
Vergaderjaar 2025-2026

- 36 264** Wijziging van de Uitvoeringswet Algemene verordening gegevensbescherming en enkele andere wetten in verband met het stroomlijnen en actualiseren van het gegevensbeschermingsrecht (Verzamelwet gegevensbescherming)

C **NOTA NAAR AANLEIDING VAN HET VERSLAG**
Ontvangen 20 november 2025

1. Inleiding

De regering heeft met belangstelling kennisgenomen van de schriftelijke inbreng van de vaste commissie voor Digitalisering bij de Verzamelwet gegevensbescherming. Uit die inbreng volgt dat de leden van de GL-PvdA fractie kennis hebben genomen van het wetsvoorstel en onderschrijven dat dit wetsvoorstel gericht is op het doorvoeren van de noodzakelijke aanpassingen in het gegevensbeschermingsrecht. Zij hebben nog enkele vragen naar aanleiding van de consultatiereactie van het Rathenau Instituut. De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Deze leden willen de regering nog enkele vragen voorleggen. Ook de leden van de ChristenUnie-fractie hebben met belangstelling kennisgenomen van de Verzamelwet gegevensbescherming. Het wetsvoorstel heeft deze leden aanleiding gegeven tot het maken van opmerkingen en het stellen van vragen. De leden van de Volt-fractie hebben met interesse kennisgenomen van de Verzamelwet gegevensbescherming. Daarover hebben deze leden een aantal vragen te stellen aan de regering. De regering is de leden van de fracties van GL-PvdA, CDA, ChristenUnie en Volt erkentelijk voor de gestelde vragen. Op de vragen die door de leden zijn gesteld is in de hierna volgende tekst gereageerd. Daarbij is de volgorde en indeling van het verslag aangehouden. Deze nota naar aanleiding van het verslag wordt gegeven mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties.

2. Advies en consultatie

Vraag 1

De leden van de GL-PvdA-fractie vragen de regering om te reflecteren op drie knelpunten die de UAVG volgens het Rathenau Instituut niet goed regelt, te weten: 1) de verwerking van genetische gegevens door commerciële analysebureaus en door werkgevers; 2) de verwerking van biometrische gegevens in de publiek ruimte; en 3) de verwerking van gezondheidsgegevens in het medische domein (WGBO) en daarbuiten (UAVG) en de verwerking van persoonsgegevens door hulpverleners in het kader van een 'goede behandeling of verzorging c.q. beheer van de beroepspraktijk'. Deze leden constateren dat de regering niet inhoudelijk is ingegaan op de oplossingsrichtingen van het Rathenau Instituut. De regering merkt enkel in algemene zin op dat er in toenemende mate wensen worden geuit tot wijziging of aanvulling van de UAVG, maar dat dit wetsvoorstel geen ruimte biedt voor de meeste aangedragen nieuwe thema's.

De leden van de GL-PvdA-fractie merken op dat het regelen van de door het Rathenau Instituut aangedragen oplossingsrichtingen in een afzonderlijk wetgevingstraject gepaard gaat met een langdurige doorlooptijd, terwijl de gesignaleerde knelpunten daardoor voorlopig onopgelost blijven. Zij vragen waarom de regering ervoor heeft gekozen om de door het Rathenau Instituut aangedragen oplossingsrichtingen voor de knelpunten in de UAVG niet in het voorliggende wetsvoorstel te verwerken. De leden van de GL-PvdA-fractie vragen de regering in te gaan op elk van de drie door het Rathenau Instituut benoemde knelpunten. Welke gevolgen en risico's zijn verbonden aan het feit dat deze onderwerpen in de UAVG niet afdoende zijn geregeld? In hoeverre

zijn deze mogelijke gevolgen meegewogen in de afweging? Indien deze gevolgen als negatief worden beoordeeld, acht de regering het dan alsnog mogelijk om deze onderwerpen in een verzamelwet en/of uitvoeringswet te regelen?

In zijn consultatiereactie heeft het Rathenau Instituut een pleidooi gehouden om een aantal aanvullende onderwerpen in het onderhavige wetsvoorstel te regelen. Daartoe heeft de regering evenwel niet besloten. Ten aanzien van de UAVG bevat het huidige wetsvoorstel een grote verzameling van veelal technische wijzigingen en wijzigingen van beperkte inhoudelijke aard. Naar het oordeel van de regering passen de door het Rathenau Instituut voorgestelde maatregelen reeds om die reden niet in het onderhavige wetsvoorstel. Voor deze onderwerpen geldt namelijk dat het in alle gevallen gaat om een complexe wijziging van de UAVG die om een uitvoerige inhoudelijke afweging vraagt en die daarmee de reikwijdte van dit wetsvoorstel te buiten gaat. Opname in dit wetsvoorstel, tezamen met allerlei noodzakelijke technische verbeteringen en verduidelijkingen van de UAVG, zou de parlementaire behandeling ook niet ten goede komen.

Daarnaast wijst de regering er in antwoord op de specifieke vragen van de leden van de fractie van GL-PvdA op dat de AVG en de UAVG voor deze door het Rathenau Instituut genoemde onderwerpen vaak al een regeling bevat. Zo beveelt het Rathenau Instituut aan om in de UAVG op zijn minst te verduidelijken wanneer de gegevensverwerkingen voor commerciële DNA-analyses mogen plaatsvinden op basis van uitdrukkelijke toestemming. Op grond van de AVG en UAVG is de verwerking van genetische gegevens in beginsel al verboden. Dat is alleen anders als wetgeving de verwerking expliciet toestaat. Analyses op DNA-materiaal door commerciële bureaus kan alleen met de “uitdrukkelijke toestemming” van degene van wie het DNA-materiaal afkomstig is. Wanneer een gegevensverwerking mag plaatsvinden op basis van uitdrukkelijke toestemming, is uitputtend geregeld in artikel 4, punt 11, AVG, zodat hiervan in de UAVG niet kan worden afgeweken.

In aanvulling daarop bepaalt artikel 28, eerste lid, UAVG expliciet dat de verwerking van genetische gegevens alleen is toegestaan met betrekking tot de persoon bij wie deze zijn verkregen. Er kunnen in beginsel dus geen analyses worden uitgevoerd ten aanzien van derden.

Voor zover het Rathenau Instituut voorstelt DNA-analyses in het arbeidsdomein alleen toe te staan op grond van een expliciete wettelijke grondslag, merkt de regering op dat toestemming van de werknemer in de arbeidsverhouding vaak geen voldoende grondslag zal vormen voor dit soort analyses. Het Europees Comité voor Gegevensbescherming heeft in het verleden geoordeeld dat dat overweging 43, in samenhang gelezen met artikel 4, punt 11, van de AVG, met zich brengt dat toestemming in de verhouding tussen een werknemer en werkgever meestal niet vrijelijk gegeven zal worden. Er is immers sprake van een disbalans tussen de betrokkene en de verwerkingsverantwoordelijke.¹ Dit betekent dat het voorstel van het Rathenau Instituut reeds in hoge mate overeenkomt met datgene wat er volgt uit de AVG, zodat de vraag of er risico's zijn verbonden aan het feit dat dit niet in de UAVG is geregeld, negatief kan worden beantwoord. Ten aanzien van biometrische gegevens in de publieke ruimte stelt het Rathenau Instituut dat het voor de hand ligt dat de wetgever uiterst terughoudend is in het toestaan van de verwerking van biometrische gegevens door private en publieke partijen. Dit uitgangspunt onderschrijft de regering. De verwerking van biometrische gegevens met het oog op de unieke identificatie van een persoon is om die reden op grond van de AVG en artikel 29 UAVG in beginsel verboden. Anders dan het Rathenau Instituut suggereert, zie ik op dit moment echter geen aanleiding om het verbod verder uit te breiden en de huidige uitzonderingen te laten vervallen. Wel verduidelijkt het onderhavige wetsvoorstel in artikel 29 UAVG de uitzonderingsgrond inzake redenen van zwaarwegend algemeen belang voor beveiligings- of authenticatiedoeleinden.

Vraag 2

De leden van GL-PvdA-fractie merken op dat, gelet op de snelle technologische ontwikkelingen, het niet ondenkbaar is dat ook in de toekomst regelmatige en voortvarende aanpassingen van de UAVG noodzakelijk zullen zijn. Deelt de regering deze inschatting? Zo nee, waarom niet? Zo ja, op welke wijze is de regering voornemens hieraan invulling te geven?

Het lijkt aannemelijk dat de UAVG ook in de toekomst aangepast zal moeten (blijven) worden aan veranderende omstandigheden. Dat geldt overigens voor de meeste regelgeving. Bij het commissiedebat van 18 maart jongstleden over het onderwerp bescherming persoonsgegevens en digitale grondrechten,² en tijdens de plenaire behandeling van het onderhavige wetsvoorstel in de

¹ Europees Comité voor Gegevensbescherming, Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679, 4 mei 2020, overwegingen 21 en 22, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_nl.pdf

² Kamerstukken II 2024/25, 32761, nr. 318, p. 38-39.

Tweede Kamer,³ heeft de toenmalige Staatssecretaris Rechtsbescherming laten weten open te staan voor een regelmatige actualisering ('revisie') van de UAVG. Daaraan is de toezegging verbonden te gaan werken aan een brede revisie van de UAVG. Daarbij zullen onder meer de onderwerpen worden betrokken die tijdens de behandeling van dit wetsvoorstel aan bod zijn gekomen en die in dit wetsvoorstel niet zijn geregeld, omdat ze gelet op hun complexiteit een separate, meer diepgaande, afweging vergen dan in een Verzamelwet kan geschieden. Aldus zullen ook andere onderwerpen worden meegenomen, waaronder de onderwerpen die zijn besproken bij het rondetafelgesprek met de vaste Kamercommissie Digitale Zaken van de Tweede Kamer op 4 december 2024.⁴

Vraag 3

De leden van de GL-PvdA-fractie merken op dat het Rathenau Instituut heeft aanbevolen om de verwerking van biometrische gegevens in de publieke ruimte volledig te verbieden. Deze leden constateren dat de regering tijdens de behandeling in de Tweede Kamer heeft aangegeven dat gezichtsherkenningstechnologie op basis van het bestaand juridisch kader slechts in beperkte gevallen kan worden ingezet, en dat zij geen aanleiding ziet voor een verdergaand verbod.⁵ In dit kader hebben de aan het woord zijnde leden enkele vragen. Allereerst vragen de leden van de GL-PvdA-fractie op basis waarvan de regering tot het oordeel komt dat het voorstel van het Rathenau Instituut een verdergaand verbod behelst. Daarnaast vragen deze leden of de regering kan toelichten op welke wijze de verwerking van biometrische gegevens in de openbare ruimte precies is geregeld. In welke situaties en onder welke voorwaarden is de verwerking van biometrische gegevens in de openbare ruimte binnen het huidige juridische kader toegestaan? Zijn er op dit moment technologische ontwikkelingen die tot een verruiming van het huidige juridische kader kunnen leiden? En voorziet de regering dat er in de toekomst dergelijke technologische ontwikkelingen zullen voordoen?

In de brief aan de Tweede Kamer van 9 oktober 2024 heeft de toenmalige Staatssecretaris Rechtsbescherming uiteengezet welke uitzonderingen er bestaan op het verbod op de verwerking van biometrische gegevens, voortvloeiend uit artikel 9 AVG.⁶ In dit kader kan worden gewezen op twee uitzonderingen. Een eerste uitzondering is de situatie waarin de betrokkene vooraf uitdrukkelijk toestemming heeft gegeven voor het verwerken van biometrische persoonsgegevens (artikel 9, tweede lid, sub a, AVG). Daarbij dient deze toestemming ook vrij, ondubbelzinnig, geïnformeerd en specifiek te zijn (artikel 4, sub 11, AVG). Een tweede uitzondering geldt op grond van artikel 29 UAVG, indien het verwerken van biometrische gegevens noodzakelijk is voor redenen van zwaarwegend algemeen belang voor beveiligings- of authenticatiedoeleinden. Met het onderhavige wetsvoorstel wordt beoogd artikel 29 UAVG te verduidelijken. In het huidige wetsvoorstel is bepaald dat in een voorkomend geval niet alleen dient te worden beoordeeld of sprake is van een beveiligings- of authenticatiedoeleinde, maar ook of sprake is van een zwaarwegend algemeen belang. Daarnaast bepaalt het onderhavige wetsvoorstel expliciet dat alleen aanspraak gemaakt kan worden op de uitzonderingsgrond uit artikel 29 UAVG ten behoeve van specifiek in die bepaling omschreven doelen, waarmee de algemene doelclausulering verder wordt gespecificeerd. De regering voorziet op dit moment geen technologieën waarvan nu reeds vaststaat dat die in de toekomst tot verruiming van het wettelijk kader moeten leiden.

Vraag 4

De leden van de GL-PvdA-fractie merken voorts op dat het Rathenau Instituut heeft aanbevolen om voor de verwerking van biometrische gegevens in niet-publieke ruimten een vergunningsplicht in te voeren. In de nota naar aanleiding van het verslag aan de Tweede Kamer stelt de regering: "Er moet ruimte blijven voor uitzonderingssituaties waarbinnen voldaan kan zijn aan de voorwaarden om een degelijke wijze van verwerking te rechtvaardigen."⁷ Deze leden zijn van mening dat een vergunningsplicht uitzonderingen niet uitsluit. Kan de regering hierop reflecteren? Ziet de regering aanleiding om, mede gelet op de snelle technologische ontwikkelingen, alsnog opvolging te geven aan de aanbeveling van het Rathenau Instituut?

³ *Handelingen II* 2024/25, nr. 76, item 34, p. 12-13.

⁴ https://www.tweedekamer.nl/debat_en_vergadering/commissievergaderingen/details?id=2024A07395

⁵ *Kamerstukken II* 2023/24, 36 264, nr. 6, p. 34.

⁶ *Kamerstukken II* 2024/25, 26 643, nr. 1223.

⁷ *Kamerstukken II* 2024/25, 36264, nr. 6, p. 34.

In zijn brief aan de Tweede Kamer van 9 oktober 2024, verzonden naar aanleiding van de motie Kathmann⁸, die de regering onder andere verzocht om een vergunningplicht voor het gebruik van gezichtsherkenning in de publieke ruimte te onderzoeken, is de toenmalige Staatssecretaris Rechtsbescherming op dit onderwerp ingegaan.⁹ Volgens het huidige wettelijke stelsel van de AVG heeft de verwerkingsverantwoordelijke een eigen plicht om te zorgen dat hij de vereisten naleeft en die naleving kan aantonen (artikel 5 AVG). Deze verantwoordingsplicht verhoudt zich niet goed tot een vergunningstelsel waarbij een derde partij verantwoordelijk is voor het controleren van de vereisten op grond waarvan de vergunning zou moeten worden afgegeven, zoals het Rathenau instituut voorstelt. Een wijziging in het uitgangspunt van de AVG dat de verwerkingsverantwoordelijke zelf verantwoordelijk is voor naleving van de AVG acht de regering onwenselijk, ook wanneer bijzondere gevoelige persoonsgegevens zoals biometrische persoonsgegevens worden verwerkt.

Daarbij komt dat de inzet van gezichtsherkenning valt onder het verwerkingsverbod voor biometrische persoonsgegevens, waarvan slechts onder voorwaarden kan worden afgeweken. In de gevallen waarin een afwijking van het verbod op persoonsgegevens op basis van het huidige juridische kader mogelijk is, biedt de AVG reeds waarborgen die gelden voorafgaand aan de verwerking. Gedacht kan worden aan de bij de verwerking van biometrische gegevens verplichte gegevensbeschermingseffectbeoordeling (DPIA), in combinatie met een eventuele verplichte voorafgaande raadpleging van de Autoriteit Persoonsgegevens (hierna: AP) als de inzet van gezichtsherkenning ook met de nodige maatregelen een hoog risico voor rechten en vrijheden oplevert. Met inachtneming van deze waarborgen en onder erkenning van de daaruit voortvloeiende verantwoordelijkheden moet het mogelijk blijven om uitzonderingen te maken op het verwerkingsverbod.

Vraag 5

De leden van de ChristenUnie-fractie constateren dat in het advies van de Raad van State wordt ingegaan op de invulling van open normen van de AVG, zoals die van het “zwaarwegend algemeen belang” als grondslag voor het verwerken van persoonsgegevens. Het wetsvoorstel voorziet in een uitbreiding van de wettelijke grondslagen voor het verwerken van (bijzondere) persoonsgegevens. Kan de regering toelichten op basis van welke concrete criteria wordt beoordeeld of er sprake is van een zwaarwegend algemeen belang? Hoe kan transparantie en kenbaarheid bij de invulling van deze open norm worden geborgd?

Het is niet goed mogelijk om de grondslag “zwaarwegend algemeen belang” met concrete criteria, die onder alle omstandigheden betekenisvol zijn, in te vullen.¹⁰ In meer algemene zin geldt dat het bij een zwaarwegend algemeen belang gaat om een algemeen belang dat zodanig is dat het zwaarder weegt dan het belang van de bescherming van de persoonlijke levenssfeer tegen inbreuk door de verwerking van bijzondere persoonsgegevens. Of daarvan sprake is zal in de gegeven context moeten worden bepaald. Wel dient te worden opgemerkt dat een algemeen belang nog geen zwaarwegend algemeen belang is. Het algemeen belang zal in de concrete situatie zodanig zwaarwegend moeten zijn dat het een beperking van de persoonlijke levenssfeer door de verwerking van (bijzondere) persoonsgegevens rechtvaardigt. Daarbij geldt overigens ook dat deze afweging geen statische eenheid is. Maatschappelijke opvattingen over de wijze waarop deze afweging uit moet vallen kunnen ook over de tijd veranderen.

Vraag 6

De aan het woord zijnde leden hebben kennisgenomen van de reactie op het advies van de Autoriteit Persoonsgegevens om in het wetsvoorstel voorzieningen te treffen voor het stellen van regels over de verwerking van persoonsgegevens van overleden personen. De regering geeft aan dat het nog te vroeg lijkt voor wettelijke maatregelen. Deze leden merken op dat digitale nalatenschap een steeds groter vraagstuk wordt, waarvoor op termijn wettelijke kaders onontbeerlijk zullen zijn. Zij vragen welke vervolgstappen de regering voornemens is te zetten om te komen tot regelgeving, en welk tijdpad de regering daarbij voor ogen heeft.

De vraag in hoeverre de verwerking van persoonsgegevens van overleden personen regeling behoeft is een complex vraagstuk. Er is voornamelijk geen consensus over een probleemdefinitie en ook niet over de richting waarin een eventuele wettelijke regeling zou moeten gaan. De regelingen die in verschillende Europese lidstaten bestaan en daarin voorzien, lopen uiteen. In sommige

⁸ Kamerstukken II 2023/24, 26 643, nr. 1171.

⁹ Kamerstukken II 2024/25, 26 643, nr. 1223.

¹⁰ Zie in deze zin ook Kamerstukken II 2022/23, 36 264, nr. 4.

Europese lidstaten ligt de regie bij de nabestaanden, in andere lidstaten bij de overledenen, doordat zij bij leven richtlijnen kunnen opstellen.¹¹ Er zijn echter ook combinaties en variaties mogelijk. Dat maakt dat er op dit punt tussen Europese lidstaten op dit moment geen sprake is van eenvormigheid. Dit betekent dat zich geen vanzelfsprekende ontwikkelingsrichting aandient en dat er nog veel vragen openstaan en afwegingen te maken zijn in deze complexe thematiek. Tegelijkertijd is duidelijk dat dit onderwerp aandacht verdient. Besluitvorming vraagt een zorgvuldige analyse en weging op basis van het beleidskompas. De prioritering van de thematiek en de keuzes over verdere ontwikkelrichtingen laat ik aan een volgend kabinet

3. ARTIKEL 1. Uitvoeringswet Algemene verordening gegevensbescherming

Onderdeel Fb

Vraag 7

Naar aanleiding van het door de Tweede Kamer aanvaarde amendement van het lid Six Dijkstra over een verplichting tot openbaarmaking van een door de Autoriteit Persoonsgegevens opgelegde bestuurlijke sanctie (nr. 19) vragen de leden van de ChristenUnie-fractie de regering of de huidige wettelijke waarborgen rondom openbaarmaking van handhavingsbesluiten door de AP voldoende zijn. Kan de regering daarop reflecteren? Daarnaast vragen deze leden hoe de regering het spanningsveld beoordeelt tussen enerzijds het belang van precedentwerking (jurisprudentie) en anderzijds de bescherming van privacy, bedrijfsvertrouwelijke informatie en opsporing.

Openbaarmaking van sanctiebesluiten geschiedt nu op basis van artikel 3.1 Wet open overheid (WOO). Volgens haar eigen beleidsregels voor openbaarmaking publiceert de AP in beginsel alle sanctiebesluiten, met uitzondering van berispingen.¹² Bij een openbaarmaking op grond van artikel 3.1 WOO vindt er een belangenafweging plaats tussen enerzijds het belang bij openbaarmaking en anderzijds de belangen van de overtreder. Deze belangenafweging is tevens vervat in artikel 5.1 WOO. Volgens vaste jurisprudentie weegt het belang van openbaarmaking van het sanctiebesluit vrijwel altijd zwaarder dan bijvoorbeeld de dreigende reputatieschade voor de overtreder, tenzij de voorzieningenrechter ernstige twijfels heeft over de rechtmatigheid van het sanctiebesluit.¹³ Het amendement van het Tweede Kamerlid Six Dijkstra stelt buiten twijfel dat er voor de AP een openbaarmakingsplicht bestaat, waarmee het grote gewicht dat ook in het kader van sanctiebesluiten aan openbaarmaking wordt gehecht is onderstreept, tenzij sprake is van voornoemde ernstige twijfels. Het hiervoor beschreven en uit de WOO voortvloeiende kader blijft evenwel onverkort van toepassing. Daarmee bevat het amendement voldoende waarborgen. Belangrijke waarborgen zijn onder meer dat de overtreder vooraf om zijn zienswijze moet worden gevraagd, dat hij bezwaar kan maken en naar de voorlopige voorzieningenrechter kan stappen. Bovendien wordt getoetst aan de gronden om van openbaarmaking af te zien zoals opgenomen in artikel 5.1 WOO als deze aan de orde zijn. Die uitzonderingsgronden hebben onder andere betrekking op de privacy van betrokken natuurlijke personen en vertrouwelijke bedrijfsinformatie. Ook de opsporing van strafbare feiten kan maken dat een sanctiebesluit niet openbaar wordt gemaakt. In zoverre geeft de WOO uitdrukking aan de noodzaak tot het vinden van een zorgvuldige balans tussen het belang van precedentwerking (jurisprudentie) en anderzijds de bescherming van privacy, bedrijfsvertrouwelijke informatie en opsporing.

Onderdeel I

Vraag 8

De leden van de Volt-fractie hebben kennisgenomen van het voorgestelde artikel 23a UAVG, waarin een uitzondering is opgenomen op het verbod om bijzondere categorieën van persoonsgegevens te verwerken. Deze uitzondering geldt voor opdrachten die een entiteit op grond van een wettelijk voorschrift moet laten uitvoeren door een accountant. In de memorie van toelichting wordt gesteld dat er in deze gevallen sprake is van een zwaarwegend algemeen belang. De leden van de Volt-

¹¹ Artikelen 84 tot en met 86 van de Franse gegevensbeschermingswet: Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/>

¹² Artikel 4.1 van de Beleidsregels openbaarmaking door de Autoriteit Persoonsgegevens.

¹³ Zie onder meer de uitspraak ABRvS 10 november 2010 [ECLI:NL:RVS:2010:BO3468](https://www.ecli.nl/nl/RVS:2010:BO3468) (r.o. 2.5), die sindsdien veelvuldig is aangehaald. Deze jurisprudentie geldt ook voor de AP, zo bleek uit de uitspraak ABRvS 29 mei 2024, [ECLI:NL:RVS:2024:2221](https://www.ecli.nl/nl/RVS:2024:2221), overweging 5.2.

fractie verzoeken de regering om toe te lichten wat er onder een zwaarwegend algemeen belang wordt verstaan.

Zoals hiervoor reeds is geantwoord op een gelijksoortige vraag van de leden van de fractie van de ChristenUnie is het niet mogelijk om de term “zwaarwegend algemeen belang” in algemene zin nader te omlijnen. Ten aanzien van deze specifieke grondslag kan worden gezegd dat daar waar een wettelijke verplichting bestaat tot het doen laten uitvoeren van een externe accountantscontrole, in het maatschappelijk verkeer groot gewicht aan die controle wordt gehecht. Investeerders, kredietverschaffers of financiers zijn immers niet in staat de getrouwheid te beoordelen van de financiële verantwoording, terwijl de externe accountant dat wel is. Die belanghebbenden willen hun beslissingen kunnen baseren op de controleverklaring van de externe accountant, die toegang heeft tot informatie om de mate van getrouwheid van de financiële verantwoording te kunnen beoordelen. Om deze reden is de externe controle ook bij wet verplicht gesteld. Indien het in het kader van de controle noodzakelijk is om bijzondere persoonsgegevens te verwerken moet daartoe de bevoegdheid bestaan om de controle te mogen uitvoeren

Vraag 9

Gelet op het feit dat accountants ook commerciële belangen nastreven, achten de leden van de Volt-fractie het van belang alert te blijven op mogelijke ongewenste prikkels die uit het voorgestelde artikel kunnen voortvloeien. Zij merken op dat accountants over kennis beschikken die in potentie kan worden benut, bijvoorbeeld voor het verkrijgen van vervolgoedochten. Dit leidt tot de vraag in hoeverre het voorgestelde artikel ruimte laat voor het nastreven van commerciële doelstellingen. De leden van de Volt-fractie wijzen erop dat de Raad van State heeft geadviseerd nader toe te lichten waarom het wetsvoorstel voorziet in een grondslag voor de verwerking van bijzondere persoonsgegevens door accountants in de UAVG. Deze leden vragen of de regering hierop kan reflecteren. Waarom is er bijvoorbeeld niet voor gekozen om deze specifieke bepaling uitsluitend in sectorale wetgeving vast te leggen?

Het voorgestelde artikel ziet enkel op de bij wettelijk voorschrift verplichte accountantscontroles, waarbij verwerking van persoonsgegevens geschiedt om redenen van zwaarwegend algemeen belang als bedoeld in artikel 9, tweede lid, onderdeel g, AVG. Een dergelijk belang ontbreekt bij de commerciële accountantsopdrachten.¹⁴ Het artikel laat daarom geen ruimte voor het nastreven van commerciële doelstellingen. Daarmee zou bovendien sprake zijn van een verwerking voor een ander doel, waaraan de AVG strikte voorwaarden stelt. De accountants vervullen met de verplichte accountantscontroles een publieke taak van zodanig groot algemeen belang dat bij wettelijk voorschrift is verzekerd dat die taak wordt uitgevoerd. Die controles dienen een grote variëteit aan belangen in het maatschappelijk verkeer die zich ook uitstrekt tot andere gebruikers dan de opdrachtgevers. De verwerking in het kader van de bij wettelijk voorschrift verplichte accountantscontroles geschiedt dan ook om redenen van zwaarwegend algemeen belang als bedoeld in artikel 9, tweede lid, onderdeel g, AVG. Een dergelijk belang ontbreekt bij de vrijwillige accountantsopdrachten. De memorie van toelichting is gezien de opmerking van de Afdeling aangevuld met een toelichting op het gemaakte onderscheid.¹⁵

Er is niet voor gekozen om deze specifieke bepaling uitsluitend in sectorale wetgeving vast te leggen. De reden hiervoor is dat er voor de regeling van de (verplichte) accountantscontroles geen algemene sectorspecifieke wet bestaat.¹⁶ Een regeling in een groot aantal specifieke wetten zou daarnaast ook geen oplossing bieden voor situaties waarin de accountantscontrole door het EU-recht wordt voorgeschreven. Naar het oordeel van de regering wordt de voorspelbaarheid en helderheid van de wetgeving omtrent verplichte accountantscontroles gediend door in de UAVG een uniforme grondslag te regelen voor alle situaties waarin voor de uitvoering van de verplichte controle de verwerking van bijzondere persoonsgegevens noodzakelijk is. Dit belang overstijgt specifieke sectoren en mede daarom heeft de regering ervoor gekozen om voor deze situatie de grondslag voor de verwerking van bijzondere persoonsgegevens in de UAVG te regelen.

Onderdeel K

Vraag 10

¹⁴ Kamerstukken II 2022/23, 36264, nr. 3, p. 20.

¹⁵ Kamerstukken II 2022/23, 36264, nr. 3, p. 18 – 20, en Kamerstukken II 2022/23, 36264, nr. 4, p. 5-6.

¹⁶ Dit is toegelicht in het nader rapport (Kamerstukken II 2022/23, 36264, nr. 4, p. 8-9), de memorie van toelichting (Kamerstukken II 2022/23, 36264, nr. 3, p. 19) en de nota naar aanleiding van het verslag (Kamerstukken II 2023/24, nr. 6, p. 27 en 30).

De leden van de ChristenUnie-fractie hebben kennisgenomen van de wijziging van artikel 29 UAVG. Op grond van artikel 29 UAVG is het verbod om biometrische gegevens te verwerken met het oog op de unieke identificatie van een persoon niet van toepassing, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden. In de wettekst is de eis opgenomen dat de verwerkingsverantwoordelijke bij het gebruik maken van deze wettelijke uitzondering in het concrete geval een actieve toets moet doen om te beoordelen of in het specifieke geval wel sprake is van een zwaarwegend algemeen belang. Gelet op de gevoeligheid en het permanente karakter van biometrische gegevens bij identificatie, vragen deze leden welke waarborgen er bestaan ter voorkoming van oneigenlijk gebruik van deze gegevens. Op welke wijze wordt verzekerd dat biometrie slechts wordt ingezet wanneer er geen minder ingrijpend alternatief voorhanden is? Met het onderhavige wetsvoorstel is beoogd om in artikel 29 UAVG te verduidelijken dat de uitzondering op het verbod op de verwerking van biometrische gegevens alleen van toepassing is als die verwerking noodzakelijk is vanwege een zwaarwegend algemeen belang, en tevens noodzakelijk is voor de specifieke in deze bepaling genoemde doelen. Dit resulteert in een dubbele noodzakelijkheidstoets. De overige vereisten voor de verwerking van persoonsgegevens uit de AVG blijven daarnaast onverminderd van toepassing. Er dient bijvoorbeeld een verwerkingsgrondslag te zijn en er dient te worden voldaan aan de beginselen van gegevensbescherming, zoals opgenomen in artikel 5 AVG. Ook zijn verwerkingsverantwoordelijken op grond van artikel 25 AVG verplicht om onder andere technische en organisatorische waarborgen in de verwerking in te bouwen ter naleving van de AVG en zo te zorgen voor een rechtmatige, behoorlijke en noodzakelijke gegevensverwerking. Ook vereist artikel 32 AVG dat bij de verwerking passende technische en organisatorische maatregelen ter beveiliging daarvan worden getroffen. De verwerkingsverantwoordelijke die biometrische gegevens wil verwerken, dient steeds te zorgen dat hieraan is voldaan. De AP is de toezichthouder op de verwerking van persoonsgegevens en kan ingrijpen wanneer een verwerking niet aan de voorwaarden voldoet.

Onderdeel T

Vraag 11

De leden van de ChristenUnie-fractie hebben kennisgenomen van het voorgestelde artikel 47a van de UAVG. Deze leden onderschrijven het voornemen om een verwerkingsgrondslag te creëren voor de verwerking van persoonsgegevens door tijdelijke commissies zoals bedoeld in de Wet vergoedingen adviescolleges en commissies en tijdelijke adviescolleges als bedoeld in de Kaderwet adviescolleges, die bij koninklijkbesluit, ministerieel besluit of ministeriële regeling worden ingesteld. Zij verzoeken de regering om te verduidelijken welke commissies of adviescolleges buiten de reikwijdte van deze bepaling zullen vallen.

Buiten de reikwijdte van het voorgestelde artikel 47a UAVG vallen ten eerste de permanente adviescolleges zoals bedoeld in artikel 4 van de Kaderwet adviescolleges. Voor zover zij persoonsgegevens verwerken, kan de grondslag daarvoor geregeld worden in de wet waarmee het permanente adviescollege is ingesteld. Ten tweede vallen adviescolleges die niet als hoofdtak hebben het geven van advies zoals bedoeld in artikel 1, onderdeel a, Kaderwet adviescolleges, niet onder het voorgestelde artikel 47a UAVG. En ten derde geldt dat ook voor specifieke adviescolleges en commissies die niet onder de Kaderwet adviescolleges vallen en ook niet onder de Wet vergoedingen adviescolleges en commissies. Te denken valt dan aan de Wetenschappelijke Raad voor het Regeringsbeleid, de Sociaal-Economische Raad.

4. ARTIKEL II. Faillissementswet

Vraag 12

De leden van de CDA-fractie hebben kennisgenomen van de voorgestelde artikelen 68a en 316a, die voorzien in een verwerkingsgrondslag voor de verwerking van bijzondere persoonsgegevens door curatoren en (Wsnp-)bewindvoerders, voor zover dat in het kader van een dringend maatschappelijk belang is vereist. Hiermee wordt gebruik gemaakt van de ruimte die artikel 9 lid 2 sub g van de AVG biedt om bij nationaal recht een uitzondering te maken op het verbod om bijzondere persoonsgegevens te verwerken om redenen van zwaarwegend algemeen belang. De leden van de CDA-fractie vragen hoe de keuze voor deze algemene, weinig specifieke wettelijke grondslagen zich verhoudt tot het Europees Verdrag voor de Rechten van de Mens (EVRM), de Grondwet en de AVG.

Voor de verwerking van bijzondere categorieën van persoonsgegevens gelden strengere regels dan voor de verwerking van reguliere persoonsgegevens. Artikel 9 AVG verbiedt dit in beginsel, met enkele strikte uitzonderingen. Een van die uitzonderingen is de situatie waarin de verwerking noodzakelijk is met het oog op een zwaarwegend algemeen belang. Voor desbetreffende gegevensverwerking moet dan ook een aparte wettelijke grondslag worden gecreëerd waarin passende en specifieke maatregelen en waarborgen worden getroffen. In het licht van de voorgestelde wijziging is de verwerking in het licht van een zwaarwegend algemeen belang noodzakelijk indien zonder die verwerking het faillissement niet kan worden afgewikkeld of ernstig nadeel optreedt voor de gezamenlijke schuldeisers.

Om die reden is het aantal taken waarvoor bijzondere categorieën van persoonsgegevens mogen worden verwerkt beperkt. Enkel voor de specifieke taken waarnaar expliciet verwezen wordt in de artikelen 68a, 215b en 316a, derde lid, Faillissementswet (hierna: Fw) biedt dit wetsvoorstel een grondslag. Voor al deze specifieke taken wordt in de memorie van toelichting bij dit wetsvoorstel nader onderbouwd waarom het verwerken van bijzondere persoonsgegevens noodzakelijk kan zijn. Dat een taak is opgenomen in artikel 68a, 215b of 316a, betekent bovendien nog niet dat verwerking van bijzondere persoonsgegevens steeds is toegestaan. De curator of bewindvoerder zal per geval dienen te beoordelen of verwerking van de bijzondere gegevens inderdaad noodzakelijk is, wat ook is vastgelegd in het derde lid van deze artikelen.

Deze gegevensverwerking door de curator of bewindvoerder kent ook verschillende waarborgen, die nader beschreven zijn in de memorie van toelichting bij dit wetsvoorstel. Zo worden curatoren bijvoorbeeld benoemd door de rechter, en staan zij onder toezicht van de rechter-commissaris. Daarbij geldt dat de curator ook de gedragscode moet respecteren.¹⁷ De curator en bewindvoerder hebben daarnaast een algemene plicht om zorgvuldig met persoonsgegevens om te gaan, en schending daarvan kan op grond van de artikelen 73, 224 of 319 Fw grond zijn voor diens ontslag. Overigens staan curatoren voor wat betreft de verwerking van persoonsgegevens ook onder toezicht van de AP, die bij overtredingen handhavend kan optreden.¹⁸

Door de beperking tot de in de artikelen 68a, 215b en 316a Fw specifiek genoemde en nauwkeurig omschreven taken en de overige waarborgen die gelden, wordt voldaan aan de vereisten van de AVG en het EVRM. In het kader van het EVRM is met name artikel 8 EVRM relevant, dat (onder meer) het recht op privacy waarborgt. Beperkingen van dit recht mogen volgens het artikel enkel bij wet geschieden, en deze dienen noodzakelijk te zijn in een democratische samenleving. Verder mag dit recht slechts worden beperkt ten dienste van een limitatieve opsomming van belangen. Concreet gaat het hier om twee van die belangen, te weten: de bescherming van de rechten van anderen en het economisch welzijn. Allereerst is verwerking van gegevens door de curator nodig om de rechten van anderen, in dit geval de gezamenlijke schuldeisers en andere belanghebbenden bij het faillissement, de surseance of de schuldsanering, te beschermen. Het kan bijvoorbeeld gaan om verwerking van gegevens betreffende de administratie of het inventariseren van de schulden. Zonder deze handelingen kan geen compleet overzicht worden opgesteld van de uitstaande schulden en vorderingen en kan een faillissement niet naar behoren worden afgewikkeld. Daarnaast is deze gegevensverwerking ook noodzakelijk voor effectieve insolventieprocedures. Effectieve insolventieprocedures zijn van belang voor een goed functionerende economie.¹⁹ De inperkingen gaan bovendien ook niet verder dan noodzakelijk. Dit volgt ook reeds uit het hiervoor beschreven AVG-kader en de daaruit voortvloeiende waarborgen. Hierdoor is sprake van een verwerking die in lijn is met de eisen van het EVRM.

Artikel 10, eerste lid, Grondwet bepaalt dat het recht op eerbiediging van de persoonlijke levenssfeer bij of krachtens de wet beperkt mag worden. Het huidige voorstel voorziet in een dergelijke beperking en voldoet daarmee aan de beperkingsvoorschriften die de Grondwet stelt. Daarmee is het voorstel ook in lijn met de Grondwet.

Vraag 13

De leden van de CDA-fractie constateren dat de Afdeling advisering van de Raad van State reeds in 2017 heeft vastgesteld dat, gelet op de rechtspraak van het Europees Hof voor de Rechten van de Mens (EHRM) omtrent artikel 8 EVRM²⁰ en de gevoelige aard van bijzondere persoonsgegevens, het

¹⁷ Zie in het bijzonder artikel 1.1 en 8.3 van de Praktijkregels van INSOLAD.

¹⁸ Zie bijv. Rb Gelderland 7 augustus 2025, ECLI:NL:RBGEL:2025:6547.

¹⁹ Zie onder meer p. 105 e.v. van bijlage 4 van de impact assessment bij richtlijn (2022/0408(COD) waarin wordt ingegaan op de economische gevolgen van (wijzigingen in) het insolventierecht, in de context van de voorgestelde EU-richtlijn (documentnr. SWD/2022/395).

²⁰ EHRM 4 december 2008 S. vs. Marper t. Verenigd Koninkrijk (no. 30562/04 30566/04), r.o. 95-99.

in de rede ligt dat voor uitzonderingen op het verbod om bijzondere persoonsgegevens te verwerken een specifieke wettelijke grondslag nodig is.²¹ Deze leden merken op dat het ontbreken van een specifieke wettelijke grondslag tot gevolg heeft dat voor burgers nauwelijks voorzienbaar is welke bijzondere persoonsgegevens kunnen worden verwerkt op grond van de artikelen 68a en 316a. Kan de regering nader motiveren hoe deze algemene, weinig specifieke grondslagen voor de verwerking van bijzondere persoonsgegevens door curatoren en (Wsnp-)bewindvoerders zich verhoudt tot het advies van de Afdeling advisering van de Raad van State?

In haar advies bij dit wetsvoorstel schetste de Afdeling advisering van de Raad van State dat een algemene en open geformuleerde taakomschrijving op gespannen voet kan staan met het uitgangspunt dat persoonsgegevens zoveel mogelijk voor welbepaalde, uitdrukkelijke omschreven en gerechtvaardigde doeleinden worden verzameld en verwerkt. Naar aanleiding van het advies is het wetsvoorstel aangepast. De algemene taakomschrijving in de artikelen 68a, 215b en 316a, eerste lid, Fw is ingeperkt, doordat hieraan is toegevoegd dat de curator of bewindvoerder alleen persoonsgegevens kan verwerken voor zover dit bij of krachtens de wet noodzakelijk is voor de uitoefening van zijn taak. Hierdoor kan niet meer enkel teruggevallen worden op de algemene taakomschrijving, maar zal er in alle gevallen een voldoende specifieke omschrijving in de wet of in de lagere regelgeving moeten zijn voor verwerking van persoonsgegevens. Het tweede lid van de artikelen 68a, 215b en 316a Fw geeft een lijst met handelingen die in ieder geval deze basis bieden. Voor het verwerken van bijzondere persoonsgegevens geldt dat dit alleen mogelijk is voor de in het derde lid van de artikelen 68a, 215b en 316a Fw specifiek genoemde handelingen, en dan ook nog alleen voor zover dit in het concrete geval noodzakelijk is voor de uitoefening van de taak van de curator of de bewindvoerder. Daarmee heeft de regering gepoogd recht te doen aan het advies van de Raad van State.

Vraag 14

De aan het woord zijnde leden verwachten dat de invoering van de voorgestelde artikelen 68a en 316a zal leiden tot knelpunten in de uitvoeringspraktijk. De beoordeling van de vraag of in een concreet geval bijzondere persoonsgegevens mogen worden verwerkt, komt in belangrijke mate te rusten op de curatoren en (Wsnp-)bewindvoerders. Deze leden vragen in hoeverre curatoren en (Wsnp-)bewindvoerders in staat zijn om de generiek geformuleerde normen uit de artikelen 68a en 316a op een consistente wijze toe te passen. Zij verzoeken de regering in dit verband te reflecteren op de uitvoerbaarheid van de voorgestelde bepalingen.

Op dit moment bestaat onduidelijkheid onder curatoren en bewindvoerders in welke gevallen zij persoonsgegevens mogen verwerken. Hierdoor bestaat het gevaar dat de huidige regels uit onder andere de AVG niet of niet consistent worden toegepast. Het doel van dit wetsvoorstel is om de curatoren en bewindvoerders meer handvatten te bieden. Daarom is in het tweede lid van de door de leden van de CDA-fractie genoemde artikelen een lijst opgenomen met taken waarvoor het is toegestaan om persoonsgegevens te verwerken. Voor bijzondere categorieën van persoonsgegevens is vervolgens een verdere aanscherping aangebracht in het derde lid van deze artikelen. Hierin staan strengere eisen opgenomen. Ik verwacht daarom dat deze grondslagen curatoren en bewindvoerders zullen helpen bij uitvoering van hun taken en zullen leiden tot meer consistentie in de uitvoeringspraktijk. Dat met deze bepalingen duidelijkheid wordt geschapen wordt ondersteund door de reacties in de internetconsultatie, van bijvoorbeeld de Nederlandse Orde van Advocaten en door de vereniging van insolventierechtadvocaten ("INSOLAD").

Vraag 15

Tot slot vragen de leden van de CDA-fractie of het feit dat de rechtmatigheid van de verwerking van bijzondere persoonsgegevens afhankelijk is van de correcte toepassing van de generiek geformuleerde bepalingen een risico vormt voor de rechtspositie van de betrokkene.

In het derde lid van de eerder door de leden van de CDA-fractie geciteerde artikelen worden de specifieke taken opgesomd waarvoor verwerking van bijzondere persoonsgegevens onder voorwaarden geoorloofd kan zijn. Daaruit volgt dat de mogelijkheid om bijzondere persoonsgegevens te verwerken aan strikte toepassingsvoorwaarden is gebonden. Een voorbeeld van een situatie waarin dit is toegestaan is de situatie dat brieven die aan de gefailleerde zijn gericht worden geopend en die brieven bijzondere persoonsgegevens bevatten. Uiteraard laten de genoemde normen een zekere beoordelingsruimte aan de curator of de bewindvoerder. Daarmee is niet gezegd dat iedere interpretatie van de wettelijke normen daarmee redelijk is. De AP houdt

²¹ Kamerstukken II 2017/18, 34 851, nr. 4.

toezicht op de toepassing van het wettelijk kader en de begrenzing die dit kader stelt aan de mogelijkheid om bijzondere persoonsgegevens te verwerken. De AP kan daarbij ook handhavend optreden indien een curator op een onjuiste grond of zonder duidelijke noodzaak persoonsgegevens verwerkt. Betrokkene kan altijd van het inzagerecht uit artikel 15 AVG gebruikmaken en daarna eventueel een klacht indienen bij de AP. Dit stelsel van toezicht beoogt juist ook de rechtspositie van betrokkenen te beschermen.

5. ARTIKEL III. Vreemdelingenwet 2000

Vraag 16

De leden van de Volt-fractie hebben kennisgenomen van het voorgestelde artikel 107 van de Vreemdelingenwet 2000, dat voorziet in de door de UAVG vereiste wettelijke grondslag voor de beoogde uitwisseling van persoonsgegevens tussen de minister en de bij ministeriële regeling aangewezen organisaties of instellingen die taken vervullen op het gebied van begeleiding of ondersteuning van vreemdelingen, met gebruikmaking van het vreemdelingennummer. Naar aanleiding van dit artikel hebben deze leden enkele vragen. Allereerst vragen zij of vreemdelingen op dit moment bescherming genieten onder de AVG. Daarnaast vernemen zij graag welke organisaties of instellingen bij ministeriële regeling zijn aangewezen, en welke vereisten aan deze partijen worden gesteld. Worden er specifieke eisen gesteld ten aanzien van de verwerking en beveiliging van persoonsgegevens? Tot slot merken de leden van de Volt-fractie op dat in lid 8 van het voorgestelde artikel wordt gesproken over het verstrekken van gegevens en inlichtingen die noodzakelijk zijn 'voor de uitvoering van hun taak'. Deze leden vragen of hiermee wordt bedoeld op een wettelijke taak.

Toepasselijkheid van de AVG is niet afhankelijk van de nationaliteit van betrokkenen, zodat in ieder geval ook vreemdelingen onder het toepassingsbereik vallen (artikel 3 AVG en overweging 2 bij de AVG). Overweging 14 van de AVG bevestigt dit: "De bescherming die door deze verordening wordt geboden, heeft betrekking op natuurlijke personen, ongeacht hun nationaliteit of verblijfplaats, in verband met de verwerking van hun persoonsgegevens." Voor toepasselijkheid van de AVG is volgens artikel 3 AVG wel vereist dat sprake is van verwerkingsverantwoordelijken of verwerkers die in de Unie gevestigd zijn ('criterium van vestiging') of verwerkingsverantwoordelijken of verwerkers die niet in de Unie gevestigd zijn maar wel persoonsgegevens verwerken van betrokkenen die in de Unie verblijven door aan hen goederen of diensten aan te bieden of hun gedrag te monitoren ('criterium van gerichtheid').

In het voorgestelde artikel 107, achtste lid, van de Vreemdelingenwet 2000 wordt geregeld dat informatie kan worden gedeeld met andere organisaties dan bestuursorganen. Vereist is dat het gaat om "bij ministeriële regeling aangewezen organisaties of instellingen die werkzaam zijn op het gebied van begeleiding of ondersteuning van vreemdelingen, niet zijnde bestuursorganen". Hierbij wordt gedacht aan het aanwijzen van VluchtelingenWerk Nederland (VWN), de Internationale Organisatie voor Migratie (IOM) en Stichting Nidos.²² Deze organisaties spelen een rol in de begeleiding en ondersteuning van vreemdelingen. Het kan daarbij ook gaan om niet-wettelijke taken. Voor wat betreft de beveiliging van de persoonsgegevens moeten deze organisaties en instellingen zich houden aan de beveiligingsplicht uit artikel 32 AVG.

6. ARTIKEL X. Wet op het financieel toezicht

Vraag 17

De leden van de GL-PvdA-fractie hebben kennisgenomen van de voorgestelde wijziging van artikel 3:17 van de Wet op het financieel toezicht (Wft). In reactie op de voorgestelde wijziging stelt Privacy First dat "de rechtsbescherming van klanten in zaken op het gebied van de Wft en het financiële recht volstrekt onvoldoende is".²³ Dit geeft de leden van de GL-PvdA-fractie aanleiding tot het stellen van de volgende vragen. Deze leden vragen allereerst welke rechten een betrokkene heeft wanneer transacties worden geblokkeerd of opgeschort. Waar en op welke wijze zijn deze rechten verankerd? Voorts vragen zij wat de rol van het Klachteninstituut Financiële Dienstverlening (Kifid) is in dergelijke situaties voor consumenten. Kunnen ook zzp'ers en mkb'ers zich tot het Kifid wenden? Daarnaast vernemen deze leden graag of banken en betaalinstellingen wettelijk verplicht zijn om actief met betrokkenen te communiceren over de blokkering of opschorting van transacties. Zo ja,

²² Kamerstukken II 2022/23, 36264, nr. 3, p. 60.

²³ Paper Privacy First inzake rondetafelgesprek Verzamelwet gegevensbescherming 4 december 2024, 1 december 2024, https://privacyfirst.nl/wp-content/uploads/paper_UAVG_SPF_TK_1dec2024.pdf.

op welke wettelijke bepaling is die verplichting gebaseerd? Zo nee, acht de regering het wenselijk om dergelijke verplichting alsnog in te voeren?

Wanneer een transactie wordt geblokkeerd of opgeschort, wordt een klant hiervan op de hoogte gesteld. Een klant kan hierover een klacht indienen bij de betaaldienstverlener op grond van de interne klachtenprocedure, waarvan in artikel 4:17 van de Wet op het financieel toezicht is bepaald dat betaaldienstverleners die moeten hebben. Wanneer een klant ontevreden is met de uitkomst, kan de klant het Kifid inschakelen om een onafhankelijk oordeel te vormen. Ook zzp'ers en mkb'ers kunnen zich tot het Kifid wenden, mits de omzet per jaar niet meer dan vijf miljoen euro bedraagt. Betaaldienstverleners zijn verplicht om te communiceren met hun klanten over het blokkeren of opschorten van transacties. Deze verplichting volgt uit artikel 79 van de richtlijn betaaldiensten, die is omgezet in artikel 533 van Boek 7 van het Burgerlijk Wetboek.

Vraag 18

De leden van de GL-PvdA-fractie merken op dat in het voorgestelde tiende lid is bepaald dat bij algemene maatregel van bestuur (AMvB) nadere regels worden gesteld met betrekking tot passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van cliënten in geval van het blokkeren of opschorten van betalingstransacties. Deze leden vragen waarom is gekozen voor regeling bij AMvB. Waarom wordt dit niet in de wettekst zelf geregeld? Wanneer is de vaststelling van AMvB voorzien? Bij AMvB worden in ieder geval nadere regels gesteld over gegevensanalyse, beveiliging en integriteit. Deze leden vragen of adequate communicatie met betrokkenen en over rechtsbescherming ook niet bij AMvB moet worden geregeld. Kan de regering hierop reflecteren?

Er is gekozen voor uitwerking bij AMvB, omdat de uitwerking technische, uitvoerings- of veiligheidsnormen bevat die sneller aan verandering onderhevig zijn en waarbij de details beter op uitvoeringsniveau geregeld kunnen worden. Een ontwerp-AMvB is opgesteld. Hierover zal online worden geconsulteerd en gelijktijdig zal het ontwerp aan de AP worden voorgelegd voor advies. Vervolgens wordt de AMvB voorgelegd aan de Afdeling advisering van de Raad van State voor advies. Hoe snel dit proces verloopt hangt af van de ontvangen consultatiereacties, het advies van de AP, het advies van de Raad van State en de tijd die het kost om deze adviezen zorgvuldig te verwerken.

De communicatie met betrokkenen en rechtsbescherming is reeds bij wet geregeld. Zo heeft de betrokkene, zoals hierboven ook benoemd, het recht om geïnformeerd te worden. Ook is een betaaldienstverlener op grond van artikel 4:17 van de Wet op het financieel toezicht verplicht om zorg te dragen van adequate behandeling van klachten. Het is daarom niet nodig om deze aspecten ook bij AMvB te regelen.

Vraag 19

De leden van de CDA-fractie hebben kennisgenomen van de twee voorgestelde leden die in artikel 3:17 van de Wet op het financieel toezicht (Wft) een verplichting tot het uitvoeren van een transactiemonitoring introduceren. Zij gaan ervan uit dat bij de uitvoering van transactiemonitoring gebruik wordt gemaakt van een zekere mate van artificiële intelligentie (AI). In dat verband wensen de leden enkele vragen te stellen. Deze leden vragen allereerst of door banken en betaalinstellingen randvoorwaarden worden verankerd die het mogelijk maken om achteraf te controleren hoe digitale uitvoering heeft plaatsgevonden en aan de hand van welke data algoritmen zijn getraind. Kan dit inzichtelijk worden gemaakt voor desbetreffende cliënten? Daarnaast vragen de leden van de CDA-fractie of banken en betaalinstellingen verplicht worden om jegens cliënten van wie transacties zijn geblokkeerd of opgeschort, inzichtelijk te maken op welke gronden dit besluit is genomen en op welke wijze algoritmen en AI hebben bijgedragen aan de totstandkoming ervan. Tot slot vragen deze leden welke mogelijkheden cliënten hebben om bezwaar te maken tegen het geautomatiseerd blokkeren of opschorten van een transactie.

De leden stellen een aantal vragen over het gebruik van AI bij transactiemonitoring. Voordat deze vragen worden beantwoord, is het belangrijk om stil te staan bij de twee verschillende vormen van transactiemonitoring. Betaaldienstverleners maken gebruik van transactiemonitoring gericht op het voorkomen van fraude, en transactiemonitoring gebaseerd op anti-witwasregelgeving. Het onderhavige wetvoorstel ziet op transactiemonitoring gericht op het voorkomen van fraude, dus in de beantwoording van de vragen zal dit als uitgangspunt worden genomen. Transactiemonitoring gericht op het voorkomen van fraude, kan leiden tot het blokkeren of opschorten van transacties wanneer er signalen zijn dat er bijvoorbeeld sprake is van een betaling die niet door de klant is

geautoriseerd. Het doel van deze vorm van transactiemonitoring is het beschermen van de klant. Zo wordt voorkomen dat klanten slachtoffer worden van fraude, en wordt het fraudeurs moeilijker gemaakt om slachtoffers te maken.

De leden vragen allereerst naar de randvoorwaarden om achteraf te kunnen controleren hoe digitale uitvoering heeft plaatsgevonden en hoe algoritmen zijn getraind. Bij de inzet van AI voor transactiemonitoring worden governance- en controlemechanismen toegepast waardoor AI-systemen worden geregistreerd. Deze registratie maakt het mogelijk om achteraf vast te stellen welke databronnen zijn gebruikt voor het trainen, welke technieken zijn toegepast en welke medewerkers verantwoordelijk zijn voor het ontwerp, de validatie en het beheer van het model. Vervolgens vragen de leden naar de inzichtelijkheid van de gronden en het gebruik van AI. Voor transactiemonitoring om fraude tegen te gaan wordt gebruik gemaakt van geautomatiseerde detectiemechanismen. Deze mechanismen zorgen voor een alert, maar de uiteindelijke besluitvorming vereist menselijke tussenkomst. Een transactie kan dan vervolgens worden opgeschort of geblokkeerd, maar alleen na een menselijke check. De klant ontvangt een motivering van het besluit tot opschorting of blokkering, tenzij ander toepasselijk Unierecht of nationaal recht dit verbiedt (artikel 7:533 van het Burgerlijk Wetboek). Hierbij wordt niet gedeeld op welke gronden het detectiemechanisme heeft gereageerd. Het delen van deze informatie is namelijk erg gevoelig. Als bekend wordt hoe het detectiemechanisme werkt, kan dit misbruikt worden door fraudeurs. Het belang van transparantie voor de klant wordt daarom afgewogen tegen het bredere belang van een effectieve transactiemonitoring.

De leden vragen tot slot naar de mogelijkheden om bezwaar te maken tegen het geautomatiseerd blokkeren of opschorten van een transactie. Het maken van bezwaar tegen geautomatiseerde besluitvorming is mogelijk. Dit volgt ook uit het voorgestelde artikel 3:17, negende lid, onder c, van de Wft, dat bepaalt dat de betrokken cliënt de mogelijkheid moet hebben om zijn standpunt over het blokkeren of opschorten van de transactie kenbaar te maken. De manier waarop de cliënt bezwaar kan maken, is doorgaans geregeld in de algemene voorwaarden en interne klachtenprocedures. Indien de klant ontevreden is met de uitkomst van de interne klachtprocedure, kan de klant het geschil voorleggen aan het Kifid. Het Kifid werkt onafhankelijk en onpartijdig. Dit betekent dat betaaldienstverleners geen enkele invloed hebben op de klachtbehandeling en het inhoudelijk oordeel. Uiteraard kan een klant ook naar de rechter stappen.

7. Overig

Vraag 20

De leden van de GL-PvdA-fractie merken op dat een aanzienlijk aantal uitvoeringsorganisaties, die in de praktijk geraakt worden door het voorliggende wetsvoorstel, een uitvoeringstoets heeft uitgevoerd. In verschillende uitvoeringstoetsen zijn concrete voorstellen tot aanpassing gedaan. Deze leden wijzen in dit verband graag op de werkzaamheden van de brainstormgroep uitvoerbaarheid van de Eerste Kamer, die beoogt de aandacht voor de uitvoerbaarheid van wetgeving te vergroten. Een van de aandachtspunten is het verkrijgen van meer inzicht in de wijze waarop signalen van de uitvoering verwerkt worden in wetsvoorstel. Tegen deze achtergrond verzoeken de leden van de GL-PvdA-fractie de regering toe te lichten welke voorstellen tot aanpassing uit de reacties van de volgende organisaties niet, of niet volledig, zijn overgenomen, en om welke reden niet: de Autoriteit Persoonsgegevens (AP), de Nederlandse Orde van Advocaten (NOvA), het Platform Bijzondere Opsporingsdiensten, de Politie, de Raad voor de Rechtspraak, de Raad voor Rechtsbijstand (RvR), de Vereniging Nederlandse Gemeenten (VNG) en VNO-NCW en MKB Nederland. Daarnaast ontvangen deze leden graag een reactie op de voorstellen uit het paper van Privacy First, dat is opgesteld in het kader van het rondetafelgesprek van 4 december 2024 in de Tweede Kamer.²⁴

De voornoemde organisaties hebben in de consultatie adviezen uitgebracht. Die adviezen hebben geleid tot kleinere en grotere aanpassingen in het wetsvoorstel. De toelichting bij het wetsvoorstel is naar aanleiding van de consultatiereacties ook aangepast, zie in het bijzonder hoofdstuk 3 voor een beschrijving van de wijze waarop de consultatiereacties zijn verwerkt, dan wel niet in het wetsvoorstel zijn meegenomen. In algemene zin geldt dat de consultatiereacties in drie categorieën kunnen worden ingedeeld. Ten eerste zijn er reacties met voorstellen om onderwerpen die niet in het onderhavige wetsvoorstel zijn opgenomen, daarin toch te regelen, omdat zij regeling in de UAVG

²⁴ Paper Privacy First inzake rondetafelgesprek Verzamelwet gegevensbescherming 4 december 2024, 1 december 2024, https://privacyfirst.nl/wp-content/uploads/paper_UAVG_SPF_TK_1dec2024.pdf.

zouden verdienen. Dat geldt bijvoorbeeld voor de voorstellen die zijn gedaan door het Rathenau instituut, waarnaar de leden van de fractie van GL-PvdA in hun vraag aan het begin van het verslag hebben verwezen. Zoals in reactie op die vraag is opgemerkt dient een voorstel als deze naar zijn aard beperkt te blijven, waarbij vooral is getracht in het onderhavige voorstel uitsluitend wijzigingsvoorstellen op te nemen die in omvang en complexiteit geen zelfstandig wetsvoorstel rechtvaardigen. Naar het oordeel van de regering voldeed een aantal voorstellen dat tijdens de consultatie is gedaan niet aan dit criterium. De belangrijkste onderwerpen waarvoor dit geldt zijn opgenomen in hoofdstuk 3 van de memorie van toelichting bij het wetsvoorstel.

Ten tweede zijn er reacties die hebben geleid tot een inhoudelijke wijziging van het wetsvoorstel, bijvoorbeeld het schrappen van onderdelen van het wetsvoorstel. Zo heeft de reactie van de AP ertoe geleid dat de voorgestelde artikelen waarbij een grondslag voor de verwerking van bijzondere persoonsgegevens en persoonsgegevens van strafrechtelijke aard bij het voldoen aan een bevel of vordering op grond van het Wetboek van Strafvordering, voor het doen van aangifte of klacht van strafbare feiten of voor het voldoen aan een wettelijke aangifteplicht, uit het voorstel is geschrapt. Ook is mede naar aanleiding van het advies van de AP de voorgestelde wijziging van artikel 41 UAVG geschrapt. Ook andere instanties die in de consultatie hebben gereageerd hadden bezwaren tegen de voorgestelde bepaling. Al deze reacties tezamen gaven uitdrukking aan het beeld dat artikel 41 UAVG mogelijk ingrijpend zou moeten worden gewijzigd. Een dergelijke ingrijpende herziening van artikel 41 UAVG past niet bij het karakter van het onderhavige wetsvoorstel. Ten derde zijn er reacties die aanleiding hebben gegeven tot verdere verduidelijking van het wetsvoorstel. Het betrof in die gevallen meestal een technische aanpassing van het wetsvoorstel. Zo hebben de consultatiereacties onder andere geleid tot een aanpassing van het voorgestelde artikel 68a van de Faillissementswet.

Vraag 21

De aan het woord zijnde leden merken op dat het wetsvoorstel niet voorziet in bijzondere bepalingen ten aanzien van de geautomatiseerde verwerking van persoonsgegevens. Naar het oordeel van deze leden kan daarvan wel sprake zijn, bijvoorbeeld bij het verwerken van biometrische gegevens, transactiemonitoring door banken of bankinstellingen en het delen van medische gegevens. Kan de regering toelichten of, en zo ja op welke wijze, zij voorziet dat er sprake zal zijn van de algoritmische uitvoering van dit wetsvoorstel of daaruit voortvloeiende regelgeving? En op welke wijze wordt gewaarborgd dat wordt voldaan aan de vereisten die de AVG stelt aan de geautomatiseerde verwerking van persoonsgegevens?

Behoudens de voorgestelde wijziging van de Wet op het financieel toezicht inzake transactiemonitoring met het oog op het tegengaan van fraude (zie het antwoord op de vragen 17 tot en met 19), voorziet het onderhavige wetsvoorstel niet in regelgeving ten aanzien van algoritmische uitvoering. Tegelijkertijd bevat de AVG natuurlijk reeds regels over geautomatiseerde besluitvorming en die regels zijn onverkort van toepassing. Op grond van artikel 22, eerste lid, AVG heeft iedereen het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden, of dat hem anderszins in aanmerkelijke mate treft. Het wetsvoorstel doet niets af aan de waarborgen die deze bepaling stelt. Het is aan elke verwerkingsverantwoordelijke om processen zo in te richten dat deze hiermee in overeenstemming zijn en aan de AP om daarop toezicht te houden.

Vraag 22

De leden van de GL-PvdA-fractie verzoeken de regering toe te lichten op welke wijze het toezicht op de uitvoering van dit wetsvoorstel wordt georganiseerd. Zij gaan ervan uit dat de Autoriteit Persoonsgegevens (AP) hierbij een centrale rol zal vervullen. Tegelijkertijd spreken deze leden hun zorgen uit over de vraag of de AP, gelet op haar reeds omvangrijke takenpakket, over voldoende capaciteit en middelen beschikt om ook de toezichttaken die uit dit wetsvoorstel voortvloeien adequaat te vervullen. Worden aan de AP hiervoor extra middelen toebedeeld? Daarnaast vernemen deze leden graag of naast de AP ook andere toezichthouders, zoals De Nederlandsche Bank (DNB), de Autoriteit Financiële Markten (AFM), de Inspectie Gezondheidszorg en Jeugd (IGJ), de Nederlandse Beroepsorganisatie van Accountants (NBA), of andere instanties, bij het toezicht betrokken zijn. Indien dit het geval is, hoe verhouden deze vormen van toezicht zich tot elkaar?

Het wetsvoorstel brengt geen veranderingen in de organisatie van het toezicht. De AP is de belangrijkste toezichthouder waar het gaat om de verwerking van persoonsgegevens. Haar toezichthoudende taak ziet op grond van artikel 6, derde lid, UAVG niet alleen op de naleving van de

AVG, maar ook op de naleving van de UAVG en andere regelingen op grond waarvan persoonsgegevens worden verwerkt. Het onderhavige wetsvoorstel introduceert niet zodanige vormen van of grondslagen voor gegevensverwerking, dat dit wetsvoorstel aanleiding geeft om extra middelen toe te delen voor het toezicht. Het wetsvoorstel kent ook geen extra taken toe aan de toezichthouders. Voor zover andere toezichthouders belast zijn met het toezicht op de naleving van regels uit specifieke bijzondere wetten, behouden deze toezichthouders die bevoegdheid. De AP beschikt voor het verrichten van haar taken over een jaarlijks budget van circa 49 miljoen euro, waarvan circa 45 miljoen voor het toezicht op de naleving van de AVG. Naar het oordeel van de regering beschikt zij hiermee over voldoende middelen voor haar taken, al moet de AP net als alle toezichthouders en overheidsdiensten keuzes maken en prioriteiten stellen in haar taakuitvoering. Op het budget van de AP is nader ingegaan in de brief van de Staatssecretaris Rechtsbescherming van 11 juli 2025 inzake de evaluatie van de AP.²⁵ Daarin staat dat de Staatssecretaris met de AP heeft afgesproken dat de AP in de nabije toekomst, in samenspraak met JenV, een meetinstrument en indicatoren ontwikkelt om inzicht te krijgen in het doelmatig en doeltreffend functioneren van de AP en om op een transparante wijze te verantwoorden dat middelen doelmatig en doeltreffend worden besteed. Over het budget van de AP heeft de Staatssecretaris geschreven dat hij samen met de AP stappen wil zetten om te komen tot een meer objectieve basis die ondersteunend is bij de besluitvorming over een passende hoogte van het budget van de AP. De Kamerbrief licht deze stappen toe en vermeldt dat tevens een vergelijkend onderzoek denkbaar is naar de budgetten van Europese gegevensbeschermingstoezichthouders.

Vraag 23

De leden van de ChristenUnie-fractie merken op dat zij signalen hebben ontvangen dat een te strikte interpretatie van de AVG gegevensuitwisseling tussen domeinen belemmert, waardoor de uitvoering onder druk komt te staan. Zij vragen de regering te reflecteren op deze signalen. Op welke wijze draagt de regering zorg voor een eenduidige voorlichting over de voorgestelde wijzigingen, teneinde misstanden en knelpunten in de uitvoering te voorkomen?

Deze signalen zijn niet nieuw. De AVG lijkt binnen veel geledingen te streng te worden toegepast. Grondslagen voor gegevensverwerking worden bijvoorbeeld soms onnodig restrictief geïnterpreteerd waardoor niets mogelijk lijkt. Dit is geen wenselijke situatie. De AP geeft actief voorlichting over de werking en de begrippen van de AVG, en draagt daarmee bij aan het wegnemen van onduidelijkheid over de interpretatie van de AVG en de reikwijdte van verwerkingsgrondslagen. Signalen over gegevensuitwisseling tussen domeinen komen ook aan bod in de tijdelijke 'Taskforce Gegevensdeling' van het ministerie van JenV, die zich richt op het aanpakken van knelpunten in gegevensdeling op gebieden zoals de georganiseerde en ondermijnende criminaliteit, maar ook op problemen bij gegevensuitwisseling met instanties zoals het UWV en de Belastingdienst. Daarnaast zijn knelpunten geïnventariseerd die het Netwerk Publieke Dienstverleners ervaart. Over de aanpak heeft de minister van Sociale Zaken en Werkgelegenheid, als coördinerend minister voor Werk aan Uitvoering, onder meer op 20 juni en 20 maart 2025, voortgangsbrieven gezonden aan de Tweede Kamer.²⁶

De onderhavige Verzamelwet is in samenspraak met verschillende betrokken partijen tot stand gekomen en geeft daarmee gevolg aan langer gevoelde behoeften tot verbetering van het gegevensbeschermingsrecht, zowel in de vorm van nieuwe waarborgen als in de zin van wijzigingen die de praktische uitvoerbaarheid ervan kunnen verbeteren. Gezien het beperkte en vooral technische karakter van de voorgestelde wijzigingen in het onderhavige wetsvoorstel zal de regering naar aanleiding van het onderhavige wetsvoorstel niet voorzien in een eigenstandig voorlichtingstraject. Als gezegd zijn veel bepalingen in het wetsvoorstel tot stand gekomen in samenspraak met diverse betrokken partijen. Deze belanghebbenden zijn ook om die reden voorbereid op het wetsvoorstel en de inhoud daarvan.

Vraag 24

De leden van de Volt-fractie vernemen bij gelegenheid van deze aanpassing van de UAVG graag – ook in het licht van de evaluatie van het functioneren van de AP – wat er wordt gedaan om de AP te ontlasten, waarbij de AP niet vooral focust op controle en boetes en een bottleneck wordt, maar die juist een ondersteunend orgaan kan worden. Deze leden willen suggereren daarbij bijvoorbeeld het

²⁵ Kamerstukken II 2024/25, 25268, nr. 242.

²⁶ Kamerstukken II 2024/25, 29362, nr. 381 en 374.

opzetten van ‘innovatie-sandboxes’ te overwegen, beheerd door en onder toezicht van de AP, zoals men al doet in Noorwegen. Dit kan leiden tot betere innovaties met al ingebouwde ‘best practices’. Biedt de AVG al de ruimte voor het delegeren van toezicht aan gecertificeerde organisaties? In hoeverre kan met de UAVG, o.a. door het meetbaar en duidelijk maken van het volgen van regels en het uitvoeren van toezicht, de uitvoering van de AVG gestroomlijnd worden met de uitvoering in de andere EU-lidstaten? Hoe kan voorkomen worden dat mismatches in de uitvoering van de AVG leiden tot het uitbuiten van persoonsgegevens en dus ook het onbeschermd laten van burgers over de landsgrenzen?

Wat betreft innovatie-sandboxes geldt dat de AVG hierin niet voorziet. Ten aanzien van de vraag naar de mogelijkheden om het toezicht door de AP te delegeren aan gecertificeerde organisaties geldt dat hoofdstuk VI AVG bepaalt dat iedere lidstaat een onafhankelijke toezichthouder moet hebben, met eigen onderzoeks- en handhavingsbevoegdheden. De kerntaken en bevoegdheden van de toezichthouder (het doen van onderzoek, het opleggen van corrigerende maatregelen en boetes) kunnen niet worden overgedragen of gedelegeerd aan derde private partijen. Wel biedt de AVG – onverminderd de taken en bevoegdheden van de toezichthoudende autoriteit – ruimte voor gedeeld toezicht in het kader van certificeringsmechanismen en gedragscodes. Dat is aan de orde bij geaccrediteerde organen die toezicht houden op een goedgekeurde gedragscode (artikel 41 AVG) of bij geaccrediteerde certificeringsorganen die beoordelen of een product, proces of dienst in aanmerking komt voor een AVG-certificaat en dit periodiek toetsen (artikel 43 AVG).

Voor het antwoord op de vraag van de leden van de Volt-fractie naar wat er wordt gedaan om de AP te ontlasten, verwijst de regering naar de brief van de Staatssecretaris Rechtsbescherming van 11 juli 2025 waarin op de evaluatie wordt gereageerd.²⁷

Vraag 25

De leden van de Volt-fractie vernemen graag hoe de monitoring van compliance effectief en preventief wordt uitgevoerd. De AVG schrijft in artikel 25 voor dat de verwerkingsverantwoordelijke al het redelijke doet om aan de rechten van de burger te voldoen door middel van ‘privacy-by-design’. Dit design dient ook waarborgen in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen in de fase van verwerking van gegevens. Niettemin treden de problemen veelal op bij de operationele uitvoering na de design. Hoe kan worden vastgesteld dat de rechten van burgers daadwerkelijk beschermd worden (outcome), in plaats van slechts uit juridisch opzicht vast te stellen de verwerkingsverantwoordelijke “compliant” is in die zin dat procedures en stappen zijn afgevinkt (output)? Welke KPI-drempel wordt dan gezien als redelijke inzet? Welke rol speelt datakwaliteit hierin en welk standaard wordt daarvoor gehanteerd? Zijn er voorbeelden uit de praktijk en hoe verschilt dit per sector?

Op deze vraag kan slechts in algemene zin een antwoord worden gegeven, nu zij niet lijkt te zien op een onderdeel van het onderhavige wetsvoorstel. Effectieve en preventieve monitoring van compliance gebeurt door een systematisch en continu proces dat bestaat uit risicoanalyse, toezicht, handhaving, en het toepassen van het klachtmechanisme waarmee schendingen van de AVG kunnen worden gemeld bij de AP. Het is aan de AP om vast te stellen of de rechten van burgers conform de AVG daadwerkelijk beschermd worden. Datakwaliteit speelt hierin een belangrijke rol gelet op het beginsel dat persoonsgegevens juist moeten zijn (het beginsel van juistheid uit artikel 5, eerste lid, onder d, AVG).

Vraag 26

Tot slot vernemen de leden van de Volt-fractie graag waar Nederland staat als het gaat om de uitvoering van de artikelen 40 t/m 43 van de AVG met betrekking tot gedragscodes, gedelegeerd toezicht en certificering. Worden deze artikelen, ook sectoraal, geïmplementeerd en hoeveel prioriteit heeft dit? Klopt het dat sectorale adviezen kunnen worden getoetst door de AP en dat deze kunnen worden gebruikt als gegevensbeheerstandaard binnen deze sectoren? Zouden sectorale toezichtsorganen dan niet juist als acceleratie kunnen worden ingezet om bijvoorbeeld regels voor accountants of andere sectoren in samenspraak met de AP vast te leggen in het geval van dilemma’s zoals het gebruik van sensitieve persoonsgegevens? Zou dat dan ook niet gelijk behulpzaam kunnen zijn om open normen in te vullen in overeenstemming met de specifieke behoeften die in een sector leven? Zou dat niet leiden tot continue communicatie tussen experts in een sector en privacy experts van de AP met als resultante standaarden die blijven overeenkomen met de sectorale werkelijkheid?

²⁷ Kamerstukken II 2024/25, 25268, nr. 242.

In de beleidsreactie op het rapport 'Bescherming gegeven? Evaluatie UAVG, meldplicht datalekken en de boetebevoegdheid' is toegezegd om in overleg te treden met de AP over de verdere toepassing van gedragscodes en het belang daarvan onder de aandacht te brengen.²⁸ Deze gesprekken zijn nog gaande, waarbij onder meer ook specifiek wordt ingegaan op de mogelijkheden van certificering en de inzet van sectorale toezichtsorganen.

De Staatssecretaris van Justitie en Veiligheid,

mr. A.C.L. Rutte

²⁸ *Kamerstukken II 2022/23*, 32761 nr. 284, p. 4.