Nadere memorie van antwoord naar aanleiding van het tweede nader verslag bij de algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid, 34 972)

1. Inleiding

De leden van de fracties van **GroenLinks** en **PvdA** danken de regering voor de uitvoerige beantwoording van de vragen van de commissie en van de vragen die zij samen met de fracties van de ChristenUnie hadden ingediend. Zij hebben nog enkele aanvullende vragen en constateren dat thans, 22 juni 2021, de novelle aan de Tweede Kamer is aangeboden, die - wanneer deze de Eerste Kamer zou bereiken - wellicht eveneens tot nadere vragen zou kunnen leiden die in het verlengde liggen van de nu te stellen vragen. De leden van de fracties van het **CDA** en de **ChristenUnie** sluiten zich bij deze vragen aan.

De leden van de fractie van de **PVV** hebben kennisgenomen van de antwoorden van de regering en hebben nog een enkele vervolgvragen.

Graag bedank ik de fracties voor hun bijdrage en ga ik in op de gestelde vragen. Bij de beantwoording zijn de indeling en volgorde van het verslag aangehouden.

2. Open source

De leden hebben een aantal vragen gesteld ten aanzien van open source. De leden hebben vragen over het feit dat open source niet als toelatingseis is opgenomen in het wetsvoorstel, maar als wegingsprincipe[1]. De leden van de fracties van GroenLinks en PvdA hebben mij gevraagd om aan te geven wat voor deze 'weging' de precieze criteria zijn. De leden refereren voorts aan het feit dat meer open source het doel is als belangrijk middel om transparantie en veiligheid te borgen en dat dit doel via een 'transitieproces' moet worden bereikt. De leden vragen naar een termijn waarbinnen deze transitie moet zijn bereikt. In het verlengde daarvan vroegen de leden naar het feit dat in de memorie van antwoord is aangegeven dat open source als harde eis stellen weliswaar is onderzocht, maar 'door de stap te snel te maken de continuïteit van het gebruik van inlogmiddelen in gevaar kan komen'.[2]

Ik dank de leden voor de vragen. De genoemde vragen zal ik zoveel mogelijk in samenhang beantwoorden, waarbij ik de beantwoording wil benutten om mijn overkoepelende beeld ten aanzien van open source toe te lichten.

Laat er geen misverstand over bestaan: open source is de weg die we opgaan. Ik vind het van belang om dat hier nog eens te onderstrepen. De precieze criteria voor de weging van inzet van open source worden, tezamen met de overige criteria die worden gesteld, op dit moment nader uitgewerkt in uitvoeringsregelgeving en zullen later dit jaar in consultatie worden gebracht. Ik kan daarom de precieze criteria nog niet delen, maar gedacht kan worden aan de mate waarin bepaalde functionaliteit open source beschikbaar is en of de open source functionaliteit veilig kan worden ingezet. Bij de criteria is de veiligheid die kan worden geborgd in de samenwerking met andere hard- en (systeem) software onderdelen van het middel, de onderhoudbaarheid ervan, maar ook de vraag of de ontwikkelgemeenschap die de open source software draagt voldoende ontwikkeld is, van belang. Dergelijke criteria, alsook de wijze waarop deze kunnen worden geobjectiveerd en daardoor toetsbaar gemaakt kunnen worden, worden in de komende tijd uitgewerkt. Voor dit moment zal ik de wegingsbelangen nader toelichten. Zoals ik aangaf maken we de beweging naar open source vanwege de

[1] *Kamerstukken I* 2020/21, 34972, P, p. 2.

[2] *Kamerstukken I* 2020/21, 34972, P, p. 4.

transparantie, veiligheid en innovatieruimte die open source biedt. Deze belangen bepalen het doel. Daarnaast moeten we ervoor zorgen dat de continuïteit van middelen waarvan veel burgers en bedrijven vandaag de dag nog afhankelijk zijn geborgd is en blijft. Dit betekent overigens niet dat deze middelen closed source zullen blijven. Ook deze middelen zullen de stap naar meer open source moeten gaan maken. Maar wel op een zodanige wijze dat dat beheerst kan plaatsvinden en burgers en bedrijven gewoon veilig en vertrouwd toegang blijven houden tot overheidsdienstverlening.

Ik begrijp de vraag van de leden om een termijn te noemen. Laat ik vooropstellen dat de termijn wat mij betreft – gelet op het doel - zo kort mogelijk is. Maar wel zo lang als nodig is om verantwoord over te gaan op open source, gelet op de continuïteit van de huidige middelen. Want daar zijn de komende periode miljoenen burgers en bedrijven afhankelijk van voor hun contact met de overheid. De snelheid waarmee het kan, hangt van vele factoren af. Zo is bepalend of specifieke functionaliteit onder open source licentie beschikbaar is. Van belang daarbij is of de sterkte van de open source gemeenschappen die de softwarecomponenten ondersteunen voldoende krachtig is. Dit laatste is randvoorwaardelijk om de voordelen van open source ook te kunnen benutten. Daarnaast is het zo dat de inzet of keuze voor open source of closed source niet alleen een "licentiekeuze" inhoudt, maar ook bepalend is voor de achterliggende organisatie en het bedrijfsmodel. Daarbij doel ik niet zozeer op verdienmodellen van (closed source) software - die zullen de richting die we inslaan moeten volgen en moeten zich aanpassen - maar vooral op de wijze waarop de softwareontwikkeling wordt gedaan en het "veiligheidsmodel" is vormgegeven. Dat vergt van leveranciers waarschijnlijk ook organisatieveranderingen, waaronder ook de ondersteuning van communities die de open source software ontwikkelen, onderhouden, doorontwikkelen en die in geval van acute problemen met de software incidentgericht en snel kunnen handelen.

Zoals meer aspecten van digitalisering is daarom ook deze ontwikkeling er een van kleine stapjes, met concrete resultaten. Open source is het doel, waarbij geldt dat de winkel veilig moet openblijven terwijl de verbouwing plaatsvindt. Daarbij geldt ook dat we uiteraard zo snel zullen gaan als het kan, maar wel zo zorgvuldig als het moet, gelet op de belangen van burgers en bedrijven.

De leden vragen de regering tevens om aan te geven om welke (bestaande) inlogmiddelen het hier gaat, en of DigiD daartoe behoort. Indien het uitsluitend om inlogmiddelen van de (rijks)overheid gaat, ligt het dan niet voor de hand om open source voor marktpartijen als toegangsvereiste in de wet op te nemen en voor de bestaande inlogmiddelen, van de (rijks)overheid, vooralsnog en onder voorwaarden een uitzondering te maken?

Tot de middelen waarvan de continuïteit geborgd moet blijven behoort inderdaad ook DigiD. Maar ook inlogmiddelen die niet van de Rijksoverheid zijn, waaronder de eHerkenningsmiddelen die op dit moment privaat worden aangeboden. De verwachting op basis van eerdere marktconsultaties is dat onder de aspirant aanbieders van andere middelen ook (deels) closed source gebruikt wordt. Ik benadruk overigens dat reeds op dit moment (aanzienlijke) delen van de gebruikte software van deze inlogmiddelen bestaat uit open source. Ook voor DigiD is dat zo. Kortom: ik verwacht dat het niet nodig is om een onderscheid of uitzondering te maken voor middelen van de Rijksoverheid, en deze op gelijke wijze naar open source toe te laten groeien.

Ten slotte hebben de leden van de GroenLinks- en PvdA-fracties gevraagd of de mogelijkheid dat nieuwe aanbieders van inlogmiddelen (tijdelijk) werken met closed source niet het risico meebrengt dat dat doel juist verder uit het zicht raakt?

In het kader van een gelijk speelveld om meer diversiteit aan (innovatieve) middelen mogelijk te maken, gelden voor nieuwe aanbieders dezelfde voorwaarden om middelen aan te bieden als voor bestaande aanbieders. Het klopt in die zin dat nieuwe aanbieders, op het moment dat zij op de korte termijn een bestaande oplossing willen aanbieden, dat kunnen doen met gebruikmaking van closed source, zolang de veiligheid en betrouwbaarheid van de middelen op toelatingsregels op basis van de eIDAS-verordening en de AVG geborgd zijn. Echter voor hen gelden ook de regels om – naarmate meer functionaliteit onder

open source beschikbaar komt, zij de stap naar open source zullen moeten maken. Doordat ook zij daarbij de ruimte krijgen om dat beheerst te doen, is de verwachting dat de inspanningen juist gericht zullen worden op het meer open source maken van hun oplossingen, in plaats van dat de energie gaat zitten in het opstellen van argumentatie waarom open source niet mogelijk zou zijn. Partijen krijgen zo de mogelijkheid om veilig en verantwoord over te gaan op open source. Door ook nieuwe partijen op deze wijze toe te laten is het ook beter mogelijk om breder te sturen op deze ontwikkeling.

3. Inlogmiddelen

De leden van de fracties van GroenLinks en PvdA vragen of, als de Wet digitale overheid zou zijn ingevoerd volgens de in het wetsvoorstel en de novelle opgenomen voorstellen, de situatie zou kunnen ontstaan dat verschillende partijen zijn toegelaten, waarvan sommige met open source middelen en andere niet?

In reactie op de vragen van de fracties van GroenLinks en PvdA merk ik op dat het uitgangspunt is dat alle inlogmiddelen die onder de Wdo toegelaten worden, voldoen aan de toelatingseisen die ik onder de Wdo aan identificatiemiddelen stel. Deze eisen vloeien, zoals ik u al eerder informeerde, voort uit de eIDAS-verordening, de AVG en nationale privacyregels. Partijen die hun inlogmiddelen willen laten erkennen dienen zich in te spannen om open source software te gebruiken. Dit betekent dat in het concrete geval wordt bezien waar redelijkerwijs gebruik kan en moet worden gemaakt van open source software. Ik hanteer hierbij een groeimodel. Open source is het uitgangspunt zonder dat in de praktijk veiligheids- en continuïteitsproblemen optreden. Dit leidt ertoe, dat enerzijds door mij geen excessieve maatregelen worden geëist met disproportionele kosten of disproportionele aanpassingen in het productieproces. Anderzijds wordt van een aanvragende partij verwacht dat deze alle redelijke maatregelen treft teneinde open source zoveel mogelijk te hanteren, gelet op wat in de tijd aan open source beschikbaar is. Het enkele feit, dat het gebruik van open source meerkosten voor de aanbieder met zich brengt, is daarbij niet doorslaggevend.
Ook wanneer een closed source oplossing veiliger is dan op grond van de vereisten voor erkenning nodig is, zal dit er niet automatisch toe leiden dat closed source wordt toegestaan en kan een dergelijke aanvraag toch afgewezen worden.
Dus ja, in de praktijk is het mogelijk dat sommige partijen open source gebruiken en andere nog niet.

De leden vragen voorts of in een dergelijke situatie overheden de inlog bij hen mogen beperken tot open source middelen. Verschillende gemeenten hebben immers eigen visies en strategieën op het gebied van IT-transparantie jegens hun burgers, zo stellen de leden. Zij vragen of er ruimte is voor (decentrale) overheden om uitsluitend partijen met open sources-inlogmiddelen of met uitsluitend decentrale opslag toe te laten? Ten slotte vragen de leden of deze overheden ook ruimte hebben om de kosten van inlogmiddelen voor burgers (sommige zijn gratis, andere kosten een bepaald bedrag per login) mee te laten wegen bij de keuze voor een bepaald inlogmiddel?

In reactie op de vragen van de fracties van GroenLinks en PvdA merk ik op dat op grond van de artikelen 7 en 15 van het wetsvoorstel overheden voor diensten die onder de reikwijdte van de Wdo vallen, een acceptatieplicht hebben met betrekking tot alle toegelaten inlogmiddelen. Overheden mogen daarom voor deze diensten in geen geval de toegang beperken tot slechts één of enkele toegelaten identificatiemiddelen. Dit is belangrijk omdat burgers en bedrijven erop moeten kunnen vertrouwen dat zij die middelen overal binnen de overheid kunnen gebruiken. De burger bepaalt immers zelf welk van de toegelaten middelen hij – overheidsbreed - gebruikt en kan en mag niet voor een dichte deur komen te staan.

De leden vragen wat dit dan betekent voor de autonomie van die decentrale overheden als zij die ruimte niet hebben.

In reactie op de vraag van de fracties van GroenLinks en PvdA merk ik op dat de autonomie van decentrale overheden inhoudt dat provincies en gemeenten vrij zijn om alle taken inzake hun huishouding ter hand te nemen, mits zij daardoor niet in strijd handelen met wettelijke voorschriften. Nu de acceptatieplicht met betrekking tot alle toegelaten identificatiemiddelen bij wet wordt geregeld, is er wat dit betreft geen sprake van de mogelijkheid tot eigen invulling door decentrale overheden. Zoals hierboven opgenomen is dit om te zorgen dat een burger niet onverwacht voor een dichte digitale deur komt te staan.

4. BSN

De leden van de fracties van GroenLinks en PvdA merken op dat op verschillende plaatsen in de nadere memorie van antwoord wordt benadrukt dat, om de privacy zoveel mogelijk te bevorderen, bij een centrale login enkel wordt gewerkt met het Burger Service Nummer (BSN) dat versleuteld wordt verstuurd en opgeslagen.[3] De leden hebben gevraagd of in die situatie de burger in deze situatie dan nog wel zelf kan zien met welk nummer er ingelogd wordt? In aanvulling daarop hebben zij de vraag gesteld in hoeverre de regering dit problematisch acht. Ten slotte vroegen de leden of het vereiste van het versleuteld aanleveren van het BSN ook voor decentrale middelen geldt, waar, zo stellen de leden geen risico voor schending van de privacy bestaat.

In de nadere memorie van antwoord heb ik aangegeven dat in het kader van privacybescherming de versleuteling van persoonsgegevens mogelijk wordt gemaakt. Dit is een passende en proportionele maatregel die, tezamen met andere maatregelen in het kader van de AVG, voor een adequaat niveau van bescherming van persoonsgegevens moet zorgen. In het bijzonder worden risico's ten aanzien van onbedoelde verwerking van het BSN voorkomen. Daarnaast is het zo dat, waar verwerking van persoonsgegevens plaatsvindt, er risico's spelen voor de bescherming van privacy. Dat staat los van de situatie waar en hoe persoonsgegevens, decentraal of centraal, worden opgeslagen. Het treffen van versleutelingsmaatregelen is in alle gevallen verstandig.

Met de leden vind ik het van groot belang dat de burger zelf kan controleren of hij/zij met de juiste gegevens is ingelogd dan wel de juiste gegevens heeft verstrekt. Met de gekozen systematiek/methodiek van versleuteling kan dat ook. De versleutelingmethode zorgt ervoor dat de tussenliggende schakels in de authenticatieketen, het BSN niet kunnen lezen. Het BSN is versleuteld en de tussenschakels beschikken niet over de sleutel. Slechts de dienstverlener waarbij wordt ingelogd kan, met diens eigen specifieke sleutel het BSN ontsleutelen. De burger kan nadat hij is ingelogd zijn gegevens controleren.

Extra waarborg is dat bij de verstrekking van de specifieke sleutels ook wordt gecontroleerd of een organisatie over het BSN mag beschikken. Zo wordt voorkomen dat het BSN wordt verstrekt aan organisaties die daarover niet mogen beschikken. Dit is in feite een doelbindingscheck vooraf. Deze methodiek is voor verschillende oplossingen, ook de als 'decentraal' gekenschetste oplossingen, van toegevoegde waarde omdat ermee wordt bereikt dat het BSN als (leesbaar) attribuut niet behoeft te worden opgeslagen, ook niet decentraal. Dit voorkomt dat, mocht een decentrale oplossing op de telefoon van een gebruiker gehackt worden, het BSN niet wordt prijsgegeven. Ook voor decentrale oplossingen zou de versleutelingsmethode daarom een goede oplossing zijn. Niet alleen omdat het BSN dan niet op het apparaat van de gebruiker hoeft te worden opgeslagen, maar ook omdat het voorkomt dat organisaties het BSN krijgen die daartoe niet gerechtigd zijn.

5. Veiligheid en betrouwbaarheid

[3] *Kamerstukken I* 2020/21, 34972, P, p. 5 e.v.

De leden merken op dat op pagina 6 van de nadere memorie van antwoord de regering over toetsing aan de wettelijke veiligheids- en betrouwbaarheidseisen schrijft: 'Op conformiteit met deze eisen wordt door mij voorafgaand aan de toelating (erkenning) getoetst, alsmede gedurende de dienstverlening; toezicht ter zake wordt opgedragen aan het Agentschap Telecom.'[4] Er is dus sprake van toetsing en controle door de overheid'. Op pagina 9 staat, zo citeren de leden: 'Toezicht is extern belegd en betreft de naleving van de toelatingseisen door partijen die inlogmiddelen aanbieden; dit wordt uitgeoefend door het Agentschap Telecom.'.[5] De leden vragen de regering nog eens precies uiteen te zetten wat de te onderscheiden rollen bij toetsing zijn van de regering en van het Agentschap Telecom. Daarbij vragen zij hoe de ministeriële verantwoordelijkheid is geregeld voor (de toetsing door) het Agentschap Telecom?

Op grond van het wetsvoorstel mag een publieke dienstverlener slechts middelen accepteren die door de minister van BZK zijn aangewezen (publieke middelen) of erkend (private middelen). Voorafgaand aan een aanwijzing of erkenning vindt toetsing plaats. De minister van BZK is bij wet bevoegd voor die toetsing.
De bevoegdheid om de beslissing over erkenning of aanwijzing te nemen, zal door Agentschap Telecom in mandaat uitgeoefend worden, namens de Minister BZK. De Minister BZK is beleidsverantwoordelijk voor een aanwijzings- of erkenningsbesluit dat in mandaat is genomen. Partijen die zijn aangewezen of erkend moeten zich daarna blijven houden aan de wettelijke regels. Daarop vindt toezicht plaats. Dat toezicht is, met artikel 17, vijfde lid, van het wetsvoorstel, rechtstreeks belegd bij het Agentschap Telecom.
Agentschap Telecom is een rijksinspectie zoals bedoeld in de Regeling vaststelling Aanwijzing inzake de rijksinspecties. Deze regeling bevat aanwijzingen die betrekking hebben op de uitoefening van toezichtstaken door rijksinspecties en geeft waarborgen voor het onpartijdig en onafhankelijk functioneren van rijksinspecties binnen de ministeriële verantwoordelijkheid. Deze aanwijzingen regelen verder dat de beleidsinhoudelijk verantwoordelijke minister algemene en bijzondere aanwijzingen kan geven aan de inspectie. Zowel het toezicht als de toelating vinden dus plaats binnen de ministeriële verantwoordelijkheid van de minister van BZK.

De leden halen pagina 10 van de nadere memorie van antwoord aan, waarin is geschreven: 'Als private aanbieders, naast middelen die door mij erkend worden om te gebruiken bij de overheid, ook middelen willen aanbieden voor commercieel gebruik (dus: buiten de overheid) staat hen dat vrij'.[6] Wat betekent hier 'naast', zo vragen de leden van de GroenLinks- en PvdA-fracties.

In reactie op de vragen van de fracties van GroenLinks en PvdA merk ik op dat het private aanbieders vrij staat om inlogmiddelen aan te bieden op de markt. Echter, aan het gebruik van inlogmiddelen bij overheidsdiensten, stel ik, zoals gezegd toelatingseisen. Private aanbieders kunnen indien gewenst een aanvraag indienen voor het gebruik van hun inlogmiddelen bij de overheid. Als aan de toelatingseisen wordt voldaan, wordt het inlogmiddel toegelaten en kan het inlogmiddel gebruikt worden voor inloggen bij de overheid. Dit inlogmiddel kan ook buiten de overheid gebruikt worden. Aan het gebruik van inlogmiddelen buiten de overheid stel ik met dit wetsvoorstel geen eisen en hiervoor is toelating niet vereist. Als private partijen ervoor kiezen om hun inlogmiddel niet aan te bieden voor gebruik bij de overheid, belet dit wetsvoorstel hen niet om hun inlogmiddel aan te bieden voor enkel commercieel gebruik, buiten de overheid. Dit valt buiten de reikwijdte van het wetsvoorstel.

Mogen die private aanbieders dezelfde middelen die erkend zijn door de minister niet ook commercieel aanbieden, of juist wel? Kan een aanbieder van een toegelaten middel datzelfde middel ook aan burgers aanbieden voor inloggen in het private domein?

Zoals al geantwoord op de vorige vraag van de fracties van GroenLinks en PvdA kunnen middelen van dezelfde aanbieder ook gebruikt worden in het private domein.

[4] *Kamerstukken I* 2020/21, 34972, P, p. 6.
[5] *Kamerstukken I* 2020/21, 34972, P, p. 9.
[6] *Kamerstukken I* 2020/21, 34972, P, p. 10.

De leden vragen, indien dat laatste het geval is, wat dan de consequentie is als de minister de toelating van het middel schorst of intrekt?

In reactie op deze vraag van de fracties van GroenLinks en PvdA merk ik op dat de eventuele schorsing of intrekking van een toegelaten inlogmiddel enkel consequenties heeft voor het inloggen bij de overheid. Dit kan dan (tijdelijk) niet meer. Het inlogmiddel kan dan wel gebruikt blijven worden buiten de overheid, dus in het private domein. Het private of commerciële domein valt immers buiten de reikwijdte van het wetsvoorstel.

De leden van de PVV-fractie vragen de regering in hoeverre er plannen of intenties zijn om het in dit wetsvoorstel (en in de novelle) bedoelde identificatiemiddel ook te (kunnen) benutten voor coronamaatregelen, zoals het vaccinatiepaspoort en testen voor toegang?

In antwoord op de vraag van de PVV-fractie merk ik op dat toegelaten/erkende middelen gebruikt kunnen worden bij alle diensten die door de overheid worden aangeboden. Dus ook voor de genoemde voorbeelden.

Indien er sprake is van dergelijke plannen of intenties, kan de regering, zo vragen de leden, specifiek aangeven op welke wijze de veiligheid van medische gegevens gewaarborgd wordt en in hoeverre er een (digitale) koppeling met patiëntengegevens (waaronder het elektronisch patiëntendossier) plaatsvindt?

In reactie op de vraag van de fractie van de PVV, merk ik namens het ministerie van VWS op dat tot inwerkingtreding van de Wet digitale overheid de rechten en plichten uit deze wet nog niet worden toegepast op de huidige maatregelen ter bestrijding van de pandemie. Denk aan maatregelen zoals nu genomen worden onder meer op grond van de tijdelijke wet coronatoegangsbewijzen. De Europese verordening met betrekking tot het digitaal EU-COVID-certificaat zal t/m 30 juni 2022 van kracht zijn. Bij inwerkingtreding van de Wet digitale overheid zal worden bezien in hoeverre in dat kader nog maatregelen van kracht zullen zijn, waarop deze wet van toepassing wordt. Overigens is Coronacheck ontworpen conform de beginselen van privacy en security by design en worden de persoonsgegevens van de gebruikers van de app goed beschermd.

In het algemeen kan gesteld worden dat bij inwerkingtreding van de Wet digitale overheid de erkende inlogmiddelen dienen te worden gebruikt bij elektronische dienstverlening vanuit bestuursorganen of aangewezen organisaties (waaronder ook zorgaanbieders) bij alle diensten die door de overheid worden aangeboden. Voor toegang tot medische gegevens zal authenticatie op betrouwbaarheidsniveau hoog vereist worden.

6. Europese Digitale Identiteit

Op 2 juni 2021 ontving de Eerste Kamer de nadere memorie van antwoord. Daarin lazen de leden van de fracties van GroenLinks en PvdA op pagina 18 dat naar verwachting van de regering er geen Europese eID wordt geïntroduceerd.[7] Op 3 juni 2021 publiceerde de Europese Commissie een 'framework' voor een Europese Digitale Identiteit.[8] De leden vragen of deze aankondiging van de Europese Commissie voor de regering onverwacht kwam? Voorts vragen de leden om aan te geven hoe voorliggend wetsvoorstel en de volgende tranches van de Wdo zich (juridisch, qua gehanteerde technieken en voor wat betreft de planning in de tijd) verhouden tot dit 'framework' van de Europese Commissie.

[7] *Kamerstukken I* 2020/21, 34972, P, p. 18.
[8] *Commission proposes a trusted and secure Digital Identity (europa.eu)*

In reactie op de vragen van GroenLinks en de PvdA wordt opgemerkt dat het voorstel van de Europese Commissie voor een verordening betreffende de invoering van een raamwerk voor een Europese Digitale Identiteit voor de regering niet onverwacht kwam. Met deze (wijzigings)verordening wordt niet een enkele Europese eID geïntroduceerd, maar worden eisen gesteld aan door/in de lidstaten uitgegeven wallets, waardoor een geharmoniseerd regime wordt gerealiseerd. Met het voorliggende wetsvoorstel, de eerste tranche WDO, wordt reeds voor een belangrijk deel aan genoemde – toekomstige – EU-verordening voldaan. Beoogd wordt om in de tweede tranche WDO het onderwerp regie op gegevens/digitale identiteit te regelen, zoals ook aan Uw kamer gemeld in de memorie van antwoord. Hierover vindt de gedachtenvorming momenteel plaats; deze komt in belangrijke mate overeen met het onderwerp van de (wijzigings)verordening. De voorbereiding van de (wijzigings)verordening en de voorbereiding van de tweede tranche WDO zullen deels parallel plaatsvinden. Dit zorgt voor een nuttige wisselwerking, waarbij er rekening mee moet worden gehouden dat inhoud, reikwijdte en accenten van de (wijzigings)verordening niet volledig zullen stroken met nationale beleidswensen. Ook zal de (wijzigings)verordening gevolgen hebben voor de inhoud en systematiek van de WDO, omdat de materiele normen in rechtstreeks werkende Europese regels zullen zijn vervat; deze mogen niet worden 'overgeschreven' in nationale regels. Wel zal de WDO moeten voorzien in bijvoorbeeld de aanwijzing van met de uitvoering belaste instanties, sanctionering en rechtsbescherming. De verdere voorbereiding van de (wijzigings)verordening zal de komende maanden plaatshebben; na vaststelling volgt een implementatietermijn – de lengte daarvan is onderwerp van onderhandeling - waarbinnen de lidstaten hun regelgeving moeten aanpassen. Het BNC-fiche terzake, waarin wordt ingegaan op de inhoudelijke aspecten, relatie tot nationale regelgeving en onderhandelingsinzet van de regering, is u medio juli toegezonden. Kortom: de WDO is nodig om de (wijzigings)verordening te kunnen uitvoeren. Dit zal op termijn wel de nodige aanpassingen met zich mee brengen. Op deze wijze realiseer ik de stapsgewijze invoering van een stelsel waarmee veilig en betrouwbaar inloggen en het delen van gegevens wordt gerealiseerd.

7. Novelle

Tot slot hebben de leden enkele vragen gesteld over de procedure van de novelle. In antwoord op vragen van het CDA antwoordt de regering in de nadere memorie van antwoord dat de regering de voorkeur heeft om zo snel mogelijk het wetsvoorstel te behandelen, dat wil zeggen vóór behandeling van de novelle.[9] Als reden wordt genoemd dat instemming met het wetsvoorstel 'een grote mate van duidelijkheid en rechtszekerheid aan betrokkenen (zij weten dan waar zij aan toe zijn) [verschaft], waardoor met de voorbereiding van de uitvoering kan worden gestart'.[10] Op pagina 20 en 21 wordt evenwel opgemerkt dat omdat het wetsvoorstel (anders dan de novelle) al enige tijd bekend is en voor een ieder kenbaar en beschikbaar, 'stakeholders (burgers, publieke dienstverleners, private partijen, toezichthouders) geruime tijd in de gelegenheid zijn zich op het nieuwe stelsel voor te bereiden.' Enerzijds dus reeds ruim voldoende tijd voor voorbereiding; anderzijds moet het wetsvoorstel zo snel mogelijk door de Eerste Kamer worden behandeld om genoeg tijd voor voorbereiding te hebben. De leden stellen een discrepantie in de antwoorden en vragen deze te verklaren.

In reactie op de vragen van GroenLinks en de PvdA wordt opgemerkt dat geen sprake is van discrepantie. Het wetsvoorstel is al enige tijd bekend, waardoor ruim gelegenheid was voor voorbereiding. Echter, tegelijkertijd is het wetsvoorstel nog onderwerp van parlementaire beraadslaging, waardoor belanghebbenden in onzekerheid verkeren omtrent de daadwerkelijke inhoud en datum van invoering. Duidelijkheid is voor hen van groot belang met het oog op de uitvoering, benodigde investeringen en capaciteit.

[9] *Kamerstukken I* 2020/21, 34972, P, p. 8.
[10] *Kamerstukken I* 2020/21, 34972, P, p. 8.

Meer principieel en daarmee van groter belang is de vraag van de leden van de GroenLinks- en PvdA-fracties, of het staatsrechtelijk zuiver en wenselijk is de Eerste Kamer te vragen in te stemmen met de tekst van een wetsvoorstel, terwijl die op verschillende fundamentele punten via een novelle zal worden aangepast. De leden vragen hierop te reageren.

In reactie op de vragen van GroenLinks en de PvdA wordt opgemerkt dat het staatsrechtelijk mogelijk is om als Eerste Kamer in te stemmen met de tekst van een wetsvoorstel, terwijl die via een novelle zal worden aangepast. Veelal wordt in de Eerste Kamer de behandeling van het wetsvoorstel aangehouden, in afwachting van de novelle. Beide voorstellen worden vervolgens gezamenlijk afgehandeld. Echter, het is mogelijk dat het wetsvoorstel wordt aangenomen, maar nog niet van kracht wordt voordat ook de novelle door beide Kamers is aangenomen. De website van uw Kamer gaat hier specifiek op in en stelt dat de Eerste Kamer eventueel ook het te wijzigen wetsvoorstel kan aanvaarden met de toezegging dat aanpassing (later) door middel van een novelle zal plaatsvinden. Zoals bij de vorige vraag aangegeven, is dat wat in het onderhavige geval mijn voorkeur verdient. In dit verband heb ik niet alleen een toezegging gedaan, maar heb ik deze ook daadwerkelijk vervolg gegeven door een novelle in te dienen; deze is voor uw Kamer kenbaar (Kamerstukken 2021-2021, 35 868).

8. Paspoortwet

Kan de regering aangeven of, en in hoeverre, de uitvoering van dit wetsvoorstel (en de novelle) samenhangt met het wetsvoorstel Wijziging van de Paspoortwet in verband met de uitvoering van de Verordening identiteitskaarten, zo vragen de leden van de PVV-fractie?[11]

In reactie op de vraag van de leden van de PVV-fractie wordt opgemerkt dat beide wetstrajecten niet met elkaar samenhangen. De genoemde wijziging van de Paspoortwet, die inmiddels door uw Kamer is aanvaard, betreft de opname van vingerafdrukken op de identiteitskaart ten behoeve van verificatie van de identiteit van een persoon en houdt geen verband met de functie van de identiteitskaart als publiek identificatiemiddel in digitale contacten tussen de burger en de overheid, hetgeen het onderwerp is van het onderhavige wetsvoorstel.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

R.W. Knops

[11] *Kamerstukken II* 2019/20, 35 552 (R2148), 1.