsadviescommissie moet bestaan uit door de deelnemers aan een samenwerkingsverband benoemde personen met deskundigheid en ervaring op het gebied van de toepasselijke wetgeving inzake gegevensverwerking en

[76] Zie maatregel 18.1.4.2, 18.2.1 en 18.2.1.2 van de Baseline Informatiebeveiliging Overheid.

de werking van het samenwerkingsverband (artikel 1.14, eerste lid, concept-BGS).
– Op basis van artikel 1.10 van het wetsvoorstel dient periodiek een onafhankelijke privacy-audit plaats te vinden. Zo wordt elk samenwerkingsverband periodiek doorgelicht op compliance met de AVG, de WGS en het BGS. De resultaten van de privacy audits moeten worden toegezonden aan de AP.
– De functionarissen voor gegevensbescherming van de afzonderlijke deelnemers hebben het recht om te allen tijde de taken uit te voeren die op grond van de privacywetgeving aan hen zijn toebedeeld. In aanvulling daarop wordt ingevolge het voorgestelde artikel 1.4, tweede lid, WGS één van de functionarissen voor gegevensbescherming van de deelnemende overheidsinstanties aangewezen die als coördinerend functionaris voor gegevensbescherming voor het samenwerkingsverband optreedt en uit dien hoofde krachtens artikel 39, eerste lid, onder b, AVG, ook toeziet op de naleving van de AVG en ander gegevensbeschermingsrecht door het samenwerkingsverband. Dit laat de bevoegdheden van de functionarissen onverlet, maar moet de coördinatie bevorderen van het bestaande toezicht door de functionarissen voor de gegevensbescherming. Zo moeten de deelnemers rapporteren aan de coördinerend functionaris voor de gegevensbescherming, indien zij besluiten af te wijken van een advies (artikel 1.13 concept-BGS).
– Het toezicht op de naleving door het samenwerkingsverband van de AVG, de WGS en het BGS valt onder de bevoegdheid van de AP.
– Het kabinet heeft extra middelen beschikbaar gesteld voor de functie van een algoritmetoezichthouder die is ondergebracht bij de AP.

Vraag 45 (D66) – inhoud jaarverslag
Wat het toezicht op de werkwijze van de samenwerkingsverbanden betreft geldt dat ook daarin nog veel onduidelijk is. Artikel 1.12 WGS schrijft voor dat er een jaarverslag moet worden gepubliceerd, maar alleen wanneer die openbaarmaking de verwezenlijking van de doeleinden van het samenwerkingsverband niet onmogelijk dreigt te maken of deze ernstig in het gedrang dreigen te brengen.
De leden van de D66-fractie vragen of dit er niet toe gaat leiden dat ook deze weer opengelaten norm tot gevolg heeft dat er maar heel erg weinig gepubliceerd zal worden en heel gemakkelijk gezegd zal kunnen worden dat dit echt niet mogelijk is aangezien dat onderzoeksdoelen zou kunnen frustreren, de effectiviteit van het samenwerkingsverband zou kunnen aantasten en criminelen een inkijkje zou kunnen geven in de werkwijze et cetera?

Momenteel worden door de samenwerkingsverbanden reeds jaarverslagen gepubliceerd. Volgens artikel 1.12 WGS moet een jaarverslag ingaan op de terugkoppeling van de deelnemers over de effectiviteit en bruikbaarheid van de resultaten van de gezamenlijke gegevensverwerking. Het inroepen van de uitzonderingsmogelijkheid betekent niet dat er heel erg weinig hoeft te worden gepubliceerd, maar veeleer dat het jaarverslag niet zodanig gedetailleerd hoeft te zijn dat hierdoor toezichts- en opsporingsbelangen zouden worden doorkruist, of anderszins de doeleinden van de gegevensverwerking zouden worden doorkruist. In de AVG zijn deze redenen erkend als uitzonderingsgronden op de plicht om informatie te verschaffen over gegevensverwerkingen (artikel 14, vijfde lid, onder b, en artikel 23, eerste lid, onder d, e en h, AVG). Hierop wordt aangesloten in artikel 1.12 WGS. In de verplichte privacy audits kan naar voren komen of de verplichtingen uit de WGS, waaronder de jaarverslagleggingsplicht, behoorlijk worden nagekomen. De auditresultaten moeten in afschrift aan de AP worden gezonden en bij niet-nakoming van de wettelijke verplichtingen moet binnen een jaar een hercontrole plaats-

vinden op die onderdelen die niet voldeden aan de gestelde voorwaarden. Van die hercontrole moeten de resultaten eveneens aan de AP worden gezonden (artikel 1.10, tweede en derde lid, WGS).

Vraag 46 (PvdD) – sancties op niet-naleving verplichtingen
In de WGS worden verplichtingen opgelegd aan deelnemers en aan samenwerkingsverbanden, zo constateren de leden van de PvdD-fractie. Is de niet-naleving van die verplichtingen strafbaar? Bestaat er een bevoegdheid van een bestuursorgaan om met een bestuurlijke sanctie op te treden tegen niet-naleving?

De Autoriteit persoonsgegevens is belast met het toezicht op de naleving van niet alleen de AVG, maar ook op de verwerking van persoonsgegevens overeenkomstig het bij of krachtens de wet bepaalde (artikelen 6, derde lid, en 15, eerste lid, Uitvoeringswet AVG). Niet-naleving van de WGS dan wel de bijbehorende amvb vormt in het bijzonder een overtreding van artikel 6, eerste en derde lid, AVG. De AP kan hiervoor een bestuurlijke boete opleggen op grond van artikel 83 van de AVG, ook aan overheden (artikel 18 Uitvoeringswet AVG). De AP kan verder op grond van artikel 58, tweede lid, tien verschillende soorten corrigerende maatregelen opleggen, zoals een tijdelijk of definitief verbod om persoonsgegevens te verwerken. Tot slot kan de AP een last onder bestuursdwang opleggen (artikel 16 Uitvoeringswet AVG) of een last onder dwangsom (artikel 5:32 Awb) ter handhaving van de bij of krachtens de WGS gestelde verplichtingen.

Vraag 47 (PVV) – gevolgen niet-naleving regels gegevensbescherming
Kan zo gedetailleerd mogelijk worden aangegeven wat de juridische gevolgen kunnen zijn voor individuen en organisaties die de regels en waarborgen inzake privacy en gegevensbescherming direct of indirect aan hun laars lappen?

Verwezen wordt naar de beantwoording van *vraag 46 (PvdD) over sancties op niet-naleving verplichtingen* en *vraag 48 (PvdD) over verzoek burger tot handhaving*.

Vraag 48 (PvdD) – verzoek burger tot handhaving
Indien een verplichting niet is nagekomen, kan een burger dan om handhaving verzoeken? Zo nee, waarom is dat niet geregeld? Zo ja, op welke wijze? En heeft de burger dan toegang tot een onafhankelijke rechter indien niet wordt gehandhaafd?

Ja, een betrokkene kan op grond van artikel 77 AVG aan de AP verzoeken tot handhaving, door middel van het indienen van een zogeheten klacht. Op grond van artikel 78 AVG moet de AP de betrokkene binnen drie maanden in kennis stellen van de voortgang of het resultaat van de ingediende klacht. In het onverhoopte geval dat de AP niet binnen deze termijn heeft gereageerd op een verzoek tot handhaving, is er ingevolge artikel 6:2, aanhef en onderdeel b, van de Awb sprake van een besluit en kan er, onder de in artikel 6:12 van de Awb genoemde voorwaarden, beroep worden ingesteld bij de bestuursrechter. Een betrokkene heeft op grond van artikel 79, eerste lid, AVG ook het recht om een doeltreffende voorziening in rechte in te stellen tegen een verwerkingsverantwoordelijke als hij van mening is dat zijn rechten uit hoofde van de AVG worden geschonden omdat zijn persoonsgegevens niet in overeenstemming met de AVG worden verwerkt.[77] Dit recht is ook van toepassing bij de

[77] Dit recht is uitgewerkt in de artikelen 34, 35 en 36 Uitvoeringswet AVG, hoofdstuk 8 Awb en het Wetboek van Burgerlijke Rechtsvordering.

overtreding van een «gedelegeerde» nationale regel ter uitwerking van de AVG.[78] De WGS en de amvb vormen zo'n gedelegeerde nationale regel in de zin van artikel 6, derde lid, AVG.

Vraag 49 (PvdD) – informatie over niet-naleving
Hoe kan een burger erachter komen dat een in de WGS vervatte verplichting niet is nageleefd door een deelnemer of een samenwerkingsverband?

Een betrokkene kan kennisnemen van niet-naleving van de WGS via het nakomen van de informatieplicht door het samenwerkingsverband jegens betrokkene (artikel 14 AVG), door een inzageverzoek te doen (artikel 15 AVG), door de melding van een datalek (artikel 34 AVG) of door sanctionering door de AP, bijvoorbeeld indien uit de verplichte audits (artikel 1.10 WGS) een onrechtmatige gegevensverwerking zou blijken.

Vraag 50 (PvdD) – controle op vernietiging
Artikel 1.8, zevende lid WGS heeft betrekking op bewaring, vernietiging en hernieuwde verwerking van persoonsgegevens. Wie controleert of persoonsgegevens die niet meer bewaard mogen worden, daadwerkelijk worden vernietigd?

Het toezicht op de daadwerkelijke vernietiging vindt in eerste instantie plaats door middel van de privacy audits die in artikel 1.10 van het wetsvoorstel zijn voorgeschreven. Verder kan ook de Autoriteit Persoonsgegevens onderzoek naar de naleving van de voorschriften over de vernietiging van de verwerkte persoonsgegevens doen. Zoals nader toegelicht in de nota naar aanleiding van het verslag, kunnen informatiesystemen met toepassing van het in artikel 25 AVG vastgelegde principe van «Privacy by Design» zo worden ingericht dat gegevens uiterlijk vijf jaar na de datum van eerste verwerking automatisch worden vernietigd.[79]

Vraag 51 (PvdD) – niet-naleving geheimhoudingsplicht
Op welke wijze is de naleving en de handhaving van de geheimhoudingsplicht vervat in artikel 1.11 WGS gewaarborgd?

Niet-naleving van de geheimhoudingsplicht die is vervat in artikel 1.11 WGS kan leiden tot bestuurlijke handhaving, zoals een bestuurlijke boete, van de Autoriteit Persoonsgegevens of tot strafrechtelijke handhaving op grond van artikel 272 van het Wetboek van Strafrecht.

Vraag 52 (PvdD) – strafbaarheid ongeautoriseerde toegang
Indien een eerder door een deelnemer geautoriseerde persoon als bedoeld in artikel 1.8, tweede lid WGS zich toegang verschaft tot een systeem op een moment dat hij als gevolg van de intrekking of het vervallen van de autorisatie geen toegang meer zou mogen hebben, is dat dan strafbaar, vragen de PvdD-fractieleden.

Personen die opzettelijk en wederrechtelijk binnendringen in een ICT-systeem zijn strafbaar wegens computervredebreuk in de zin van artikel 138ab van het Wetboek van Strafrecht. Onder het binnendringen in een ICT-systeem kan ook vallen het inloggen op een besloten gedeelte van een site waartoe iemand vanwege wisseling van dienstverband niet meer gerechtigd was.[80]

---

[78] Zie uitgebreid P.T.J. Wolters, «De handhaving door de betrokkene onder de AVG», Tijdschrift voor Consumentenrecht en handelspraktijken 2019–1, p. 18.
[79] Kamerstukken II 2020/21, 35 447, nr. 6, antwoord 160, blz. 125.
[80] Rb. Den Haag 24 oktober 2008, ECLI:NL:RBSGR:2008:BG1507.

Vraag 53 (PvdD) – controle en toezicht op autorisaties
Welke wettelijke garantie bestaat er dat een persoon van wie de autorisatie is ingetrokken of vervallen geen toegang meer heeft? Wie ziet daar op toe? Waar is dat geregeld?

Uit artikel 1.8, achtste lid, van het wetsvoorstel volgt dat het samenwerkingsverband voldoende controlemechanismes moet inbouwen om na te gaan of de toegekende autorisaties allemaal nog kloppen. Op grond van die bepaling moeten de samenwerkingsverbanden zich namelijk houden aan de Baseline Informatiebeveiliging Overheid (BIO). In punt 9.2.5.3 van de BIO is bepaald dat een periodieke controle van de autorisaties verplicht is: «Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.» Dit dient ingebed te zijn in de organisatie van de deelnemers, maar ook van het samenwerkingsverband.
De verplichting tot logging van gegevensverwerkingen uit artikel 1.8, vierde lid, WGS draagt eraan bij dat ongeautoriseerde toegang traceerbaar is. De ICT-systemen moeten bovendien op grond van artikel 1.8, tweede lid, WGS zodanig worden ingericht dat iemand die geen autorisatie meer heeft ook niet in de systemen kan. In de informatiebeveiligingsaudits waartoe de BIO verplicht, of in de periodieke privacy audits waartoe artikel 1.10 van de WGS verplicht, kan naar voren komen of de autorisaties correct worden bijgehouden, en of sprake is geweest van ongeautoriseerde toegang.
De voorgaande regels zijn een concretisering van artikel 32 van de AVG, dat de verwerkingsverantwoordelijken verplicht tot het nemen van passende technische en organisatorische maatregelen teneinde veiligheidsrisico's tegen te gaan.
Niet-naleving van de voorgaande regels kan leiden tot handhaving door de AP, bijvoorbeeld door een bestuurlijke boete, afhankelijk van de omstandigheden van het geval.

Vraag 54 (PvdD) – betrouwbaarheidsvereisten
Waarom is in artikel 1.8, derde lid WGS bepaald dat betrouwbaarheidsvereisten met betrekking tot eventueel te autoriseren personen «kunnen» worden geregeld, in plaats van een wettelijk verplichting om dat bij AMvB te regelen?

De reden hiervoor is dat er al diverse andere betrouwbaarheidsvereisten worden toegepast op basis van andere wetgeving. Daargelaten of artikel 1.8, derde lid, WGS een verplichte of facultatieve delegatiegrondslag betreft, is dit uitgewerkt in artikel 1.11 concept-BGS. Dat is bedoeld als vangnetbepaling/minimumvereiste.

8. Uitvoering

Vraag 55 (SGP) – verhouding tot bestaande situatie en vereiste aanpassingen in de praktijk
De leden van de SGP-fractie lezen dat het wetsvoorstel noodzakelijk is vanuit het oogpunt van rechtsstatelijkheid. Gegevensverwerking tussen samenwerkingsverbanden dient op basis van een wettelijke grondslag plaats te vinden. De leden van de SGP-fractie vragen de regering of deze wettelijke grondslag een weergave is van de huidige gegevensverwerking tussen samenwerkingsverbanden en of dit wetsvoorstel slechts het «coderen» van de praktijk behelst of dat de samenwerkingsverbanden hun gegevensverwerkingsstructuur op een groot aantal vlakken moeten aanpassen.

Dankzij de WGS worden gegevensverwerkingen door bestaande samenwerkingsverbanden wettelijk ingekaderd. Hiermee kan er geen twijfel meer bestaan over de grenzen en grondslagen waaronder de

bestaande samenwerkingsverbanden mogen opereren. De WGS beschrijft welke gegevens er mogen worden gedeeld, voor welke doeleinden dat mag plaatsvinden en welke waarborgen daarvoor gelden. Het wetsvoorstel maakt ook duidelijk wanneer welke deelnemers van bepaalde samenwerkingsverbanden gegevens met elkaar mogen delen en verwerken. Met de WGS wordt daarmee de huidige gegevensverwerking tussen samenwerkingsverbanden van een duidelijke wettelijke basis voorzien. De deelnemers, de doeleinden en de verwerkingsactiviteiten blijven in de basis hetzelfde. In zoverre wordt het kader verduidelijkt en toekomstbestendig gemaakt. Zoals aangegeven in antwoord op vraag 1 van de nota naar aanleiding van het verslag[81], bevat het wetsvoorstel slechts in beperkte mate nieuwe verwerkingsmethoden, zoals de themagerichte analyse op subjectniveau door iCOV. In de memorie van toelichting is toegelicht dat het hierbij gaat om een deels nieuwe methode: de iCOV Rapportage Thema compact.[82] Ook nieuw is de mogelijkheid tot gegevensuitwisseling tussen samenwerkingsverbanden.[83]
Het wetsvoorstel heeft ook tot doel om in aansluiting op de AVG waarborgen te concretiseren die zijn vereist voor een goede bescherming van de persoonsgegevens die door deze samenwerkingsverbanden worden verwerkt. Daarom brengt het verplichtingen en waarborgen met zich mee, zoals de inrichting van een rechtmatigheidsadviescommissie, het uitvoeren van audits en het loggingsvereiste. Deze kunnen inderdaad betekenen dat processen en structuren zullen moeten worden aangepast. Veel van de waarborgen die opgenomen zijn in de WGS betreffen uitvloeisels van de reeds geldende privacywetgeving. De WGS vult deze waarborgen concreet in, zodat voor de deelnemers aan de samenwerkingsverbanden duidelijk is aan welke waarborgen zij moeten voldoen.

Vraag 56 (D66) – kwaliteit van de uitvoeringspraktijk
Daarbij nemen deze D66-leden het advies van de Raad van State ter harte. De Afdeling Advisering van de Raad van State stelt: «De Afdeling realiseert zich dat het wetsvoorstel potentieel vérgaande vormen van gegevensverwerking mogelijk maakt. Niet alle risico's die daarmee gepaard gaan kunnen door de wet worden uitgesloten. Cruciaal is daarom dat de wetgever moet kunnen vertrouwen op een kwalitatief goede uitvoeringspraktijk. Dat vereist niet of niet primair nadere regels of protocollen, maar professionaliteit en (ook juridische) deskundigheid op de werkvloer. De mate waarin dat wordt gerealiseerd zal bepalend zijn voor het vertrouwen in een overheid die rechtmatig én effectief persoonsgegevens verwerkt.» [84] Mede in het kader van de goede uitvoerbaarheid van het wetsvoorstel vragen de D66-fractieleden de regering aan te geven welk plan er uitgerold wordt om de noodzakelijke professionaliteit en (ook juridische) deskundigheid op de werkvloer te verbeteren en binnen welke termijn. Deze leden hebben daarbij tevens in gedachten de lessen die de (mede-)wetgever uit de kindertoeslagaffaire heeft getrokken.[85]

---

[81] Kamerstukken II 2020/21, 35 447, nr. 6.
[82] Zie artikel 2.13, onder d, WGS. Dit is toegelicht in Kamerstukken II 2019/20, 35 447, nr. 3, blz. 27 en is uitgewerkt in artikel 2.9 van het concept-BGS. Hierdoor is het voortaan mogelijk om niet alleen de risico's op witwassen in vogelvluchtperspectief te tonen, maar ook de betrokkenen daarbij. Zo wordt beter zicht verkregen op de criminele geldstromen. Zo kunnen politie en justitie ze nader onderzoeken of kunnen er andere maatregelen worden genomen om witwaspraktijken de pas af te snijden.
[83] Zie artikel 1.7, achtste lid, WGS. In artikel 1.10 van het concept-BGS wordt deze mogelijkheid afgebakend.
[84] Kamerstukken I 2021/22, 35 447, H, p. 1.
[85] Rapport «Zelfevaluatie naar aanleiding van de toeslagenaffaire», Eerste Kamer der Staten-Generaal 22 december 2021.

Met de vorige Minister van Justitie en Veiligheid (zie de brief van 17 december 2021, onder 7.3) ben ik van mening dat professionaliteit en (juridische) deskundigheid op de werkvloer van groot belang zijn. Om deze te verbeteren worden onder meer de volgende maatregelen getroffen:

– Artikel 1.17 concept-BGS bevat nadere waarborgen inzake de opleiding en training ten aanzien van gegevensverwerking.
– Het wetsvoorstel WGS voorziet in aanvullende waarborgen met betrekking tot de uitvoeringspraktijk, zoals de inrichting van rechtmatigheidsadviescommissies, waarvan de leden aan bepaalde kwaliteitseisen dienen te voldoen (zie artikel 1.14 concept-BGS), de betrouwbaarheidsvereisten voor personen in verband met toegang tot systemen (artikel 1.11 concept-BGS) en specifieke waarborgen bij het uitvoeren van een geautomatiseerde gegevensanalyse (artikel 1.9 WGS en artikel 2.11 en 2.12 concept-BGS).
– In de verplichte privacy audits en in de wettelijke verplichte evaluatie van de WGS zal ook de kwaliteit van de uitvoeringspraktijk bij de gegevensverwerking worden onderzocht.

De notie van de Afdeling advisering van de Raad van State laat overigens onverlet dat de samenwerkingsverbanden reeds veel benodigde kennis en expertise hebben opgebouwd. De in het wetsvoorstel WGS geregelde samenwerkingsverbanden zijn bestendig en kunnen bogen op ruime ervaring en expertise. Het FEC bestaat bijvoorbeeld al sinds 1998, de RIEC's sinds 2009 en iCOV sinds 2013. Er zijn dan ook al veel acties ondernomen in het kader van professionaliteit en deskundigheid op de werkvloer. De Zorg- en Veiligheidshuizen kennen al enkele jaren een trainingsprogramma, specifiek gericht op gegevensdeling en privacy. Ook fungeert aldaar de Werkgroep gegevensuitwisseling in het zorg- en veiligheidsdomein. ICOV kent reeds een rechtmatigheidsadviescommissie. Het FEC kent een privacy platform. Deze samenwerkingsverbanden kennen uitgebreide convenanten, privacy protocollen, werkprocessen en/of handboeken. Dat neemt niet weg dat professionaliteit en deskundigheid moeten worden verbeterd op de punten waarop de uitvoering niet overal even scherp verloopt. Deze punten kunnen niet alleen naar voren komen via de voornoemde verplichte privacy audits, de wetsevaluatie, of de rechtmatigheidsadviescommissies maar ook via de functionarissen gegevensbescherming, die volledig los van alle andere organisatieonderdelen opereren.

Vraag 57 (GroenLinks/PvdA) – investeren in de uitvoeringspraktijk
De mate waarin de uitvoeringspraktijk de vereiste zorgvuldigheid, deskundigheid en professionaliteit betracht, zal bepalend zijn voor de rechtmatigheid en effectiviteit van de verwerking van persoonsgegevens door de overheid, zo benadrukt de Raad van State in haar brief d.d. 18 november 2021. De consequenties van een ondermaatse uitvoeringspraktijk zijn dus groot.
De leden van de fracties van GroenLinks en PvdA vragen hoe de regering een goede uitvoeringspraktijk wil faciliteren en garanderen, zowel op het gebied van regels en protocollen, professionaliteit en (juridische) deskundigheid? Hoeveel extra fte hebben de afzonderlijke uitvoeringsinstanties nodig om dit te bewerkstelligen? Hoeveel middelen reserveert de regering om te investeren in professionaliteit en (juridische) deskundigheid, zoals de Raad van State adviseert? Indien er zich personeelstekorten voordoen, in het heden of in de toekomst, welke stappen neemt het kabinet om de kwaliteit van de uitvoeringspraktijk te bewaken?

De regering onderkent het belang van een goede uitvoeringspraktijk. Zoals opgemerkt in de brief van de Minister van Justitie en Veiligheid aan de Eerste en Tweede Kamer van 17 december 2021 dient de overheid vanzelfsprekend te waarborgen dat wordt geïnvesteerd in professionaliteit

en (juridische) deskundigheid op de werkvloer.[86] Verwezen wordt verder naar *vraag 56 (D66) – kwaliteit van de uitvoeringspraktijk*.
In hoeverre de invoering en naleving van de aanvullende waarborgen, zoals die worden uitgewerkt in het BGS, een lastenverzwaring met zich meebrengen voor de deelnemers, en welke middelen daarvoor benodigd zijn, zal moeten blijken uit de uitvoeringstoetsen die worden uitgevoerd ten tijde van de consultatie inzake deze amvb. Deze zijn niet op voorhand te kwantificeren, maar bedacht moet worden dat het wetsvoorstel en het concept-BGS in substantiële mate een specificering of concretisering vormen van regels die samenwerkingsverbanden nu al op basis van de AVG moeten toepassen en dat de in de WGS opgenomen samenwerkingsverbanden bestendig zijn en kunnen bogen op ruime ervaring en expertise, zoals is toegelicht in het antwoord op de vorige vraag.

Vraag 58 (PvdD) – kwalitatief goede uitvoeringspraktijk
De Raad van State wijst op risico's: «De Afdeling realiseert zich dat het wetsvoorstel potentieel vergaande vormen van gegevensverwerking mogelijk maakt. Niet alle risico's die daarmee gepaard gaan, kunnen door de wet en de daarop gebaseerde AMvB's worden uitgesloten. Cruciaal is daarom dat de wetgever moet kunnen vertrouwen op een kwalitatief goede uitvoeringspraktijk. (...) Dat vereist niet primair nadere regels of protocollen, maar professionaliteit en (ook juridische) deskundigheid op de werkvloer.» [87] Is die professionaliteit, deskundigheid en een bestuurscultuur die doordrongen is van het voorkomen van onterechte inbreuken op grondrechten, naar het oordeel van de regering op dit moment voldoende gewaarborgd, zo vragen de aan het woord zijnde leden. Zo ja, aan welke onderzoeksgegevens ontleent de regering een grond voor dat oordeel? Zo nee, is de regering bereid om de WGS pas in werking te stellen indien door middel van onafhankelijk onderzoek is vastgesteld dat die vereiste professionaliteit, deskundigheid en bestuurscultuur die doordrongen is van het voorkomen van onterechte inbreuken op grondrechten, is gegarandeerd?

Verwezen wordt naar het antwoord op *vraag 56 (D66) – kwaliteit van de uitvoeringspraktijk*, waaruit blijkt dat het niet zo is dat pas na inwerkingtreding van de WGS de kennis en expertise opgebouwd gaat worden. Het betreft bestendige samenwerkingsverbanden waarin professionals reeds samenwerken op het terrein van zorgvuldige gegevensdeling en privacy. De WGS roept extra waarborgen in het leven. In periodiek onderzoek naar professionaliteit, deskundigheid en bestuurscultuur wordt in feite voorzien door de verplichte privacy audits, de verplichte coördinerend functionaris voor gegevensbescherming, het toezicht door de AP, en de verplichte wetsevaluatie.

Vraag 59 (CU) – zorgvuldige uitvoeringspraktijk
Uit de reacties en adviezen volgt bij herhaling dat een zorgvuldige praktijk van uitvoering van vitaal belang is om gegevens te verwerken op een manier die burgers recht doet. Kan de regering nader toelichten wie daadwerkelijk met de uitvoering van deze regels zijn en zullen worden belast? En in hoeverre is daar sprake van investeringen in professionaliteit en (juridische) deskundigheid op de werkvloer, evenals in een cultuur waarin kan en mag worden afgeweken van algoritmische uitkomsten[88], zoals de Raad van State zo fraai formuleert?

---

[86] Kamerstukken II 2021/22, 35 447, nr. 21, paragraaf 7.3.
[87] Kamerstukken I 2021/22, 35 447, H, p. 1.
[88] Kamerstukken I 2021/22, 35 447, H, p. 1–2.

Op grond van artikel 1.4, derde lid, van het wetsvoorstel wijzen de deelnemers van de samenwerkingsverbanden personeel aan ten behoeve van de inzet in het samenwerkingsverband. Deze deelnemers zijn opgesomd in het wetsvoorstel, met enkele aanvullingen in het concept-BGS. Dit personeel is feitelijk belast met de uitvoering van deze regels. Voor het antwoord op de overige vragen verwijs ik naar het antwoord op *vraag 56 (D66) – kwaliteit van de uitvoeringspraktijk* en *vraag 57 (GroenLinks/PvdA) – investeren in de uitvoeringspraktijk* en *vraag 40 (VVD) – expertise inzake algoritmen en tegengaan ongewenste profilering*.

Vraag 60 (PVV) – organisaties toegerust voor uitvoering
Zijn de betreffende organisaties meer dan voldoende toegerust (zowel «kwalitatief», als «kwantitatief») om de taken m.b.t. voorliggend wetsvoorstel uit te voeren? Graag ontvangen de leden een gemotiveerd antwoord.

Dit zal nader worden onderzocht in de te verrichten uitvoeringstoetsen op het concept-BGS, maar bedacht moet worden dat het wetsvoorstel en het concept-BGS in substantiële mate een specificering of concretisering vormen van regels die samenwerkingsverbanden nu al op basis van de AVG moeten toepassen en dat de in de WGS opgenomen samenwerkingsverbanden bestendig zijn en kunnen bogen op ruime ervaring en expertise, zoals is toegelicht in het antwoord op de vorige vraag. Verwezen wordt verder naar de beantwoording van *vraag 56 (D66) – kwaliteit van de uitvoeringspraktijk* en *vraag 57 (GroenLinks/PvdA) – investeren in de uitvoeringspraktijk*.

Vraag 61 (SGP) – regeldruk door het wetsvoorstel
De leden van de SGP-fractie lezen dat gegevensverwerking onmiskenbaar een belangrijk instrument is in de bestrijding van ernstige en ondermijnende criminaliteit. Deze leden onderschrijven de noodzaak dat samenwerkingsverbanden in de bestrijding van deze criminaliteit hun werk adequaat moeten kunnen blijven uitvoeren en niet onnodig tegen vertragende regelgeving aan moeten lopen. De leden van de SGP-fractie vragen de regering of het wetsvoorstel zélf niet voor onnodige vertraging zorgt in de bestrijding van ondermijnende criminaliteit en of de samenwerkingsverbanden hun werk ongestoord kunnen blijven voortzetten. Deze leden vragen de regering of zij kan aantonen dat dit wetsvoorstel niet voor een ongewenst grote regeldruk voor de samenwerkingsverbanden zorgt. Kan de regering deze verhoging van de regeldruk in kaart brengen?

Het wetsvoorstel is tweeledig: enerzijds brengt het een verruiming met zich mee van de mogelijkheden om gegevens te delen en gezamenlijk te verwerken, anderzijds komen er waarborgen waaraan moet zijn voldaan. Het wetsvoorstel brengt daarmee het nodige evenwicht aan tussen enerzijds de belangen van de samenwerkingsverbanden en anderzijds de in acht te nemen normen op het gebied van onder meer gegevensbescherming. Veel van de waarborgen in het wetsvoorstel vloeien voort uit de reeds bestaande privacywetgeving, en worden in het wetsvoorstel concreet ingevuld waardoor voor de deelnemende partijen aan de samenwerkingsverbanden duidelijk is aan welke waarborgen zij dienen te voldoen. Ten aanzien van enkele aanvullende waarborgen is het aannemelijk dat deze leiden tot administratieve lastenverzwaring, waaronder met name de inrichting van een rechtmatigheidsadviescommissie, het uitvoeren van audits en het loggingsvereiste. Deze waarborgen kunnen echter bijdragen aan het verminderen van de risico's voor rechten en vrijheden van betrokkenen en het voorkomen van lasten als gevolg van onrechtmatige verwerkingen of informatiebeveiligingsincidenten. De waarborgen zullen worden uitgewerkt in het concept-BGS. Op de vraag of

de regering deze verhoging van de regeldruk in kaart kan brengen, kan ik antwoorden dat er uitvoeringstoetsen zullen worden aangevraagd, die hierover meer duidelijkheid moeten bieden, en dat er in de nota van toelichting op voornoemd besluit nader op de regeldruk zal worden ingegaan.

Tegenover een verzwaring van de regeldruk staat dat de WGS ook zorgt voor een verlichting daarvan. Het wetsvoorstel WGS creëert heldere grondslagen voor multilaterale gegevensverwerking en voorziet de huidige gegevensverwerkingen van een duidelijk juridisch kader. Aldus zorgt de WGS juist voor meer overzichtelijkheid en duidelijkheid over wat wel en wat niet mag, en welke waarborgen concreet vereist zijn. Hierdoor is minder tijd en capaciteit benodigd om uit te zoeken wat juridisch is toegestaan, welke waarborgen vereist zijn, en het daar over eens te worden. Hiermee wordt een einde gemaakt aan de bestaande situatie, waarin de samenwerkingsverbanden kampen met versnippering, onvolledigheid en grote complexiteit in de gegevensuitwisseling, evenals onduidelijkheden omtrent de grondslagen, omdat bestaande sectorale wetgeving onvoldoende rekening houdt met de integrale werkwijze van deze samenwerkingsverbanden.
Al met al meen ik dat het wetsvoorstel de juiste balans heeft gevonden tussen de verschillende te beschermen belangen en dat van onnodige regeldruk geen sprake zal zijn.

Vraag 62 (SGP) – spanningsveld privacy en effectief bestrijden van ondermijnende criminaliteit
De leden van de SGP-fractie lezen dat de regering met het wetsvoorstel vanuit rechtsstatelijk oogpunt een afweging maakt tussen enerzijds de waarborging van het recht op eerbiediging van de persoonlijke levenssfeer en het recht op bescherming van persoonsgegevens en anderzijds het effectief bestrijden van ondermijnende criminaliteit. Deze leden vragen de regering of het effectief bestrijden van ondermijnende criminaliteit niet ondergeschikt raakt aan het beschermen van persoonsgegevens van criminelen.

Het effectief bestrijden van ondermijnende criminaliteit raakt niet ondergeschikt aan het recht op gegevensbescherming van betrokkenen, maar wordt bevorderd door heldere grondslagen te bieden voor multilaterale gegevensverwerking en daarvoor een duidelijk juridisch kader te scheppen. Het wetsvoorstel neemt de onduidelijkheid weg die samenwerkingsverbanden ervaren over de bestaande juridische mogelijkheden en die nu leidt tot handelingsverlegenheid waar die niet zou hoeven te bestaan. Onder de huidige wetgeving verschilt het bijvoorbeeld per deelnemer of en in welke mate een deelnemer gegevens met het samenwerkingsverband mag delen of van het samenwerkingsverband mag ontvangen. De consequentie hiervan is dat de deelnemers aan een samenwerkingsverband, zelfs als zij ieder voor zich de fragmenten hebben die nodig zijn om de complexe puzzel van de criminaliteitsbestrijding op te lossen, die puzzeldelen nu niet volledig bij elkaar mogen leggen. Het wetsvoorstel maakt een einde aan deze versnippering van informatie door te zorgen voor heldere juridische grondslagen voor gezamenlijke gegevensverwerking. Dat voorkomt dat samenwerkingsverbanden in een grijs gebied moeten opereren waarvan de grenzen niet altijd helder zijn. Die helderheid stelt de samenwerkingsverbanden in staat effectiever te functioneren. Ook volgens de Afdeling advisering van de Raad van State – aldus haar advies uit 2019 – is rechtszekerheid nodig om als samenwerkingsverband effectief te kunnen functioneren en is het daarom ook nodig om in het wetsvoorstel regels op te nemen over de voorwaarden en de

waarborgen die de samenwerkingsverbanden moeten treffen.[89] Dit advies is opgevolgd. De voorwaarden en waarborgen zijn nodig om de gegevensverwerkingen juridisch houdbaar te laten zijn in het licht van de AVG en artikel 8 EVRM.
De regering meent met het aangepaste wetsvoorstel een evenwichtig en proportioneel kader te hebben gecreëerd voor de gezamenlijke verwerking van gegevens door samenwerkingsverbanden, waarbij mogelijkheden tot informatie-uitwisseling gepaard gaan met heldere begrenzing van deze mogelijkheden en waarborgen ter bescherming van het belang van de privacy van burgers. Wanneer er een grondslag voor de verwerking van persoonsgegevens bestaat en de verwerking zelf vindt zorgvuldig plaats, dan is er binnen de kaders van de privacywetgeving en het wetsvoorstel WGS veel mogelijk. Bij elke casus zal steeds een afweging moeten worden gemaakt welke gegevens met welke deelnemers kunnen worden gedeeld en of dat noodzakelijk is voor het realiseren van het doel van het samenwerkingsverband.
Overigens is het op voorhand geen gegeven dat sprake is van «persoonsgegevens inzake criminelen», zoals de vraagstelling lijkt te impliceren. Om aan gegevensverwerking in de samenwerkingsverbanden toe te komen, is onder meer vereist dat er duidelijke en objectieve aanwijzingen zijn voor risico's met het oog op de doelen van het samenwerkingsverband. Dat wil niet zeggen dat een verdenking van een strafbaar feit is vereist. Het gaat om een integrale aanpak van deze risico's: zo is bijvoorbeeld ook bestuursrechtelijke handhaving denkbaar of zorg, in het geval van de Zorg- en Veiligheidshuizen.

Vraag 63 (SGP) – afwegingskader privacy en effectieve misdaadbestrijding
De leden van de SGP-fractie lezen dat de proportionaliteit tussen enerzijds de bescherming van persoonsgegevens en anderzijds de effectieve misdaadbestrijding noodzakelijk afgewogen dient te worden. Kan de regering aangeven hoe in de praktijk dit afwegingskader vorm krijgt voor de samenwerkingsverbanden? Is er een duidelijk kader of besluitvormingsproces waarin zij adequaat stappen kunnen nemen? Kunnen zij nog wel tot actie overgaan of worden zij geremd door procedures waarin de bescherming van persoonsgegevens moet worden afgewogen?

De afweging tussen de bescherming van persoonsgegevens en effectieve misdaadbestrijding is verankerd in de vormgeving van het wetsvoorstel en de bijbehorende amvb, door voorwaarden te stellen waaronder kan worden samengewerkt. Voor alle samenwerkingsverbanden geldt dat elke deelnemer uit het samenwerkingsverband op grond van artikel 1.5 van het wetsvoorstel te allen tijde een gedegen afweging moet maken of de gegevensverstrekking aan het samenwerkingsverband noodzakelijk is gelet op het doel daarvan, of er zwaarwegende redenen zijn die zich tegen gegevensverstrekking verzetten en of de gegevensverstrekking valt onder de in de WGS opgesomde categorieën gegevens.
De gegevensverwerking start met de aanmelding van een signaal, verzoek of casus door een deelnemer. Het concept-BGS stelt hieraan nadere eisen. Als een signaal, verzoek of casus in behandeling wordt genomen, dan moeten bovendien de specifieke stappen worden gevolgd die zijn opgenomen in de bepalingen over het betreffende samenwerkingsverband, zoals artikel 2.23 WGS voor de RIEC's en artikel 2.31 WGS voor de Zorg- en Veiligheidshuizen. De verwerking van persoonsgegevens door het samenwerkingsverband eindigt indien dit niet meer noodzakelijk is voor het doel van het samenwerkingsverband, maar in ieder geval uiterlijk na vijf jaar (artikel 1.8, zevende lid, WGS), behoudens een uitzondering,

[89] Kamerstukken II 2019/20, 35 447, nr. 4, blz. 7.

waarop is ingegaan in het antwoord op *vraag 26 (PvdD) – uitzonderingen op maximale bewaartermijn*.

9. Financiering

Vraag 64 (PvdA/GroenLinks) – wijze van financiering WGS
In het kader van de uitvoerbaarheid en daarmee de rechtmatigheid van de WGS maken de fractieleden van de PvdA en GroenLinks zich zorgen over de (financiële) ondersteuning van de samenwerkingsverbanden. In oktober 2019 is de motie-Rosenmöller[90] aangenomen.
Is de regering op de hoogte van de conclusie van een door Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC), Stichting Economisch Onderzoek (SEO) en onderzoeksbureau Andersson Elffers Felix (AEF) uitgevoerd onderzoek n.a.v. de motie-Rosenmöller dat ketensamenwerking tussen de politie, het Openbaar Ministerie (OM) en de rechtspraak wordt bemoeilijk door de wijze van financiering, namelijk een wisselend beleid in bekostigingssystematieken en de beschikbaar gestelde middelen?[91] Op welke wijze worden de samenwerkingsverbanden in de WGS gefinancierd? Heeft de regering hiervoor extra financiële middelen gereserveerd?

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

Vraag 65 (PvdA/GroenLinks) – appreciatie motie-Rosenmöller
Heeft de regering een soortgelijke analyse uitgevoerd naar de mogelijke risico's van de wijze van financiering van samenwerkingsverbanden op de kwaliteit van de uitvoeringspraktijk? Zo nee, is de regering voornemens dit te onderzoeken en de conclusies van zo'n onderzoek te vertalen naar gepaste (financiële) maatregelen? Is de regering op de hoogte dat het vorige kabinet de bevindingen van bovenstaand rapport apprecieert als een belangrijke les voor de toekomst, «want continuïteitsrisico's voor de individuele organisaties in de rechtsstaat komen uiteindelijk ook niet ten goede aan het functioneren van de rechtsstaat als zodanig».[92] Is de regering op de hoogte dat de status van de motie-Rosenmöller «niet uitgevoerd» is? De fractieleden van GroenLinks en de PvdA horen graag de appreciatie van de nieuwe regering en zijn concrete plannen om uitvoering te geven aan deze motie in het kader van de WGS. Hoe bewaakt en versterkt de regering de onafhankelijke rechtstaat bij de uitvoering van de WGS?

In de brief van 20 april 2022 van mijn collega voor Rechtsbescherming en van mij is uw Kamer inmiddels geïnformeerd over wat er sinds het verschijnen van het onderzoek met de aanbevelingen is gedaan.[93] Het wetsvoorstel heeft overigens geen implicaties voor de wijze van finan-

---

[90] Kamerstukken I 2019/20, 35 300, C.
[91] Kamerstukken I 2020/21, 35 300 VI / 35 300 BK; Eindrapport «Continuïteit in de bekostiging van politie, openbaar ministerie en rechtspraak.» WODC, Amsterdam, maart 2021.
[92] Kamerstukken I 2020/21, 35 300 VI / 35 300 BK, p. 2.
[93] *Kamerstukken I 2021/22, 35 300 VI, nr. BP .*

ciering van samenwerkingsverbanden. Er is dan ook geen aanleiding om hiernaar in het kader van de WGS onderzoek te verrichten.

10. Kunstmatige intelligentie

Vraag 66 (GroenLinks/PvdA) – kunstmatige intelligentie en zelflerende systemen
Wordt daarbij (bij de geautomatiseerde gegevensanalyse, red.) *gebruik gemaakt van kunstmatige intelligentie en zelflerende systemen?*

Zelflerende systemen of kunstmatige intelligentie zijn niet aan de orde in de samenwerkingsverbanden die door het wetsvoorstel worden geregeld, zoals nader is toegelicht aan het begin van het antwoord op *vraag 38 (PvdA/GroenLinks) – evaluatie en toezicht geautomatiseerde gegevensanalyse*.
Systemen die nu getypeerd worden als «Artificiële Intelligentie» zijn in de praktijk gebaseerd op «Machine Learning».[94] Bij Machine Learning wordt, op basis van algoritmes en grote hoeveelheden voorbeelddata, een computer getraind om een bepaalde taak uit te voeren. Machine Learning is gebaseerd op algoritmes die in staat zijn om te leren op basis van eerdere ervaringen, zogenoemde zelflerende algoritmes. Het is dit zelflerende karakter dat Machine Learning algoritmes onderscheidt van «traditionele» computeralgoritmes.
Artikel 1.9, zesde lid, WGS, verbiedt bovendien om algoritmes te hanteren waarvan de uitkomsten niet navolgbaar en controleerbaar zijn. Wanneer gebruik is gemaakt van zelflerende algoritmes is de toets hoe de uitkomsten tot stand zijn gekomen nagenoeg onmogelijk.
Het is wel toegestaan om zelflerende algoritmes te gebruiken als de input en output te controleren zijn. Bij bijvoorbeeld entiteitsextractie leert de computer bijvoorbeeld zelf bankrekeningnummers uit een tekstdeel te halen. Op die manier kan informatie uit een stuk tekst anders weergegeven worden en op die manier geschikter gemaakt worden voor analyse met andere data.
ICOV sluit aan bij de Richtlijnen voor het toepassen van algoritmen door overheden en publieksvoorlichting over data-analyses.[95] Algoritmes moeten technisch transparant en uitlegbaar of auditeerbaar zijn.

Vraag 67 (PvdA/GroenLinks) – risico's kunstmatige intelligentie
De leden van de fractie van de PvdA en GroenLinks maken zich zorgen over het risico van een glijdende schaal als het gaat om de toepassing van kunstmatige intelligentie (KI) bij de geautomatiseerde analyse van persoonsgegevens en het risico op discriminatie. Op welke wijze is gegarandeerd dat in bezwaar en beroep voldoende kennis aanwezig is van de geautomatiseerde processen waarvan gebruik is gemaakt? Dit geldt voor zowel de verstrekking van de relevante gegevens hieromtrent als voor de kennis deze zinvol te kunnen interpreteren.

Zoals is toegelicht in het antwoord op de vorige vraag, is kunstmatige intelligentie in het wetsvoorstel niet aan de orde. Ten aanzien van geautomatiseerde gegevensanalyse in de zin van het wetsvoorstel deelt de regering de vrees voor het risico van een glijdende schaal niet. Voor zover dit wetsvoorstel geautomatiseerde gegevensanalyse (nu of in de toekomst) mogelijk maakt, worden daaraan immers specifieke waarborgen verbonden in het voorgestelde artikel 1.9 en in de amvb. Aan dat artikel is door een amendement van het toenmalig Tweede Kamerlid Buitenweg (GroenLinks) nog een zesde lid toegevoegd, luidende dat bij

[94] Autoriteit Persoonsgegevens, Toezicht op AI & Algoritmes, 2020, p. 4.
[95] https://www.rijksoverheid.nl/documenten/richtlijnen/2021/09/24/richtlijnen-voor-het-toepassen-van-algoritmen-door-overheden-en-publieksvoorlichting-over-data-analyses

geautomatiseerde gegevensanalyse geen algoritmes worden gehanteerd waarvan de uitkomsten niet navolgbaar en controleerbaar zijn. Uiteraard is het van groot belang dat binnen de samenwerkingsverbanden de nodige expertise voorhanden is. In dit verband zij verwezen naar de antwoorden op de vragen 56 en 57 over de professionaliteit en (juridische) deskundigheid op de werkvloer.
Verder speelt in het kader van de te betrachten zorgvuldigheid binnen de opsporing het Kwaliteitskader Big Data[96] een rol, dat is opgesteld door de politie en het OM. Dit wordt gebruikt voor het toetsen van big data toepassingen aan rechtmatigheid en ethiek. Hierin komen onder meer terug de richtlijnen voor het toepassen van algoritmes door de overheid uit de brief van 8 oktober 2019.[97] Het kwaliteitskader ziet op de ontwikkeling en toepassing van algoritmes en data-analysemethoden in de opsporing.

Vraag 68 (PvdD) – Zelflerende algoritmen
De leden van de PvdD-fractie vragen de regering of aangeven kan worden welke belangen geschaad worden indien verboden wordt om zelflerende algoritmen toe te passen?

Verwezen wordt naar het antwoord op *vraag 66 (GroenLinks/PvdA) – kunstmatige intelligentie en zelflerende systemen*.

11. Amendement of novelle over bij amvb nieuwe samenwerkingsverbanden regelen

Vraag 69 (CU) – aanwijzing nieuwe samenwerkingsverbanden
De vier bestaande samenwerkingsverbanden (FEC, ICOV, RIEC en ZVH) worden nu genoemd in de tekst van de wet in formele zin. Eventuele toekomstige samenwerkingsverbanden worden volgens het wetsvoorstel echter aangewezen bij AMvB. De leden van de ChristenUnie-fractie vragen de regering welke inhoudelijke motivatie aan deze keuze ten grondslag ligt. En is de regering bereid nu reeds toe te zeggen dat het wetsvoorstel op dit onderdeel zal worden aangepast, zodat elk samenwerkingsverband waarop de voorgestelde wettelijke regeling betrekking zal hebben bij formele wet zal worden aangewezen? De Raad van State suggereerde nog een spoedvoorziening bij AMvB. Hoe kijkt de regering daar tegenaan? Zijn er concrete situaties te noemen waarin een dergelijke spoedvoorziening in de afgelopen jaren nodig zou zijn geweest?

In §5.1 van zijn brief van 17 december 2021 heeft de toenmalige Minister van Justitie en Veiligheid geschreven dat hij bereid is om toe te zeggen dat de artikelen 3.1 tot en met 3.3, die de mogelijkheid regelen om nieuwe samenwerkingsverbanden bij amvb te regelen, niet in werking zullen treden, en dat een wetsvoorstel wordt ingediend waarmee die artikelen worden aangepast.[98] Ik ben hiertoe eveneens bereid.
De bevoegdheid is gewenst met het oog op gevallen waarin de totstandkoming van een wet in formele zin niet kan worden afgewacht. Tijdelijke delegatie is hiervoor een oplossing, omdat hierbij de voorschriften tijdelijk bij amvb kunnen worden vastgesteld, mits zo spoedig mogelijk een wetsvoorstel wordt ingediend om het betreffende samenwerkingsverband alsnog in de wet te regelen. De amvb wordt dan uiteindelijk ingetrokken op het tijdstip van inwerkingtreding van dat wetsvoorstel, of onverwijld nadat het wetsvoorstel is verworpen.

---

[96] Kamerstukken II 2019/20, 29 628, nr. 948, bijlage «Kwaliteitskader Big data».
[97] Kamerstukken II 2018/19, 29 628, 641.
[98] Kamerstukken II 2021/22, 35 447, nr. 21, blz. 4.

Zoals aangegeven in de nota naar aanleiding van het verslag bij het wetsvoorstel,[99] heeft de WGS geen implicaties voor de talloze bestaande samenwerkingsverbanden die binnen de grenzen van het huidige recht voldoende ruimte hebben om op de door hen gewenste wijze persoonsgegevens te verwerken. Niet kan worden uitgesloten dat zich bij die samenwerkingsverbanden ontwikkelingen voordoen, die nopen om met spoed een regeling te treffen voor de gegevensverwerking in een samenwerkingsverband, bijvoorbeeld indien juridische lacunes rijzen die een spoedige oplossing behoeven omwille van een optimale, effectieve samenwerking van dat samenwerkingsverband.
Tegen de achtergrond dat de mogelijkheid van tijdelijke delegatie bedoeld is voor situaties waarin de totstandkoming van formele wetgeving niet kan worden afgewacht, is het niet goed mogelijk om een volledige inventarisatie te geven van samenwerkingsverbanden waarvoor tijdelijke delegatie nodig zal blijken. Gedacht kan worden aan een samenwerkingsverband ten behoeve van het voorkomen of bestrijden van een ernstige vorm van criminaliteit – bijvoorbeeld cybercrime – dat de bevoegdheid mist om gemeenschappelijke casusanalyses of data-analyses te verrichten. Om die tijdig en adequaat te kunnen regelen, zou het samenwerkingsverband dan tijdelijk in een amvb kunnen worden geregeld. Omdat er de afgelopen jaren geen grondslag is geweest voor zo'n spoedvoorziening, is het ook lastig om met terugwerkende kracht te beoordelen in welke concrete situaties een spoedvoorziening nodig zou zijn geweest, bijvoorbeeld omdat daarvoor inmiddels een andere voorziening is getroffen. Te denken valt aan het wetsvoorstel gegevensverwerking casusoverleggen radicalisering en terroristische activiteiten.[100]

Vraag 70 (D66) – mogelijke aanpassingen van het wetsvoorstel
Over uitbreiding van de vier in de tekst van het wetsvoorstel genoemde samenwerkingsverbanden zijn zowel de Autoriteit Persoonsgegevens als de Afdeling Advisering van de Raad van State kritisch. Daarop heeft de regering toegezegd dat de artikelen 3.1 tot en met 3.3 WGS, die de mogelijkheid regelen om nieuwe samenwerkingsverbanden bij AMvB te regelen, niet in werking zullen treden, en dat een wetsvoorstel wordt ingediend waarmee die artikelen worden aangepast. Met deze toezegging, aldus de regering, hoeft in de tussentijd het wetsvoorstel dat die drie artikelen aanpast de behandeling van het onderhavige wetsvoorstel niet op te houden. Wat de leden van de D66-fractie betreft zijn hiermee niet al hun zorgen alsmede die geformuleerd door de Raad van State weggenomen. Zoals hierboven besproken geldt voor veel meer onderdelen dat de invulling van de wettelijke normering nog vrijwel geheel bij AMvB moet plaats hebben. De toezegging van de regering dat de artikelen 3.1 tot en met 3.3 WGS niet in werking zullen treden voordat een wetsvoorstel is ingediend waarin die artikelen worden aangepast, komt de leden van de D66-fractie mager voor. Zie alleen al het feit dat door de Raad van State wordt gehamerd op het cruciaal zijn van een kwalitatief hoogstaande uitvoering en professionaliteit en (juridische) deskundigheid op de werkvloer, terwijl ook ten aanzien van de aan de bij die uitvoering betrokken personen te stellen opleidingseisen geldt dat die nog bij of krachtens AMvB van nadere regels zullen worden voorzien (art 1.8 lid 9). De leden van de D66-fractie zouden graag van de regering vernemen hoe de aanpassing van de wetsartikelen er uit komt te zien, en op welke termijn het wetsvoorstel bij de Tweede Kamer wordt ingediend. Bovendien wensen deze leden te vernemen waarom de regering er niet

---

[99] *Kamerstukken II 2020/21, 35 447, nr. 6,* antwoorden 42 en 106, blz. 35–36 en blz. 89.
[100] Het bij koninklijke boodschap van 15 oktober 2022 ingediende voorstel van wet houdende regels omtrent gegevensverwerking in de persoonsgerichte aanpak van radicalisering en terroristische activiteiten (Wet gegevensverwerking persoonsgerichte aanpak radicalisering en terroristische activiteiten, Kamerstukken 36225).

voor heeft gekozen een novelle in te dienen waar nog meer verbeteringsslagen in de tekst kunnen worden verwerkt ervan uitgaande dat de behandeling van een novelle niet veel langer hoeft te duren dan die van het door de regering geopperde tijdelijke delegatievoorstel.

Het kabinet is voornemens de artikelen 3.1 tot en met 3.3 aan te passen om te regelen dat uitsluitend in geval van spoed een nieuw samenwerkingsverband bij amvb kan worden geregeld en dat in dat geval zo spoedig mogelijk een wetsvoorstel moet worden ingediend om het betreffende samenwerkingsverband alsnog in de wet te regelen. Dit betreft «tijdelijke delegatie». Volgens aanwijzing 2.39 van de Aanwijzingen voor de regelgeving betekent tijdelijke delegatie dat na de plaatsing van de amvb in het Staatsblad zo spoedig mogelijk een wetsvoorstel wordt ingediend. Indien een van de beide Kamers der Staten-Generaal het wetsvoorstel verwerpt, wordt de amvb onverwijld ingetrokken. Wordt het voorstel tot wet verheven, dan wordt de amvb ingetrokken op het tijdstip van inwerkingtreding van die wet. Uit de formulering van de modelbepaling in aanwijzing 2.39 blijkt dat hier geen sprake is van een voor- of nahangprocedure, maar dat het parlement invloed uitoefent in de vorm van wel of niet aannemen van een wetsvoorstel dat automatisch op de amvb volgt. In de grondslag voor tijdelijke delegatie moet worden opgenomen dat de amvb onverwijld wordt ingetrokken indien het wetsvoorstel wordt ingetrokken of indien een van de beide Kamers der Staten-Generaal besluit het wetsvoorstel niet aan te nemen.

De voorgenomen aanpassing van de artikelen 3.1 tot en met 3.3 van de WGS betreft geen novelle, maar een wetsvoorstel dat procedureel geen afhankelijkheid kent met het onderhavige wetsvoorstel. Ik volg mijn ambtsvoorganger hierin. Met die toezegging hoeft in de tussentijd het wetsvoorstel dat die drie artikelen aanpast de behandeling van het onderhavige wetsvoorstel niet op te houden. Ik deel de opvatting van de Afdeling advisering dat aldus op korte termijn recht kan worden gedaan aan het belang om de gegevensverwerking binnen bestaande samenwerkingsverbanden van een toereikende wettelijke grondslag te voorzien.

Vraag 71 (GroenLinks/PvdA) – nieuwe samenwerkingsverbanden
De Raad van State stelt in zijn advies dat het onduidelijk is of het wetsvoorstel, dat nu het de wezenlijke elementen van nieuwe samenwerkingsverbanden middels een algemene maatregel van bestuur (AMvB) regelt, in het licht van artikel 10 van de Grondwet een adequate wettelijke grondslag biedt voor de beoogde verwerking en verstrekken van gegevens. Wat is de reactie van de regering hierop? Wil de regering ervoor zorgen dat de wezenlijke elementen van een nieuw samenwerkingsverband uiteindelijk bij wet worden geregeld, zoals de Raad van State adviseert, en zo ja hoe? Wat is de reactie van de regering op het advies van de Autoriteit Persoonsgegevens om de mogelijkheid van het oprichten van een nieuw samenwerkingsverband bij AMvB te schrappen?

In de hiervoor genoemde brief van 17 december 2021 heeft de Minister van Justitie en Veiligheid toegezegd dat de artikelen 3.1 tot en met 3.3, die de mogelijkheid regelen om nieuwe samenwerkingsverbanden bij amvb te regelen, niet in werking zullen treden, en dat een wetsvoorstel wordt ingediend waarmee die artikelen worden aangepast. Deze mogelijkheid zal worden beperkt tot spoedgevallen, voor de tijd die nodig is ter overbrugging om een wetswijziging tot stand te brengen om het betreffende samenwerkingsverband in de WGS zelf te regelen.[101]

[101] Kamerstukken II 2021/22, 35 447, nr. 21, blz. 4.

Vraag 72 (PVV) – aanpassing artikelen over nieuwe samenwerkingsverbanden
De leden van de fractie van PVV lezen op pagina 4 van de brief van 17 december 2021 het volgende: «Gelet op de voorlichting van de Afdeling advisering ben ik bereid om toe te zeggen dat de artikelen 3.1 tot en met 3.3, die de mogelijkheid regelen om nieuwe samenwerkingsverbanden bij AMvB te regelen, niet in werking zullen treden, en dat een wetsvoorstel wordt ingediend waarmee die artikelen worden aangepast.» [102] *en vragen de regering wanneer het wetsvoorstel kan worden verwacht?*

Het streven is het wetsvoorstel in de eerste helft van 2023 aan de Afdeling advisering van de Raad van State te kunnen voorleggen.

Vraag 73 (PVV) – tijdelijke delegatie
Op pagina's 4 en 5 van dezelfde brief staat: «Via het nieuwe wetsvoorstel zal in de artikelen 3.1 tot en met 3.3 van de WGS worden geregeld dat uitsluitend in geval van spoed een nieuw samenwerkingsverband bij AMvB kan worden geregeld en dat in dat geval zo spoedig mogelijk een wetsvoorstel moet worden ingediend om het betreffende samenwerkingsverband alsnog in de wet te regelen. Dit betreft «tijdelijke delegatie».» [103] *Kunnen de leden van de PVV-fractie ervan uitgaan dat in het nieuwe wetsvoorstel gedetailleerd wordt aangegeven wat precies onder «in geval van spoed» en «tijdelijk» wordt verstaan?*

Voor tijdelijke delegatie kan volgens aanwijzing 2.39 van de Aanwijzingen voor de regelgeving aanleiding zijn indien met betrekking tot een materie die op zich regeling bij wet behoeft, «snelle interventie is geboden of anticipatie op nieuwe maatregelen moet worden voorkomen». Tijdelijke delegatie mag dus alleen in die gevallen waarin «de totstandkoming van een wet niet kan worden afgewacht». Vanwege het onvoorzienbare karakter van de omstandigheden waarin van deze bevoegdheid gebruik gemaakt zou kunnen worden, valt een nadere concretisering van het criterium spoed niet goed te geven.

Vraag 74 (SGP) – doelstellingen nieuwe samenwerkingsverbanden
De leden van de SGP-fractie lezen dat op grond van de Algemene Verordening Gegevensbescherming (AVG) gegevens slechts worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden, de zogenoemde doelbinding. De leden van de SGP-fractie constateren dat de doelstellingen van gegevensverwerking in het voorstel vrij algemeen zijn aangegeven. De leden van de SGP-fractie vragen de regering of deze algemene doelstellingen ook voor toetredende samenwerkingsverbanden voldoende zijn of moeten toetredende samenwerkingsverbanden een striktere doelstelling hanteren?

Deze vraag wordt zo begrepen dat met «toetredende samenwerkingsverbanden» is gedoeld op de mogelijkheid uit de artikelen 3.1 tot en met 3.3 van de WGS om nieuwe samenwerkingsverbanden onder de WGS te brengen door middel van een algemene maatregel van bestuur. Volgens artikel 3.1 is dit uitsluitend mogelijk voor een samenwerkingsverband met een doelstelling die past binnen de maximale bandbreedte van de in artikel 3.1 opgesomde doelstellingen van zwaarwegend algemeen belang, zoals «het voorkomen en bestrijden van ernstige vormen van criminaliteit». Het is bij de regeling van een nieuw samenwerkingsverband niet voldoende om een in artikel 3.1 opgesomde doelstelling naar de amvb te kopiëren, aangezien die doelen algemeen zijn omschreven. Het zal

[102] Kamerstukken II 2021/22, 35 447, nr. 21, p. 4.
[103] Kamerstukken II 2021/22, 35 447, nr. 21, p. 4–5.

moeten gaan om een meer afgebakende, striktere doelstelling ten opzichte van artikel 3.1. Overigens is in de brief van de toenmalige Minister van Justitie en Veiligheid van 17 december 2021 aan de Tweede en Eerste Kamer aangekondigd dat de mogelijkheid om nieuwe samenwerkingsverbanden bij amvb onder de WGS te brengen, zal worden beperkt tot spoedgevallen, voor de tijd die nodig is ter overbrugging om een wetswijziging tot stand te brengen om het betreffende samenwerkingsverband in de WGS zelf te regelen.[104]

12. Signaal of andere startpunten van de gegevensverwerking verduidelijken

Vraag 75 (D66) – het startpunt van de gegevensverwerking verduidelijken

Is het juist dat het meeste werk van een samenwerkingsverband ontstaat als gevolg van een signaal bij een van de deelnemers van het samenwerkingsverband? In de definitiebepaling van art 1.1 WGS staat dat een signaal een melding is van een of meer deelnemers in een samenwerkingsverband over bepaalde gedragingen of situaties. De vraag van de leden van de D66-fractie is aan welke concrete criteria zo'n melding moet voldoen wil het in behandeling mogen worden genomen? Dezelfde vraag hebben deze leden ten aanzien van het begrip «sturingsinformatie» uit artikel 1.1 WGS. De leden van de fractie van D66 constateren dat bijvoorbeeld art. 2.23 WGS handvatten biedt voor wat betreft de afweging of een signaal voldoende aanleiding geeft tot gezamenlijke gegevensverwerking. Maar in lid 9 van dat artikel wordt gesteld dat nadere criteria waaraan een signaal moet voldoen en de criteria voor verstrekking van resultaten van de gezamenlijke verwerking van gegevens aan een derde bij of krachtens AMvB kunnen worden gesteld. Waarom worden deze nadere criteria niet in de wettekst zelf opgenomen? In art 2.6 lid 2 WGS staat dat bij AMvB criteria kunnen worden gesteld aan de betrouwbaarheid en kwaliteit van het signaal. Waarom neemt de regering deze criteria niet in de wettekst zelf op? Deze vraag sluit aan bij de kritiek van de Autoriteit Persoonsgegevens in haar bovenvermelde brief dat een duidelijk en objectief signaal op basis van voldoende aanwijzingen als startpunt in de wettekst moet worden neergelegd voor alle samenwerkingsverbanden. [105]

In de artikelen 2.4, 2.8, 2.9, 2.11, 2.16 en 2.20 van het concept-BGS wordt het startpunt van de gegevensverwerking zoveel mogelijk geconcretiseerd met nadere criteria waaraan een signaal, casus of verzoek moet voldoen om aanleiding te kunnen zijn voor gezamenlijke gegevensverwerking ten behoeve van het doel van het samenwerkingsverband. Zoals opgemerkt in de nota naar aanleiding van het verslag, is het van belang om dit type aspecten van de gezamenlijke gegevensverwerking bij amvb te regelen om voldoende flexibiliteit te bieden.[106] Door de hoofdelementen op het niveau van formele wet te regelen en ruimte te bieden voor uitwerking daarvan bij amvb, is zoveel mogelijk een balans gezocht tussen beide elementen.

Vraag 76 (VVD) – startcriteria

Er lijkt veel ruimte te zijn voor de samenwerkingsverbanden om zelf te bepalen wanneer zij in actie komen. Hoe wordt gewaarborgd dat de actie proportioneel is en de inbreuk op de privacy rechtvaardigt?

---

[104] *Kamerstukken II 2021/22, 35 447, nr. 21.*
[105] Kamerstukken I 2021/22, 35 447, G, p. 5, 19, 25.
[106] Kamerstukken II 2020/21, 35 447, nr. 6, antwoorden 29 en 37, blz. 26–27 en blz. 31–32.

Samenwerkingsverbanden mogen de gegevensverwerking uitsluitend starten indien is voldaan aan de criteria voor het in behandeling nemen van een signaal, verzoek of casus, die zijn uitgewerkt in de artikelen 2.4, 2.8, 2.11, 2.16 en 2.20 van het concept-BGS. Deze criteria dragen eraan bij dat de inbreuk op de privacy gerechtvaardigd is.

Vraag 77 (GroenLinks/PvdA) – startcriteria
De Autoriteit Persoonsgegevens stelt dat het startsignaal voor activering van een samenwerkingsverband onvoldoende concreet omlijnd is. Het Hof van Justitie van de EU heeft geoordeeld dat rondom de bescherming van persoonsgegevens er duidelijke, precieze regels en criteria moeten zijn voor wanneer er inbreuk gemaakt kan worden op grondrechten. De leden van de fracties van GroenLinks en PvdA zijn van mening dat zonder een helder startpunt voor het delen van persoonsgegevens een risico bestaat dat er te makkelijk inbreuk gemaakt wordt op de privacy van burgers. Burgers kunnen zo (al dan niet terecht) als «verdacht» – niet alleen in strafrechtelijke zin – te boek komen te staan, zonder de waarborgen die daarvoor in het strafrecht gelden. Wat zijn de concrete criteria waarop een samenwerkingsverband kan worden geactiveerd?

De regering onderkent dat er duidelijke, precieze regels en criteria moeten zijn voor wanneer er inbreuk gemaakt kan worden op grondrechten, waaronder het recht op bescherming van persoonsgegevens. Daarom mogen samenwerkingsverbanden de gegevensverwerking uitsluitend starten indien is voldaan aan de criteria voor het in behandeling nemen van een signaal, verzoek of casus, die zijn uitgewerkt in de artikelen 2.4, 2.8, 2.11, 2.16 en 2.20 van het concept-BGS. Hiermee wordt verduidelijkt en gepreciseerd wat het startpunt voor het delen van persoonsgegevens is en wordt voorkomen dat er te makkelijk een inbreuk wordt gemaakt op de privacy van burgers.

Vraag 78 (D66) – doorwerking in een strafzaak van een «besmet» signaal
Volgens de regering moeten samenwerkingsverbanden grondig en met veel transparantie opereren. «Dat moet voorkomen dat een niet op juistheid en op objectiviteit geverifieerd signaal wordt opgepakt, dat er ten onrechte een risico wordt gesignaleerd en dat mensen inderdaad ten onrechte benadeeld worden.» [107] Dit brengt de leden van de D66-fractie op de vraag over de gevolgen van een ten onrechte opgepakt signaal als gevolg waarvan gegevens zijn verwerkt, gedeeld en benut. De regering heeft herhaaldelijk gesteld dat de reikwijdte van het wetsvoorstel ophoudt als een van de deelnemers op basis van de verkregen gegevens tot actie overgaat. Stel nu, zo vragen de leden van de D66-fractie aan de regering, dat het Openbaar Ministerie tot strafvervolging overgaat tegen een verdachte, nadat de data tegen de persoon in kwestie zijn verkregen op basis van een onterecht opgepakt signaal. Is daardoor de strafzaak (geheel of gedeeltelijk) besmet? Bestaat er een kans dat de strafrechter met de besmetting rekening houdt bij de beoordeling van de strafwaardigheid van de verdachte?

Vooraf wordt opgemerkt dat wordt beoogd om deze situatie zoveel mogelijk te voorkomen, onder meer door hiervoor specifieke waarborgen in het concept-BGS op te nemen. Een deelnemer mag uitsluitend een signaal, verzoek of casus aanmelden bij het samenwerkingsverband na de feitelijke juistheid en de kwaliteit van de daarbij te verstrekken gegevens te hebben getoetst, voor zover dat mogelijk is (artikel 1.6 van het concept-BGS). De deelnemers beoordelen of een signaal, verzoek of casus in overeenstemming is met het doel van het samenwerkingsverband. Bij

[107] Kamerstukken II 2020/21, 35 447, nr. 20, p. 39.

de verstrekking van de resultaten uit het samenwerkingsverband vindt opnieuw een toets plaats op de feitelijke juistheid en kwaliteit (artikel 1.8 concept-BGS).
Na ontvangst van een resultaat zal er altijd eigenstandig nader onderzoek verricht moeten worden naar aanleiding van ontvangen resultaten, conform de wettelijke taken en bevoegdheden van de ontvanger. Hierbij vindt nader onderzoek plaats conform de wettelijke kaders om te beoordelen of handhaving of interventies ingezet kunnen worden. De vervolgstappen die een deelnemer zet, vinden plaats op grond van het wettelijk kader dat van toepassing is op die betreffende deelnemer; gelet op de vraag van de leden van de D66-fractie is dat voor wat betreft het OM het Wetboek van Strafvordering. Verdere beoordeling van die vervolgstappen vindt dan ook plaats onder die wettelijke kaders.

Vraag 79 (PvdD) – invulling van de begrippen «signaal» en «sturingsinformatie»
De regering gaat in op de aanbeveling in het advies van de Autoriteit Persoonsgegevens om «in de wet een duidelijke en objectief signaal op basis van voldoende aanwijzingen als startpunt neer te leggen voor alle samenwerkingsverbanden»,[108] omdat duidelijke en precieze regels en criteria in de wetgeving vereist zijn.[109] De regering heeft het voornemen dit bij AMvB te regelen. De leden van de PvdD-fractie vragen de regering waarom dit niet in de WGS wordt geregeld? Kan de regering in het antwoord ingaan op de stelling dat het omschrijven welke signalen als «duidelijk en objectief» kunnen worden aangemerkt en welke aanwijzingen uit een oogpunt van kwaliteit en betrouwbaarheid als voldoende kunnen worden aangemerkt, niet een vaststelling betreft die naar verwachting regelmatig aanpassing behoeft? Op grond van welke juridische redenering wordt het toelaatbaar geacht om het startpunt van de gegevensverwerking niet bij formele wet maar bij AMvB nader te omschrijven? Is het juist dat een nahangprocedure zoals opgenomen in artikel 3.3 WGS niet van toepassing is op deze door de regering bedoelde AMvB? Zo ja, moet dan rekening worden gehouden met de kans dat een rechter, nu de kwestie niet in een formele wet wordt geregeld en de Staten-Generaal geen formele invloed meer kan uitoefenen op de totstandkoming van de regeling, zal oordelen dat de inbreuk op de grondrechten van de burger niet voldoet aan de eisen die voortvloeien uit de Grondwet, de AVG en de fundamentele burgerrechten die in bovennationale regelingen zijn vastgelegd?

De door de leden van de PvdD-fractie bedoelde juridische redenering is er enerzijds op gebaseerd dat het wetsvoorstel nu de wezenlijke elementen inzake deze samenwerkingsverbanden bevat. Anderzijds is voorzien in de benodigde delegatiegrondslagen om het startpunt van de gegevensverwerking bij amvb nader te omschrijven: artikelen 1.8, eerste lid, 2.6, tweede lid, 2.7, tweede lid, 2.14, tweede lid, 2.23, negende lid, en 2.31, twaalfde lid.
Het is correct dat op de nadere omschrijving van het startpunt de nahangprocedure niet van toepassing is. Wel herhaal ik, zoals hierboven gesteld in antwoord op vraag 31, dat ik het gehele concept-BGS na de consultatiefase aan uw Kamer zal toezenden opdat optimaal inzicht wordt geboden in de uitwerking van de waarborgen en de concretisering van de regels over de gegevensverwerkingen.
Voor het overige wordt verwezen naar bovengenoemde *vraag 75 (D66) – het startpunt van de gegevensverwerking verduidelijken*, naar *vraag 10 (PvdD) – verenigbaarheid met de Grondwet en verdragsbepalingen*, naar

[108] Kamerstukken I 2021/22, 35 447, G, p. 19.
[109] Kamerstukken I 2021/22, 35 447, G, p. 17.

vraag 7 (PvdD) – aanbevelingen AP en de amvb alsook naar de memorie van toelichting, paragraaf 7 (Grondrechtelijke aspecten).

13. Rechtmatigheidsadviescommissies

Vraag 80 (D66) – invulling rechtmatigheidsadviescommissie
Ook over de rechtmatigheidscommissie die de rechtmatigheid van nieuwe verwerkingen van persoonsgegevens en wijzigingen daarvan zou beoordelen is nog veel onduidelijk: wie zijn dat, hoe krijgen zij hun informatie aangeleverd, hoe kunnen zij hun toezicht uitoefenen, welke middelen en bevoegdheden krijgen zij daartoe, hebben zij de mogelijkheid in te grijpen en sanctioneren en zo ja hoe dan? Ook dat moet allemaal middels een AMvB nog worden ingevuld.

In artikel 1.14 van het concept-BGS is de samenstelling van de rechtmatigheidsadviescommissies uitgewerkt. Het gaat in beginsel om een of enkele personen per deelnemer aan het samenwerkingsverband. Zij moeten relevante deskundigheid en ervaring hebben op het gebied van de toepasselijke wetgeving inzake gegevensverwerking en de werking van het samenwerkingsverband.
De werkwijze is uitgewerkt in artikel 1.13 van het concept-BGS. De rechtmatigheidsadviescommissie kan adviseren op verzoek van de deelnemers of op eigen initiatief.
De adviestaak is bepaald in artikel 1.8, zesde lid, van het wetsvoorstel, namelijk om «de rechtmatigheid van de verwerking van persoonsgegevens in het samenwerkingsverband structureel te beoordelen bij nieuwe verwerkingen en wijziging in verwerkingen en om voorstellen aan het samenwerkingsverband te doen om onrechtmatigheden op te lossen». Hieruit volgt dat er geen bevoegdheid is tot sanctioneren of ingrijpen. Indien de deelnemers afwijken van een advies, dan kan dat uitsluitend beargumenteerd plaatsvinden en moet deze afwijking worden gedocumenteerd. Dit zorgt ervoor dat de afwijking traceerbaar is en dat later kan worden herleid waarom is afgeweken van een advies, zodat in de verplichte privacy audits kan worden onderzocht hoe het heeft uitgepakt. De afwijking moet bovendien gerapporteerd worden aan de coördinerend functionaris voor gegevensverwerking van het samenwerkingsverband, die zo nodig in actie kan komen.

Vraag 81 (ChristenUnie) – samenstelling rechtmatigheidsadviescommissies
In het kader van de rechtsbescherming zijn deze leden ook benieuwd naar de wijze waarop de regering voornemens is de rechtmatigheidsadviescommissie in te richten. Kan de regering aangeven hoe deze commissie zal worden samengesteld, welke disciplines of deskundigheidsgebieden in de commissie vertegenwoordigd zullen worden en wat de werkwijze van de commissie zal zijn, zo vragen de leden van de fractie van ChristenUnie. In de adviezen en reacties is de vraag aan de orde gesteld of ook toezicht op mogelijke discriminatierisico's valt onder de taak van de commissie. Kan de regering dat bevestigen?

De positie en inrichting van de rechtmatigheidsadviescommissies is in artikel 1.13 en 1.14 van het concept-BGS uitgewerkt door middel van de vaststelling van regels over de werkwijze en samenstelling. De rechtmatigheidsadviescommissie heeft tot taak de rechtmatigheid van de verwerking van persoonsgegevens in het samenwerkingsverband structureel te beoordelen en om voorstellen aan het samenwerkingsverband te doen om onrechtmatigheden op te lossen. Onderdeel van die toetsing is of toepassing van bepaalde criteria of methoden niet tot discriminatie of andere ongewenste uitkomsten kunnen leiden. Artikel 1.14, vierde lid, van het concept-BGS vereist daarom dat de deelnemers

zorgdragen dat in de rechtmatigheidsadviescommissie ook aandacht is voor het tegengaan van risico's op ongelijke behandeling en discriminatie.

Vraag 82 (PvdD) – onafhankelijkheid rechtmatigheidsadviescommissies
Artikel 1.8, zesde lid WGS heeft betrekking op het instellen van een rechtmatigheidsadviescommissie. Uit welk voorschrift van de WGS volgt dat deze commissie onafhankelijk dient te zijn, vragen de fractieleden van de PvdD. Uit welk voorschrift volgt dat als zo'n commissie een verwerking onrechtmatig oordeelt, het samenwerkingsverband die verwerking dient te staken en de gevolgen van de onrechtmatigheid dient te herstellen? Indien de onafhankelijkheid van de commissie niet bij formele wet is gewaarborgd en de commissie slechts een adviserende taak heeft, is dan voldaan aan de grondrechtelijke waarborgen die door de wetgever in acht dienen te worden genomen?

Er is geen wettelijk voorschrift waaruit volgt dat het samenwerkingsverband een verwerking dient te staken die de commissie onrechtmatig heeft bevonden. De positie van de rechtmatigheidsadviescommissies wordt echter versterkt in het concept-BGS:
– Een rechtmatigheidsadviescommissie is bevoegd rechtstreeks te adviseren aan de bestuurders van de deelnemers in het bestuurlijk gremium dat het samenwerkingsverband aanstuurt, zonder tussenkomst van een managementteam van een samenwerkingsverband. Dit is in artikel 1.13, tweede lid, van het concept-BGS opgenomen. Hierin komt de onafhankelijke rol tot uiting.
– De bestuurlijke gremia van waaruit het samenwerkingsverband wordt bestuurd mogen uitsluitend beargumenteerd afwijken van een advies van de rechtmatigheidsadviescommissie (artikel 1.13, zesde lid, van het concept-BGS). Dit betekent dat de bestuurders moeten motiveren waarom wordt afgeweken van het betreffende advies en welke risico-inschatting zij daaraan verbinden. Dit moet worden gedocumenteerd en gerapporteerd aan de rechtmatigheidsadviescommissie en de coördinerend functionaris voor gegevensbescherming voor het samenwerkingsverband. Dit is opgenomen in artikel 1.13, zesde lid, van het concept-BGS. Het is van belang te zorgen voor transparantie, dat afwijking van de adviezen traceerbaar is, en dat later door de (coördinerend) functionaris voor gegevensbescherming of in de privacy audits kan worden onderzocht hoe de afwijking heeft uitgepakt.
– De leden van de rechtmatigheidsadviescommissie moeten beschikken over relevante deskundigheid en ervaring op het gebied van de toepasselijke wetgeving inzake gegevensverwerking en de werking van het samenwerkingsverband (artikel 1.14, eerste lid, van het concept-BGS). Het is immers van belang dat organisaties leden aanwijzen die een bepaalde zwaarte/functie hebben zodat zij 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.

Vraag 83 (PvdD) – taak rechtmatigheidsadviescommissie bij tegengaan discriminatie
De regering stelt dat de wettelijke taakomschrijving zo gelezen kan worden dat daaronder ook valt «bij te dragen aan het tegengaan van risico's op ongelijke behandeling en discriminatie».[110] *Waarop baseert de regering dit? De wettelijke taak van de commissie is het «beoordelen van de rechtmatigheid van de verwerking».*

[110] Kamerstukken II 2021/22, 35 447, nr. 21, p. 9.

Artikel 1.14, vierde lid, van het concept-BGS stelt buiten twijfel dat de deelnemers zorgdragen dat in de rechtmatigheidsadviescommissie ook aandacht moet zijn voor het tegengaan van risico's op ongelijke behandeling en discriminatie.

Vraag 84 (PvdD) – beoordelen aangeleverde datasets op discriminatoire informatie
De Raad van State onderscheidt drie fasen waarop de WGS van toepassing is, en twee fasen waarvoor dat niet meer geldt. Fase 1 betreft «gegevensverstrekking aan het samenwerkingsverband». Fase 2 betreft «gegevensverwerking door het samenwerkingsverband». De beoordeling van de rechtmatigheid die de wettelijke taak van de commissie is, betreft de «verwerking», dus pas fase 2. Indien nu in fase 1 datasets worden aangeleverd die tot stand zijn gekomen door een vergaren van informatie op een wijze waarbij mogelijk onbewust bepaalde personen of een bepaalde bevolkingsgroep discriminatoir is benaderd, betreft dat vergaren en aanleveren van informatie niet de «verwerking van gegevens door het samenwerkingsverband». Omdat zulke «bias» in de datasets onzichtbaar is tijdens de verwerking van de gegevens, zal de commissie die de rechtmatigheid van de «verwerking» moet beoordelen, niet tot een schending van het verbod van discriminatie kunnen concluderen. Kan de regering in dit verband uitleggen hoe hij tot het oordeel komt dat de commissie tot taak heeft om te beoordelen of aangeleverde datasets discriminatoire informatie bevatten?

Van de rechtmatigheidsadviescommissie wordt niet verwacht om bij iedere verstrekking van gegevens aan het samenwerkingsverband te beoordelen of de aangeleverde data discriminatoire informatie bevatten. Haar rol is veeleer om te controleren of bepaalde werkwijzen binnen het samenwerkingsverband of de verkrijging van bepaalde producten door het samenwerkingsverband zodanig zijn ingericht dat deze rechtmatig zijn en dat de genoemde «bias» in gegevens zo veel mogelijk wordt voorkomen. Iedere keer als een werkwijze of een verkrijging van een product wijzigt of wanneer een nieuw initiatief wordt gestart, dient de rechtmatigheidsadviescommissie daar weer een toets op uit te voeren.
De rechtmatigheidsadviescommissie kan zich in principe enkel buigen over de fase van gezamenlijke verwerkingen. Een rechtmatigheidsadviescommissie is niet in staat om de verwerkingen te overzien die *niet* vallen onder de gezamenlijke verantwoordelijkheid van het samenwerkingsverband.
De partijen die de gegevens aanleveren hebben zelfstandig de verantwoordelijkheid om te voldoen aan de geldende wet- en regelgeving. In de fase van verstrekking aan het samenwerkingsverband gelden in principe de sectorale regels die op de verstrekkende deelnemer van toepassing zijn, waarbij toetsing plaatsvindt onder eigen verantwoordelijkheid. Iedere deelnemer is er zelf voor verantwoordelijk om voorafgaand aan de verstrekking van gegevens aan het samenwerkingsverband deze gegevens te controleren op juistheid en volledigheid. Hiermee wordt voorkomen dat een niet op juistheid en objectiviteit geverifieerd signaal wordt verstrekt, en dat ten onrechte een risico wordt gesignaleerd. Artikel 1.6 van het concept-BGS bepaalt dat een deelnemer uitsluitend een signaal, verzoek of casus mag aanmelden bij het samenwerkingsverband na, voor zover mogelijk, de feitelijke juistheid en de kwaliteit van de daarbij te verstrekken gegevens te hebben getoetst.
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. Wel dient bij de verstrekking van de resultaten uit het samenwerkingsverband een extra verificatie door de deelnemers plaats te vinden op de feitelijke juistheid en kwaliteit (artikel 1.8 concept-BGS).

Vraag 85 (PvdD) – beoordeling discriminatoire gevolgen na ontvangst resultaat

Het College voor de Rechten van de Mens beveelt aan dat de commissie «als taak krijgt om niet alleen te kijken naar de impact van de verwerking van (bijzondere) persoonsgegevens op de privacy van de burgers, maar ook om eigenstandig te kijken naar de eventuele discriminatoire gevolgen hiervan».[111] Blijkens het gestelde in paragraaf 7.2 wil de regering niet zover gaan, met als argument dat de fasen 4 en 5 die de Raad van State heeft onderscheiden «buiten de reikwijdte van de WGS vallen». Is de regering het met de leden van de fractie van de PvdD eens dat als in fasen 4 en 5 handelen van deelnemers op basis van de resultaten van de gegevensverwerking discriminatoir blijkt uit te pakken, de commissie tot taak heeft om na te gaan of dat het gevolg is van het gebruik van datasets met een discriminatoir karakter in de fasen 1, 2 of 3? Wat is er tegen om de wettelijke taak van de commissie uitdrukkelijk uit te breiden met een onderzoek naar en beoordeling van een mogelijk discriminatoir karakter of «bias» dat aan de aangeboden datasets heeft gekleefd?

Nadat het samenwerkingsverband een resultaat aan een deelnemer heeft verstrekt, valt het gebruik van die gegevens onder de zelfstandige verantwoordelijkheid van de betreffende deelnemer. Voorkomen moet worden dat deelnemers van de rechtmatigheidsadviescommissie, die niet werkzaam zijn voor de betreffende deelnemer, treden in vraagstukken die vallen onder de verantwoordelijkheid van die deelnemer. Waar nodig, bijvoorbeeld omdat het vraagstuk voortvloeit uit de eerdere gezamenlijke gegevensverwerkingen door het samenwerkingsverband, kan wel samenwerking gezocht worden met de rechtmatigheidsadviescommissie om tot beantwoording van een bepaalde rechtmatigheidsvraag te komen die tevens betrekking heeft op de gezamenlijke gegevensverwerking binnen het samenwerkingsverband.
Zoals in antwoord op de vorige vraag is gesteld, ligt de inhoudelijke beoordeling van de data die een deelnemer verstrekt aan het samenwerkingsverband, primair bij die aanleverende deelnemer. Het is immers diens individuele verantwoordelijkheid om de juiste data aan te leveren. Wat een rechtmatigheidsadviescommissie wel kan toetsen is of bij de aanlevering voldaan is aan de regels daaromtrent, en daarmee aan de voorwaarden voor aanlevering aan het samenwerkingsverband. Dit betreft een toets op de rechtmatigheid van de werkwijze. Zoals aangegeven in de brief van 17 december 2021, moeten de deelnemers en de rechtmatigheidsadviescommissies tijdens gezamenlijke gegevensverwerking anticiperen op mogelijke discriminatie of ongelijke behandeling voortvloeiend uit de verkregen resultaten.[112]

Vraag 86 (PvdD) – dwingend oordeel rechtmatigheidsadviescommissie

Artikel 1.7 WGS heeft betrekking op verstrekking van de resultaten van een verwerking aan deelnemers en derden. Uit welk voorschrift volgt dat als in een geval als bedoeld in artikel 1.7, tweede lid WGS, de commissie een eventuele verstrekking aan een derde niet rechtmatig heeft geoordeeld, het op die grond verboden is de resultaten van de verwerking aan die derde te verstrekken? Indien niet wettelijk is gewaarborgd dat de commissie onafhankelijk is en de commissie niet dwingend kan voorschrijven dat tot verstrekking van resultaten van de verwerking aan derden niet mag worden overgegaan, dient dan in het licht van door de Autoriteit Persoonsgegevens aangevoerde oordeel van het Hof van Justitie EU over de PNR-overeenkomst tussen de EU en Canada te worden geconcludeerd dat de verstrekking onrechtmatig zal zijn? Zo nee, op

---

[111] Kamerstukken I 2021/22, 35 447, D, p. 3.
[112] Kamerstukken II 2021/22, 35 447, nr. 21, paragraaf 7.2.

grond van welke juridische redenering komt de regering dan tot die ontkennende beantwoording?

Graag verwijst de regering naar onderdeel 9 (Toets door onafhankelijke bestuurlijke autoriteit bij verstrekking aan derden) van de bijlage bij de Kamerbrief van 17 december 2021. Zoals daarin is gemotiveerd, gaat de vergelijking met de situatie waarover het bindend advies van het Hof van Justitie gaat, niet op, zodat hieruit geen conclusies behoeven te worden overgenomen. Dat laat onverlet dat het wenselijk is dat de rechtmatigheidsadviescommissie een stevige positie krijgt en dat een eventuele afwijking van een advies moet worden gedocumenteerd en gerapporteerd. Hiervoor wordt verwezen naar het antwoord op *vraag 82 (PvdD) – onafhankelijkheid rechtmatigheidsadviescommissies*.

Vraag 87 (SGP) – taakomschrijving en doeleinden rechtmatigheidsadviescommissie
Is de regering met de SGP-fractie van mening dat rechtmatigheidsadviescommissie enkel kan functioneren indien zij een duidelijke taakomschrijving en toetsingskader heeft?

De in te stellen rechtmatigheidsadviescommissie zal ingevolge het voorgestelde artikel 1.8, zesde lid, van het wetsvoorstel tot taak krijgen de rechtmatigheid van de verwerking van persoonsgegevens in het samenwerkingsverband structureel te beoordelen bij nieuwe verwerkingen en wijziging in verwerkingen en om voorstellen aan het samenwerkingsverband te doen om onrechtmatigheden op te lossen. Zoals aangegeven in de memorie van toelichting, 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. Een rechtmatigheidsadviescommissie is nodig om uitspraken te doen over nieuwe verwerkingswijzen en ook kunnen aan de rechtmatigheidsadviescommissie kwesties voorgelegd worden, waarbij er twijfel bestaat over de rechtmatigheid van een verwerking.[113]
De rechtmatigheidsadviescommissie dient een sterke positie te hebben. Daartoe worden in de artikelen 1.13 tot en met 1.15 van het concept-BGS regels vastgesteld over de werkwijze, samenstelling en benoeming. Hiervoor wordt verwezen naar het antwoord op *vraag 82 (PvdD) – onafhankelijkheid rechtmatigheidsadviescommissies*.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius

[113] Kamerstukken II 2019/20, 35 447, nr. 3, blz. 60.