Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2287

Vragen van het lid **Verhoeven** (D66) aan de Ministers van Defensie, van Justitie en Veiligheid, van Sociale Zaken en Werkgelegenheid, voor Rechtsbescherming en van Binnenlandse Zaken en Koninkrijkrelaties over *grootschalige en onrechtmatige verzameling van data van burgers door de krijgsmacht, de politie, de Belastingdienst, de Inlichtingen- en Veiligheidsdiensten en andere overheidsorganisaties.* (ingezonden 15 januari 2021).

Antwoord van Minister **Dekker** (Rechtsbescherming), van Minister **Grapperhaus** (Justitie en Veiligheid), van Minister **Bijleveld-Schouten** (Defensie) en van Minister **Koolmees** (Sociale Zaken en Werkgelegenheid) (ontvangen 9 april 2021). Zie ook Aanhangsel Handelingen, vergaderjaar 2020–2021, nr. 1568.

Vraag 1
Wat is uw mening over het feit dat het afgelopen jaar de overheid op grote schaal niet voldoet aan de AVG of het Europees Verdrag voor de Rechten van de Mens en de Fundamentele Vrijheden (EVRM) – met als voorbeeld de dataverzameling op Nederlands grondgebied door LIMC bij Defensie, de algoritmes in proeftuinen die gebruikt worden door de politie, persoonsgegevens van meer dan vier miljoen personen die in te zien zijn door duizenden ambtenaren van het UWV, het Fraude Signaleringsysteem (FSV) van de belastingdienst, het feit dat vrijwel alle politiesystemem niet voldoen aan de AVG en informatieveiligheid, en onrechtmatige gegevensuitwisseling tussen COA en politie?

Antwoord 1
Het kabinet meent dat de overheid zelf voorop moet lopen bij de eerbiediging van de persoonlijke levenssfeer en de bescherming van persoonsgegevens. De overheid heeft een voorbeeldfunctie bij de naleving van wettelijke en verdragsrechtelijke normen. Burgers moeten erop kunnen vertrouwen dat hun gegevens goed zijn beschermd waar deze worden verwerkt door de overheid. Dat geldt uiteraard ook voor de in de vraag aangehaalde voorbeelden, waarover het kabinet met uw Kamer in veel gevallen al heeft gesproken. Daarbij is tevens gesproken over de lessen die daaruit getrokken kunnen worden. Ook bij deze gelegenheid wil het kabinet tot uitdrukking brengen dat wanneer de overheid het in haar gestelde vertrouwen beschaamt, het kabinet zich dat aan trekt. De Minister voor Rechtsbescherming heeft dit eveneens benadrukt in het debat met uw Kamer over het Privacylek in de systemen van

ah-tk-20202021-2287
ISSN 0921 - 7398
's-Gravenhage 2021

de GGD van 3 februari jl[1]. Verder is tijdens het debat onderstreept dat elk onderdeel van de overheid zelf is gehouden om processen zo in te richten dat de verwerking van persoonsgegevens voldoet aan de regels uit de Algemene verordening gegevensbescherming (AVG) en diens uitvoeringswet, en dat voldoende middelen worden gealloceerd voor het treffen van passende technische en organisatorische maatregelen. Een functionaris voor gegevensbescherming dient vervolgens interne controle uit te oefenen op de naleving ervan en hierover te adviseren. Indien blijkt dat overheidsorganisaties hier niet of onvoldoende toe in staat zijn, dan gaat het kabinet hierover met het desbetreffende onderdeel in gesprek.

Vraag 2
Geen van de 36 «mission critical»-systemen van de politie voldoet aan de privacywetgeving. Ook blijkt geen enkel politiekorps te voldoen aan alle gestelde eisen van de bescherming van gegevens van burgers. Sommige van de gebruikte systemen van de politie verwerken zeer gevoelige informatie, zoals over verdachten of kroongetuigen. Hoe is het mogelijk dat de politie applicaties gebruikt waarvan de ontwikkeling al jaren stilstaat?

Antwoord 2
Voor een toelichting op de nulmeting 2018/2019 die de politie zelf uitvoerde op de mate waarin de 36 door de politie geselecteerde systemen voldoen aan wet- en regelgeving verwijs ik u naar de verslaglegging van een schriftelijk overleg over de politie over het onderwerp datagebruik. Vernieuwing en verbetering van de systemen is een doorlopend proces.[2]

Vraag 3
Hoe rijmt u de achterstand van de digitale infrastructuur van de politie met de regels rond privacy en informatiebeveiliging?

Antwoord 3
Het vernieuwen van de digitale infrastructuur is – gezien de aard, omvang en complexiteit van de politieorganisatie en voortdurende technologische en maatschappelijke ontwikkelingen – een doorlopend proces, waarbij de politie eveneens voortdurend werkt aan compliance op het gebied van gegevensbescherming en informatiebeveiliging.

Vraag 4
Vindt u het niet zorgwekkend dat de politie niet kan voldoen aan alle eisen rond privacy en informatiebeveiliging, zoals bewaartermijnen of toegang, met de huidige verouderde systemen?

Antwoord 4
De politie heeft de nulmeting ten aanzien van de kritieke systemen in 2018/19 uitgevoerd om daarmee inzicht te krijgen in hoeverre deze systemen voldoen aan de verplichtingen in de Wet politiegegevens (Wpg) en aan het eigen beleid op dit terrein. Ten tijde van deze nulmeting voldeed het grootste deel van de 36 onderzochte applicaties niet aan alle wettelijke eisen. De mate waarin en de oorzaken hiervan zijn divers en zijn niet enkel gelegen in de betreffende ICT-systemen. Zo is uit evaluaties gebleken dat de Wpg niet goed aansluit op de technologische ontwikkelingen. Er wordt gewerkt aan een nieuw wettelijk kader.
Naar aanleiding van de nulmeting heeft de politie verbeteringen aangebracht. Zoals in het antwoord 2 en 3 is aangegeven betreft dit een doorlopend proces. Voor een verdere toelichting hierop verwijs ik u wederom naar het verslag van een schriftelijk overleg over de politie.[3] Bij de ontwikkeling van nieuwe systemen worden de principes van Privacy and Security by Design gevolgd, zoals vereist in de Wpg sinds 2019.

---

[1] Kamerstuk 27 529, ongecorrigeerd stenogram.
[2] Kamerstuk 29 628, nr. 985.
[3] Kamerstuk 29 628, nr. 985.

Vraag 5
Hoe kan het dat de politie jarenlang zelf de wet overtreedt, zonder dat er enig vooruitzicht is op het herstellen van de huidige problemen?

Antwoord 5
Zie de antwoorden 1 t/m 5 in het verslag van een schriftelijk overleg over de politie met betrekking tot datagebruik.[4]

Vraag 6
Bent u op deze risico's aangesproken door de Autoriteit Persoonsgegevens?

Antwoord 6
De AP heeft de Minister van Justitie en Veiligheid hier niet op aangesproken. Voldoen aan privacywetgeving is de verantwoordelijkheid van de verwerkingsverantwoordelijke en dus van het desbetreffende bestuursorgaan zelf. Hierop houdt de AP toezicht en het contact op dit gebied verloopt tussen de AP en het betreffende bestuursorgaan. De politie is op deze risico's overigens evenmin aangesproken door de AP. Organisaties horen natuurlijk niet te wachten tot ze aangesproken worden, zij zijn verplicht zelf actief aan de slag te gaan om te laten zien dat ze aan de wet voldoen. Dit vraagt om degelijke positionering en borging van het interne toezicht, hetgeen gestalte krijgt in de vorm van een Functionaris Gegevensbescherming (FG). De FG is de wettelijke, onafhankelijke, interne toezichthouder op het gebied van gegevensbescherming. De FG is niet verantwoordelijk voor het opstellen en naleven van het privacybeleid, maar houdt hier wel toezicht op en signaleert eventuele risico's. De politie heeft zelf het initiatief genomen tot genoemde nulmeting.

Vraag 7
Ook is er sprake van grootschalige dataverzameling door de krijgsmacht, het onderdeel LIMC. Op welke grond mag Defensie op zulke grote schaal data van Nederlandse burgers verzamelen en bewaren?

Antwoord 7
Op 27 november 2020 is uw Kamer per brief door de Minister van Defensie geïnformeerd over een eigenstandig onderzoek naar de naleving van de Algemene Verordening Gegevensbescherming (AVG) bij de dataverzameling door het Land Informatie Manoeuvre Centre (LIMC) dat de FG Defensie verricht.[5]
De FG Defensie legt de resultaten van haar onderzoek en de aanbevelingen vast in een rapport. De Minister van Defensie zal dat rapport dan samen met haar appreciatie naar de Tweede Kamer sturen. Zoals ook gemeld in de brief van 15 december jl. wacht de Minister van Defensie voor de beantwoording van Kamervragen over het LIMC de resultaten van dit onderzoek af.[6]

Vraag 8 tot en met 12
Wie is verantwoordelijk voor het toezicht voor het verzamelen van de data door LIMC?
Welke waarborgen gelden bij het verzamelen van deze data?
Zijn er bewaartermijnen vastgelegd voor de verzamelde data?
Is de grootschalige verzameling van data door LIMC een manier om toezicht op het gebruik van gegevens (waaronder bulkdatasets), zoals vastgelegd in de Wet op de Inlichtingen- en Veiligheidsdiensten, te omzeilen?
Wat wordt verstaan onder «semi-openbare bronnen» waarvan LIMC informatie verzameld? Kunnen hier voorbeelden van worden gegeven?

Antwoord 8 tot en met 12
Zie het antwoord 7.

---

[4] Kamerstuk 29 628, nr. 985.
[5] Kamerstuk 32 761, nr. 175.
[6] Aanhangsel Handelingen, vergaderjaar 2020–2021, nr. 1099.

Vraag 13
Is er nog steeds sprake van het verzamelen van data op Nederlands grondgebied door LIMC of door andere onderdelen van Defensie? Is het programma nu definitief stopgezet? Zo nee, waarom niet?

Antwoord 13
De Minister van Defensie heeft uw Kamer op 27 november 2020 per brief geïnformeerd dat zij in afwachting van de uitkomsten van het onafhankelijke onderzoek van de FG Defensie, heeft besloten het verzamelen en analyseren van informatie door het LIMC te staken. Het AVG-onderzoek bij LIMC is tevens aanleiding bij alle defensieonderdelen nadrukkelijk aandacht te besteden aan naleving van de AVG bij de verwerking van persoonsgegevens. Uit voorzorg is in afwachting van het onderzoek een aantal activiteiten aangepast of stilgelegd. Hierover wordt uw Kamer nader geïnformeerd door de Minister van Defensie in de brief met haar appreciatie bij het rapport van de FG over het LIMC.

Vraag 14
In september 2020 kwam de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) met een kritisch rapport naar buiten over het verzamelen en bewaren van gegevens. Kunt u toelichten hoe de CTIVD oordeelt over de nieuwe tijdelijke maatregelen, genomen rondom de verzameling en opslag van bulkdata?

Antwoord 14
De CTIVD heeft in haar reactie op de Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017 gesteld dat dit beleid in het licht kan worden geplaatst van haar aanbeveling (in de rapporten 70 en 71) om overkoepelend beleid voor bulkdatasets te maken ongeacht de bevoegdheid waarmee deze zijn verkregen.[7] Tevens merkt de CTIVD op dat, zoals ook de toelichting op het beleid duidt, het beleid onverlet laat dat de bepalingen van de Wiv 2017 onverkort van toepassing zijn. De CTIVD herhaalt in dit licht hetgeen zij in de rapporten 70 en 71 heeft gesteld omtrent de relevantiebeoordeling van gegevens in bulkdatasets. De CTIVD heeft op 13 januari jl. een technische briefing over dit onderwerp gegeven aan uw Kamer.

Vraag 15
Bij de UWV bleken persoonsgegevens van miljoenen burgers in te zien door duizenden medewerkers. Hoe is het mogelijk dat zo veel ambtenaren toegang hebben tot gegevens van burgers die nu of in het verleden gebruik hebben gemaakt van het UWV?

Antwoord 15
Zoals vermeld in de Kamerbrief van 5 oktober 2020, kent het systeem SONAR tekortkomingen op het gebied van informatiebeveiliging en privacy (IB&P).[8] SONAR is een essentieel systeem voor de UWV dienstverlening aan werkzoekenden. In de kern zijn de informatiebeveiliging en privacy (IB&P) tekortkomingen van SONAR het gevolg van eerdere ontwerpkeuzes gericht op effectieve dienstverlening aan klanten. De wetgeving op het gebied van privacy – en vooral ook de maatschappelijke en politieke aandacht hiervoor – heeft de afgelopen jaren een grote ontwikkeling doorgemaakt. Waar de nadruk eerder juist lag op transparantie in het systeem, kwam er ook bij UWV steeds meer aandacht voor de risico's voor privacy die hierbij kunnen ontstaan. Om de IB&P-risico's van SONAR volledig in kaart te brengen heeft UWV het initiatief genomen voor een extern onderzoek. Uit dat onderzoek is onder meer gebleken dat de toegang tot gegevens in SONAR te breed is ingericht. In de Kamerbrief van 5 oktober jl.[9] – en in meer detail in de brief Stand van de Uitvoering van december 2020[10] – is uiteengezet welke maatregelen UWV op korte en langere termijn neemt om de geconstateerde tekortkomingen op te lossen.

---

[7] https://www.ctivd.nl/actueel/nieuws/2020/11/05/index.
[8] Kamerstuk 26 643, nr. 714.
[9] Kamerstuk 26 643, nr. 714.
[10] Kamerstuk 26 448, nr. 641 bijlage Stand van de uitvoering.

Vraag 16
Waarom behouden ambtenaren bij het UWV toegang tot persoonsgegevens als zij deze gegevens niet nodig hebben voor hun werk?

Antwoord 16
De Minister van Sociale Zaken en Werkgelegenheid is van mening dat gegevens van burgers uitsluitend ingezien mogen worden door medewerkers die daartoe bevoegd zijn voor het uitvoeren van hun wettelijke taken. Het is belangrijk te benadrukken dat de gegevens in SONAR toegankelijk zijn voor geautoriseerde medewerkers en dat deze gegevens relevant zijn voor de belangrijke taak van UWV in de arbeidsbemiddeling. Geautoriseerde medewerkers hebben voor hun werkzaamheden toegang nodig tot een bepaalde set persoonsgegevens. Er is echter geconstateerd dat de toegang tot gegevens te breed is ingericht, waardoor geautoriseerde gebruikers toegang hebben tot gegevens die mogelijk niet direct noodzakelijk zijn voor de uitvoering van hun specifieke taken. Dat moet worden opgelost. UWV heeft een aanpak ontwikkeld om de IB&P-risico's stap voor stap te mitigeren. SONAR wordt zoveel mogelijk verbeterd en in fases volledig vervangen.

Vraag 17
Klopt het dat wettelijke bewaartermijnen van persoonsgegevens niet worden nageleefd? Hoe is dit mogelijk?

Antwoord 17
Het klopt dat UWV de bewaartermijn met betrekking tot persoonsgegevens in SONAR onvoldoende heeft nageleefd. Op grond van de Archiefwet hanteert UWV voor deze gegevens een bewaartermijn van 5 jaar. Derhalve dient UWV de gegevens van klanten die 5 jaar of langer inactief zijn, uit het systeem te verwijderen. De mogelijkheden om het systeem «te schonen» waren echter beperkt. Dit is één van de geconstateerde tekortkomingen die verholpen moeten worden. UWV heeft dit inmiddels met prioriteit opgepakt, en de gegevens van klanten die 5 jaar of langer inactief zijn, worden door UWV in het eerste kwartaal van 2021 verwijderd. In het vervolg wordt de bewaartermijn van persoonsgegevens in SONAR structureel nageleefd.

Vraag 18
Binnen welke termijn stelt u dat het Sonar systeem bij het UWV wel conform de AVG werkt?

Antwoord 18
Niet alle IB&P kwetsbaarheden en tekortkomingen in relatie tot de AVG kunnen worden verholpen in het huidige systeem (SONAR). Daarom wordt SONAR zoveel mogelijk verbeterd en in fases volledig vervangen. De volledige vervanging van SONAR zal niet voor 2025 afgerond zijn. Met deze gefaseerde aanpak worden de IB&P risico's stap voor stap verminderd, waardoor er ook in de aanloop naar de (volledige) vervanging van SONAR al in toenemende mate wordt voldaan aan de AVG. Hierbij prioriteert UWV de benodigde verbeteringen op basis van de aard en omvang van de geconstateerde IB&P risico's. Uiteraard zou het wenselijk zijn dat alle tekortkomingen al eerder volledig opgelost worden. Tegelijkertijd is het essentieel dat de UWV dienstverlening aan klanten te allen tijde doorgang heeft. Dat maakt deze operatie bijzonder complex. UWV kiest daarom bewust voor een zorgvuldige, geleidelijke aanpak.

Vraag 19
Gaat het UWV er in de toekomst voor zorgen dat persoonsgegevens van oud-klanten niet langer zo maar toegankelijk zijn?

Antwoord 19
De gegevens van klanten die 5 jaar of langer inactief zijn, worden door UWV verwijderd. Voor (oud-)klanten die minder dan 5 jaar inactief zijn is het – naast wettelijke verplichtingen die volgen uit de Archiefwet – ook onwenselijk om gegevens (eerder) te verwijderen, omdat een deel van deze klanten regelmatig in- en uitstroomt als gevolg van korte dienstverbanden of tijdelijk werk. Deze klanten zouden dan telkens opnieuw hun gegevens moeten doorgeven. UWV onderzoekt of het technisch mogelijk is om de gegevens

van klanten in SONAR – gedurende inactiviteit – onzichtbaar te maken. De Minister van Sociale zaken en Werkgelegenheid blijft met UWV in gesprek over de ontwikkelingen in dit dossier en zal uw Kamer hierover steeds in de Stand van de Uitvoering informeren.

Vraag 20
Kunt u toelichten hoe het mogelijk was dat het Centraal Orgaan opvang Asielzoekers (COA) structureel bijzondere persoonsgegevens zeven jaar deelde met de politie, terwijl dit hoogstwaarschijnlijk niet was toegestaan?

Antwoord 20
Op 17 juli 2020 heeft de Staatssecretaris van Justitie en Veiligheid uw Kamer geïnformeerd over de opschorting van de verstrekking van dagelijkse bezettingsgegevens van alle asielzoekers door het COA aan het Nationaal Vreemdelingen Informatieknooppunt (NVIK) van de politie.[11] In de beantwoording op de vragen van lid Van Toorenburg (CDA) en de vragen van leden Verhoeven en Van Beukering-Huijbregts (beiden D66) benadrukken de Minister en Staatssecretaris van Justitie en Veiligheid dat er geen twijfel over de rechtmatigheid van de verstrekking mag zijn.[12] Na onderzoek van het extern adviesbureau PMP blijkt dat deze verstrekking een onevenredige impact had op de persoonlijke levenssfeer van asielzoekers.[13] In de afgelopen jaren is het belang van data-minimalisatie en databescherming duidelijk geworden. De ketenpartners hebben uit deze casus belangrijke lessen getrokken. Het NVIK is overgestapt naar het gebruik van de Basisvoorziening Vreemdelingen (BVV) waarbij de privacy van asielzoekers is gewaarborgd en waardoor het delen van dagelijkse bezettingsgegevens van alle asielzoekers niet meer noodzakelijk is.

Vraag 21
Kunt u onderbouwen waarom de politie structureel recht zou hebben op bijzondere persoonsgegevens als deze «incidenteel relevant» zouden kunnen zijn bij hun handhavingstaak?

Antwoord 21
Het NVIK is bevoegd om gegevens en inlichtingen op te vragen bij bestuursorganen ten behoeve van de uitvoering van de Vreemdelingenwet.[14] Het rapport van het externe adviesbureau PMP stelt dat het NVIK de noodzaak van de verwerking van bijzondere persoonsgegevens heeft kunnen aantonen. Deze gegevens kunnen relevant zijn in de uitvoering van de toezicht- en handhavingstaken van de politie. Zo kunnen deze gegevens van belang zijn voor het voorkomen van geweldsincidenten en bij het opsporen van weggelopen asielzoekers. De juridische grondslag voor het gericht opvragen en verwerken van bijzondere persoonsgegevens ten behoeve van de uitvoering van de Vreemdelingenwet staat daarmee ook niet ter discussie.

Vraag 22
Acht u de bovenstaande grond voor het delen van gevoelige informatie, over de gezondheid of religieuze achtergrond, niet veel te breed en een onnodige inbreuk is op de persoonsgegevens van mensen die zich niet hebben misdragen?

Antwoord 22
Het NVIK vervaardigt informatieproducten voor de vreemdelingenketen. Met behulp van deze informatieproducten kan het NVIK trends met betrekking tot vreemdelingen waarnemen en daarop tijdig acteren. Hierbij zijn bijzondere persoonsgegevens relevante informatie om bijvoorbeeld ontwikkelingen van asielstromen in kaart te brengen. Geaggregeerde bijzondere persoonsgegevens zijn dus van belang bij een effectieve uitvoering van het vreemdelingenbeleid. Het NVIK werkt aan een werkwijze waarbij deze informatieproducten

[11] Kamerstuk 19 637, nr. 2646.
[12] Aanhangsel Handelingen, vergaderjaar 2020–2021, 124 en 125.
[13] Kamerstuk 19 637, nr. 2695.
[14] Machtigingsbesluit politieambtenaren NVIK.

kunnen worden vervaardigd zonder dat de persoonlijke leefsfeer van asielzoekers onevenredig wordt geschaad.

Vraag 23
Hoe gaat u ervoor zorgen dat onrechtmatig verzamelde data, zoals in de voorbeelden hierboven naar voren komen, die breed gedeeld wordt via samenwerkingsverbanden, zoals onder Wet Gegevensverwerking door Samenwerkingsverbanden (WGS), niet gebruikt gaat worden in geautomatiseerde analyses of beslissingen? Op welke wijze gaat u de risico's hierop minimaliseren?

Antwoord 23
In aanvulling op het algemene regels uit de AVG, voorziet de WGS in diverse aanvullende waarborgen. Zo beoordelen de verplichte rechtmatigheidsadviescommissies de rechtmatigheid van de verwerking van persoonsgegevens en doen zij aanbevelingen op dat vlak. Daarnaast zijn er onafhankelijke privacy audits; elk samenwerkingsverband wordt periodiek doorgelicht op compliance met de AVG en de WGS. De resultaten van de privacy audits moeten worden toegezonden aan de AP. Tevens komt er een coördinerende functionaris voor de gegevensbescherming, voor de coördinatie van het bestaande toezicht door de functionarissen voor de gegevensbescherming.

Vraag 24
Kunt u toelichten wat er gebeurt met gedeelde data die onrechtmatig blijkt te zijn verkregen?

Antwoord 24
De WGS bevat een transparantieplicht over de gehanteerde patronen en indicatoren of andere onderliggende logica (artikel 1.9, derde lid). Het resultaat van geautomatiseerde gegevensanalyse mag uitsluitend worden gedeeld na menselijke tussenkomst, waarbij wordt beoordeeld of het resultaat op een zorgvuldige wijze tot stand is gekomen. Daarbij moet uitleg worden gegeven over gehanteerde patronen, indicatoren en andere onderliggende logica. Zo wordt voorkomen dat een niet op juistheid en objectiviteit geverifieerd signaal wordt verstrekt, en dat ten onrechte een risico wordt gesignaleerd. Onrechtmatige data zullen worden hersteld en niet worden gebruikt als sturingsinformatie of interventie-advies. Tot slot verbiedt de WGS oncontroleerbare of onnavolgbare algoritmes (artikel 1.9, zesde lid, zoals ingevoegd bij amendement van de leden Van Nispen (SP) en Buitenweg (GroenLinks).

Vraag 25
In de hier boven geschetste kwesties komt naar voren dat het afgelopen jaar overheidsinstanties, die zelf de wet moeten handhaven, de wet overtreden door onrechtmatig data van burgers te verzamelen en te gebruiken. Hoe kan het dat er niet gehandhaafd wordt op wetshandhavers die de wet overtreden?

Antwoord 25
Het is van belang om per casus te beoordelen welke wetgeving van toepassing is.
In het geval dat de AVG of WPG van toepassing is op de verwerking van gegevens ziet de AP toe op naleving, ook door de overheid. De AP heeft het thema «digitale overheid» voorts aangewezen als één van haar focusgebieden voor de periode 2020–2023.[15] Verder heeft de AP geadviseerd over voorgenomen verwerkingen door de overheid en bijbehorende wettelijke grondslagen, zoals de adviezen over de trajecten om gegevens in te zetten ter bestrijding van de COVID-19 pandemie.
Het is vervolgens aan de toezichthouder in kwestie om per casus te bepalen of er een onrechtmatige gegevensverwerking plaats heeft gevonden. Indien dit het geval is wordt er ook ten aanzien van wetshandhavers door de toezichthouder in kwestie gehandhaafd.

[15] Focus Autoriteit Persoonsgegevens 2020–2023, te raadplegen op www.autoriteitpersoonsgegevens.nl.

Vraag 26
Hoe is de Minister voor Rechtsbescherming van plan om in de toekomst soortgelijke overtredingen die hierboven zijn geschetst Rijksbreed te voorkomen?

Antwoord 26
Er is wet- en regelgeving over verwerken van gegevens, dit omvat ook de verzameling van gegevens. Dit betreft in hoofdzaak de normen uit het bestuurs- en gegevensbeschermingsrecht. Kern van die wetgeving is dat gegevensverwerkingen binnen de overheid, rechtmatig, behoorlijk en transparant zijn en berusten op een wettelijke grondslag. Dit is neergelegd in de AVG en uitgewerkt in de UAVG. Voor politie en justitie geldt de richtlijn politie en justitie, die is neergelegd in de Wpg en de WjSG. Op grond van de AVG is vereist dat overheidsorganisaties, indien zij gegevens verzamelen ten behoeve van een wettelijke taak, daarvoor een wettelijke grondslag hebben, met de nodige waarborgen. Dit kan uitgewerkt worden in sectorale wetgeving. Conform de systematiek van genoemde wetgeving is het aan de overheidsorganisatie in kwestie om er zorg voor te dragen dat de verwerking past binnen de wettelijke grondslag en geschiedt op een wijze zoals in de wet voorzien. Dit omvat logischerwijs mede dat het beginsel van doelbinding wordt gerespecteerd; en verzamelde gegevens dus niet voor een ander doel worden gebruikt. De overheidsorganisatie in kwestie moet aan de toezichthouder aan kunnen tonen dat haar gegevensverwerking rechtmatig, behoorlijk en transparant is en voldoet aan de in de AVG en nationale wetgeving gestelde eisen. Zoals in antwoord 25 aangegeven is het aan de toezichthouder, en in voorkomend geval de rechter, om te beoordelen of overheidsorganisaties conform deze wetgeving hebben gehandeld bij de verzameling van gegevens.
In aanvulling hierop wordt vanuit het Rijk gewerkt aan een verbetering van haar informatiehuishouding. Het stelt hiervoor meerjarenplannen op. Hier komt bij dat er door het kabinet beleid wordt gevoerd om het analyseren van rechtmatig verzamelde data aan verdere waarborgen te onderwerpen. Dit doet het door in te zetten op verdere waarborgen vóór (algoritmische) data-analyse en de ontwikkeling van een mensenrechten impact assessment, als door in te zetten op extra normen die in acht moeten worden genomen wanneer data-analyse wordt toegepast (de richtlijnen voor data-analyse door de overheid).[16] Over de stand van zaken betreffende deze initiatieven wordt uw Kamer dit kwartaal nog nader geïnformeerd.

Vraag 27
Toont deze lange lijst van misstanden niet aan dat de Autoriteit Persoonsgegevens beschikking moet krijgen over meer middelen, zodat er adequaat toezicht op naleving van privacywetgeving kan worden gehouden?

Antwoord 27
De resultaten van het vorig jaar uitgevoerde onderzoek van KPMG naar taken en middelen van de AP laten zien dat zowel het werkveld als de organisatie van de AP nog volop in ontwikkeling is. De AP heeft in de afgelopen jaren steeds extra budget toegekend gekregen om haar taken uit te kunnen voeren. Eind 2020 heeft de AP nog eens 4,7 miljoen euro extra ontvangen voor het oplossen van incidentele problematiek en voor het doen van een investering in haar bedrijfsvoering. Voor 2021 is haar budget éénmalig verhoogd naar in totaal 24,6 miljoen euro. Zoals de Minister voor Rechtsbescherming per brief van 19 november 2020 en tijdens het debat over het privacylek in de systemen van de GGD van 3 februari jl. heeft medegedeeld, is het aan een volgend kabinet om te besluiten over een eventuele structurele verhoging van de middelen van de AP. De Minister voor Rechtsbescherming gaat in zijn brief, in antwoord op de aangenomen motie, hier nader op in.[17]

Vraag 28
Kunnen deze vragen ieder apart worden beantwoord?

---

[16] Kamerstuk 26 643, nr. 641 (bijlage).
[17] Kamerstuk 27 529, nr. 240.

Antwoord 28
De vragen zijn zoveel mogelijk separaat beantwoord.