Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

35 868 Wijziging van het voorstel van wet houdende algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid)

Nr. 6

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 30 november 2021

INLEIDING

Met interesse heb ik kennisgenomen van de opmerkingen over en de vragen bij deze novelle bij het wetsvoorstel digitale overheid. Het is het streven van de regering om met de Wet digitale overheid een degelijk en adequaat kader neer te zetten om toekomstige ontwikkelingen op het terrein van de digitale overheid steeds te voorzien van de nodige wettelijke waarborgen en op passende wijze vorm te geven. Omwille van de leesbaarheid heb ik de beantwoording van de vragen van de fracties thematisch geordend.
Ik vertrouw erop dat mijn reactie op deze vragen voor Uw Kamer aanleiding zal betekenen het voorstel voortvarend te behandelen.

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel wijziging van het voorstel van wet houdende algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur. Het betreft hier een zogenaamde novelle. Graag willen deze leden de regering een aantal vragen stellen.

De leden van de D66-fractie hebben kennisgenomen van de wijziging van het voorstel Wet digitale overheid. Voor deze leden zijn basisprincipes van privacy by design, open source en het verhandelverbod belangrijke kernpunten voor een goed functionerende digitale overheid, echter hebben de aan het woord zijnde leden nog enkele vragen.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van onderhavig wetsvoorstel. Deze leden menen dat een voortvarende behandeling van belang is.

De leden van de SP-fractie hebben kennisgenomen van de wijziging van de Wet digitale overheid en hebben hierover nog verscheidende vragen en opmerkingen.

kst-35868-6
ISSN 0921 - 7371
's-Gravenhage 2021

De leden van de GroenLinks-fractie hebben kennisgenomen van de wijziging van het voorstel van wet houdende algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid). De leden hebben nog enkele vragen.

De leden van de Volt-fractie hebben met belangstelling kennisgenomen van het gewijzigde wetsvoorstel. Zij hebben hierover nog enkele vragen.

Het lid van de BBB-fractie heeft kennisgenomen van het voorliggende wetsvoorstel.

Algemeen

De leden van de VVD-fractie hebben gevraagd of, als het gaat om privacy by design, verhandelverbod en open source, in het onderhavige wetsvoorstel iets anders geregeld wordt dan in het wetsvoorstel dat in de Tweede Kamer is aanvaard en nu in de Eerste Kamer ligt of dat alleen voorgesteld wordt om deze punten bij wet te regelen in plaats van bij algemene maatregel van bestuur.

Inderdaad is het grote verschil met het oorspronkelijke wetsvoorstel dat de novelle voorziet in een sterkere verankering in de wet zelf van de door de leden van de fractie van de VVD genoemde punten. De uitwerking van deze onderwerpen vindt plaats in algemene maatregelen van bestuur en ministeriële regelingen die op het wetsvoorstel worden gebaseerd. De novelle zorgt voor een versteviging van de opensource-eis in de wet zelf. Het kader is op het niveau van de wet bepaald, waarmee de wijze waarop daar inhoudelijk mee wordt omgegaan, zoals gedeeld met uw Kamer, bij algemene maatregel van bestuur vorm kan krijgen.

Uitvoeringstoetsen

Daarnaast vroegen deze leden de regering inzicht te geven in de uitvoeringstoetsen. Welke uitvoeringstoetsen met betrekking tot de Wet digitale overheid zijn tot op heden gedaan? Zij vroegen wat de uitkomsten daarvan waren en wat de betrokkenheid van de Vereniging van Nederlandse Gemeenten (VNG) is geweest.

Om te beginnen hecht ik eraan te benadrukken dat uitvoeringstoetsing een proces is, en niet een invulformulier of momentopname. Ik heb daarom het voorbereidingsproces multidisciplinair ingericht, door wetgevers, beleid, uitvoerders en (ICT-)technici vroegtijdig en doorlopend te betrekken. De Wdo (incl. lagere regelgeving Wdo) is vanaf het begin zo vormgegeven dat alle betrokken departementen, uitvoeringsorganisaties, VNG, IPO, KvK etc. systematisch betrokken zijn bij de voorbereiding. Betrokkenheid was er op alle niveaus: bij de te maken beleidskeuzes en de inrichting van het stelsel (governance) en bij het ontwerpen van wetteksten. Daardoor kon het voorontwerp van het wetsvoorstel, dat begin 2017 in consultatie was, op breed draagvlak rekenen. Het wetsvoorstel is, alvorens dit bij uw Kamer werd ingediend, op basis van deze verkregen input nog op enkele onderdelen aangepast om redenen van uitvoerbaarheid. Vanuit de uitvoerders is erop gehamerd dat aansluiting op het stelsel eenvoudig moet zijn. Ik verwijs hiervoor naar paragraaf 11.1 van de memorie van toelichting.

Naast deze doorlopende betrokkenheid zijn ook meer formele afstemmomenten geweest. Zo zijn in het kader van de consultatie van het wetsvoorstel in 2017 en 2018 uitvoeringstoetsen gedaan door publieke dienstverleners, al dan niet in koepelverband, en door private organi-

saties. De reacties op deze consultatie zijn gepubliceerd op internetconsultatie.nl (www.internetconsultatie.nl/wetgdi/details).

Ook is in verband met het amendement Middendorp/Verhoeven (34 972-20) een afzonderlijke uitvoeringstoets gedaan door uitvoeringsorganisaties gezamenlijk. De uitvoerbaarheid van dit amendement inzake online identiteit/regie op gegevens bleek op dat moment in de eerste tranche problematisch. Naar aanleiding daarvan is met uw Kamer afgesproken vooruitlopend op de uitvoering wel alvast het wetsvoorstel hierop aan te passen (artikel 5, eerste lid, van het wetsvoorstel aangepast en aangevuld (onderdeel g)) en om dit artikel bij de volgende tranche van de Wdo in werking te laten treden en nader te regelen (zie Kamerstukken 2019–2020, 34 972, nr. 20).

Recentelijk zijn door de VNG, de UvW en het IPO aanvullende uitvoeringstoetsen uitgevoerd naar de impact van de nu beschikbare uitvoeringsregelgeving onder het wetsvoorstel.

Tot slot heb ik u in de nadere memorie van antwoord van 2 juni 2021 geïnformeerd dat voor de novelle geen afzonderlijke consultatieronde is gehouden bij marktpartijen. Wel heb ik de huidige aanbieders van inlogmiddelen, waaronder DigiD, binnen het publieke domein gevraagd een uitvoeringstoets te doen ter borging van de continuïteit van het aanbieden van diensten. Daaruit bleek dat de novelle uitvoerbaar is.

Toekomstbestendige wetgeving voorzien van waarborgen

De fracties van CDA, SP, GroenLinks en D66 stellen vragen over de manier waarop de regering in de wet en de daarop berustende regelgeving keuzes maakt ten aanzien van regelingen in de wet zelf of in de algemene maatregelen van bestuur. Zij zoeken hierin naar een goede balans tussen toekomstgericht kunnen zijn en waarborgen bieden. De fracties begrijpen dat uitwerking in lagere regelgeving nodig kan zijn, maar zoeken naar die balans.

Met oog op de ontwikkelingen die nu eenmaal snel gaan in het domein van digitalisering is het belangrijk voor de overheid om slagvaardig te kunnen handelen om burgers en bedrijven steeds betrouwbare overheidsvoorzieningen, goede toegang tot de overheid en een goede bescherming van hun rechten te kunnen blijven bieden. Dat vraagt dat er een snellere wetgevingsprocedure kan worden gevolgd voor de uitwerking van onderwerpen die niet de hoofdlijnen van die toegang en bescherming betreffen en dat ook die procedure voorzien is van parlementaire betrokkenheid. Aanvankelijk werd in het wetsvoorstel ingezet op een zuivere kaderwet waarin veel naar het niveau van de algemene maatregel van bestuur en ministeriële regelingen werd gedelegeerd. Op basis van de inbreng uit uw Kamer zijn er al diverse aanpassingen gedaan in het wetvoorstel waardoor meer op wetsniveau wordt ingekaderd. Naar aanleiding van opmerkingen van de Eerste Kamer is dat nog verder uitgebreid in de voorliggende novelle.

Bij de novelle die nu in Uw Kamer voorligt, verwees de Raad van State naar opmerkingen die gemaakt zijn tijdens een deskundigenbijeenkomst in aanloop van de behandeling van het wetsvoorstel in de Eerste Kamer. Tijdens die deskundigenbijeenkomst werd overigens eveneens de opvatting naar voren gebracht dat bij dit type wetgeving delegatie alsmede betrokkenheid van het parlement (gecontroleerde delegatie) in de rede ligt.

De zorg van een aantal deskundigen bij die bijeenkomst hield met name verband met de onderwerpen privacybescherming en open source. Het wetsvoorstel is naar aanleiding van de deskundigenbijeenkomst en het voorlopig verslag van de Eerste Kamer juist op die punten door middel van de voorliggende novelle aangevuld, waardoor waarborgen voor privacy by design, open source en het verhandelverbod naar het niveau van de formele wet zijn getild. Verder is als gevolg van het verzoek daartoe van de Eerste Kamer voor alle relevante artikelen van de wet in de Memorie van Antwoord aangegeven hoe het wetsvoorstel zich verhoudt tot de uitgangspunten inzake delegatie van wetgeving.

Niet alleen heeft er ten opzichte van het oorspronkelijke voorstel inkadering plaatsgevonden, maar daarnaast zijn ook de mogelijkheden van Uw Kamer door middel van gecontroleerde delegatie invloed uit te oefenen op de nadere invulling van die wettelijke regeling, vergroot. Alle algemene maatregelen van bestuur onder het voorstel kennen een voorhangprocedure, waardoor het parlement hierbij nauw betrokken kan zijn.

De onderwerpen waarover de leden van CDA-, SP-, GroenLinks- en D66-fracties wat dat betreft duidelijkheid wensen, zijn de keuze tussen een wet en algemene maatregel van bestuur als meest geschikte niveau van wetgeving en de wenselijkheid van de keuze voor techniekonafhankelijke formuleringen.

De leden van de D66-fractie geven aan dat privacy by design, open source en het verhandelverbod wat hen betreft belangrijke kernpunten zijn voor een goed functionerende digitale overheid. Deze leden constateren dat de regering in de wijziging van het voorstel meerdere keren kiest voor een delegatiebepaling door middel van algemene maatregelen van bestuur. Als voorbeelden vragen deze leden specifiek naar een concrete transitietermijn of handvatten over het al dan niet in voldoende mate gebruik maken van open source.

Ook de leden van de GroenLinks-fractie vragen of de regering het niet wenselijk acht dat begrippen zoals «voldoende gebruik» van open source in het voorstel zelf worden opgenomen als heldere criteria.

Ik begrijp de wensen van de fracties om bij de behandeling van de wet inzicht te hebben in het geheel aan regelgeving en onderschrijf de wens om heldere criteria te hanteren in de wet. Echter, de in te zetten beweging naar gebruik van meer open source software vraagt steeds nauwkeurig afstemmen op de huidige stand van de beschikbaarheid ervan. Het begrip «voldoende gebruik» wordt uitgewerkt in een algemene maatregel van bestuur. Bij de beantwoording van de vragen over open source wordt nader ingegaan op hoe mij de invulling van het begrip «voldoende gebruik» voor ogen staat op een manier dat de regeling van voldoende waarborgen is voorzien.

Techniekonafhankelijk wetgeven

De leden van de D66-fractie erkennen dat flexibiliteit nodig kan zijn om wetgeving aan te laten sluiten bij snel veranderende digitale standaarden. Ze sluiten zich echter aan bij de opmerking van de Raad van State dat te abstracte wetten leiden tot onzekerheid over de gevolgen van de hoofdelementen van de desbetreffende wetten. Ook de leden van de SP-fractie vragen zich af of de wet niet wat meer substantie zou kunnen bevatten en vragen in te gaan op de keuze voor techniekonafhankelijke formuleringen. Zij vragen of de regering nader in kan gaan op de kritiek op dit punt van de Raad van State en halen het advies van de Raad van

State aan om begrippen als MijnOverheid en het BSN-Koppelregister in de wet zelf op te nemen. Ook de leden van de CDA-fractie stellen die vraag. De leden van de SP-fractie vragen zich af waarom de regering denkt dat er wel aan het advies is voldaan. Ook de leden van de GroenLinks-fractie halen de adviezen van de Raad van State aan over techniekonafhankelijk formuleren.
Zoals opgenomen in het nader rapport bij het oorspronkelijke wetsvoorstel deelt de regering de mening van de Afdeling dat te abstracte formulering afbreuk doet aan de duidelijkheid en rechtszekerheid. Om die reden bevat het wetsvoorstel de functionaliteiten van een aantal belangrijke voorzieningen (centrale onderdelen), waarbij concretisering, waaronder de begrippen, en uitwerking in algemene maatregelen van bestuur en ministeriële regelingen plaatsvindt. De grondslagen hiervoor worden in het wetsvoorstel ingekaderd en begrensd. Met deze systematiek wordt een zekere mate van toekomstbestendigheid en flexibiliteit bewerkstelligd.

De leden van de GroenLinks-fractie vragen in dit verband wat de verwachte omlooptijd is waarin dezelfde technieken worden gebruikt.

Juist omdat dit nooit op voorhand is te zeggen – innovatie laat zich niet sturen of plannen – is flexibiliteit nodig. Anders dan de leden van de GroenLinks-fractie noemen, wordt uitwerking van de voorzieningen niet overgelaten aan lagere overheden, maar wordt die op een lager niveau van regelgeving, te weten de algemene maatregel van bestuur, geregeld.

Die leden wijzen ook op de mogelijkheid om de regering tijdelijk de mogelijkheid te geven om op onderdelen van de wet af te wijken om ruimte te geven aan innovatie en vragen of de regering bij het standpunt blijft dat het onnodig is om in de wet de voorzieningen met een door de techniek ingegeven benaming aan te duiden.

De mogelijkheden omwille van de innovatie af te wijken van de wet ziet niet op de GDI- voorzieningen en dus niet op de onderwerpen die de Raad van State noemt in de discussie over het wel of niet noemen van de namen van de voorzieningen. Het noemen van begrippen als DigiD of MijnOverheid in de wet leidt niet tot een betere inkadering van de voorzieningen. Integendeel; door deze begrippen niet te benoemen moet in de wet zelf een beschrijving gegeven worden van welke functie deze voorzieningen hebben, hetgeen een grotere waarborg voor het in stand houden van een dergelijke functie garandeert.

Wdo in relatie tot de huidige eIDAS-verordening en de voorgenomen herziening

De leden van de D66-fractie horen graag van de regering welke gevolgen voorzien worden op de wijziging van het voorstel met de aankondiging van een herziening van de eIDAS-verordening door de Europese Commissie.

De herziening van de eIDAS-verordening raakt de novelle niet. De novelle stelt eisen aan inlogmiddelen die te zijner tijd – mocht de eIDAS-herziening in de huidige vorm van kracht worden – ook in die context gehanteerd kunnen worden.

De leden van de D66-fractie vragen ook of de regering problemen of oneerlijke concurrentie voorziet als er voor Nederlandse aanbieders andere eisen bestaan op het gebied van open source dan andere Europese aanbieders die toegang krijgen tot de Nederlandse markt.

De eIDAS-verordening stelt Europese lidstaten in de gelegenheid om een eigen stelsel in te richten voor toegang tot digitale overheidsdienstverlening. Daarbij kunnen lidstaten bepalen welke eisen zij hanteren voor eventuele private partijen die binnen hun stelsel diensten aanbieden. Het wetsvoorstel digitale overheid bevat de randvoorwaarden voor het Nederlandse stelsel, zoals de verplichting om open source software te gebruiken. Deze eisen zijn binnen de Nederlandse context gerechtvaardigd en noodzakelijk, in het geval van het gebruik van open source, omdat dit bijdraagt aan de transparante werking en de veiligheid van de desbetreffende middelen. Partijen die willen worden toegelaten tot het Nederlandse stelsel moeten aan die verplichtingen voldoen. Het is ook mogelijk om in Nederland inlogmiddelen te gebruiken die in andere EU-lidstaten zijn uitgegeven. Die mogelijkheid is in het leven geroepen om inwoners van andere EU-lidstaten in de gelegenheid te stellen om in de gehele EU toegang te krijgen met het inlogmiddel dat zij gebruiken voor toegang tot overheidsdienstverlening in de lidstaat waar zij wonen. Het gaat om inlogmiddelen die functioneren binnen de context van het stelsel van de desbetreffende EU-lidstaat en die, wanneer het een privaat middel betreft, daar zijn erkend. Andere EU-lidstaten worden verplicht om deze inlogmiddelen te accepteren wanneer deze voldoen aan minimumeisen die op grond van de eIDAS-verordening zijn vastgesteld. Binnen deze context verwacht ik dat middelen uit andere EU-lidstaten in hoofdzaak worden gebruikt door personen die reeds van dat middel gebruik maken om toegang te krijgen tot digitale dienstverlening in de lidstaat van herkomst. Het gebruik van deze middelen zal naar verwachting een uitzondering blijven, zoals ook nu het geval is, en deze worden voor gebruikers die primair toegang zoeken tot Nederlandse digitale dienstverlening geen concurrerend alternatief voor het aanvragen van een in Nederland toegelaten inlogmiddel.

De leden van de SP-fractie hebben nog verscheidene vragen en opmerkingen. Genoemde leden hebben al eerder tijdens de behandeling van dit wetsvoorstel hun kritiek geuit, met name op de verhouding tussen publieke en private middelen en de ernstige tekortkomingen in de wet omdat veel voorstellen niet voldoende waren uitgewerkt. Zij vinden het dan ook terecht dat de wet wordt aangepast, maar zien echter nog niet voldoende verbetering in de voorgestelde wijziging. Zij vragen naar de motivering om de wet niet verder uit te breiden met meer waarborgen rondom digitalisering. In een wet die de titel «Wet digitale overheid» draagt zou dat volgens genoemde leden passend zijn, zo besluiten de leden.

De regering is het met de leden eens dat er waarborgen moeten zijn rondom digitalisering van de overheid. Ik hecht eraan te benadrukken dat de Wdo die ook bevat. De nu voorliggende novelle bevat diverse extra waarborgen ten aanzien van de privacy: eisen die worden gesteld aan publieke en private inlogmiddelen. Het betreft extra eisen in aanvulling op eisen die in de Wdo, de eIDAS-verordening en de AVG al gelden. De waarborgen die de Wdo als geheel biedt reiken verder dan de waarborgen die de Wdo specifiek stelt ten aanzien van publieke en private inlogmiddelen. De Wdo regelt namelijk ook waarborgen voor overheidsvoorzieningen die nodig zijn voor de toegang tot de digitale overheid en (veiligheids)eisen aan overheidsorganisaties om te zorgen dat de aansluiting op de digitale overheid veilig is.

De Wdo biedt ook de mogelijkheid om standaarden te verplichten, bijvoorbeeld om interoperabiliteit te borgen, waardoor systemen van verschillende organisaties beter kunnen samenwerken. Maar ook om standaarden voor informatiebeveiliging te verplichten. Een voorbeeld hiervan is de mogelijkheid om e-mailstandaarden te verplichten ter voorkoming van ransomware-aanvallen. De Wdo dwingt daarnaast af dat

overheden de toegang tot hun dienstverlening op de hogere betrouwbaarheidsniveaus moeten ontsluiten. De wet biedt daarvoor een kader om de dienstverlening op een niveau in te schalen. Naast het feit dat dienstverlening daardoor over de volle breedte veiliger wordt, leidt het feit dat overheden dit kader gebruiken er ook toe dat gelijksoortige dienstverlening bij verschillende organisatie op hetzelfde betrouwbaarheidsniveau wordt ontsloten. Voor burgers biedt dit eenduidigheid in de toegang tot de digitale overheid.

De leden van de Volt-fractie vragen naar de noodzakelijkheid van de voorgestelde Wet digitale overheid. De leden geven aan dat de eIDAS-verordening zelfstandige regels bevat omtrent het aanbieden van (elektronische) authenticatiemiddelen bij overheidsinstellingen, en als EU-verordening rechtstreeks van toepassing is in de EU-lidstaten. De leden vragen daarom welke afwegingen gemaakt zijn ten aanzien van bepalingen in de voorliggende Wet digitale overheid tot al bestaande bepalingen in de eIDAS-verordening. De leden vragen hoe de regering de proportionaliteit en subsidiariteit in dit kader beoordeelt.

De leden van deze fractie vragen de regering voorts of en op welke manier zij kennis heeft genomen van hoe andere Europese lidstaten de toelating van private middelen als identificatiemiddelen (wettelijk) hebben geregeld en geïmplementeerd voor overheidsinstellingen. Voor zover de regering heeft gekozen voor een andere implementatiemethode dan andere Europese lidstaten, vragen de leden naar de onderbouwing daarvoor.

In algemene zin merk ik, ten opzichte van de noodzakelijkheid van de Wdo op, dat de Wdo meer zaken regelt dan de eIDAS-verordening. Dat geldt zowel voor de huidige als voor de herziene eIDAS-verordening, zoals het verplichten van standaarden, veiligheidseisen aan overheden én grondslagen en verantwoordelijkheden van de generieke digitale infrastructuur van de overheid. Dit biedt voor burgers bredere waarborgen. Deze noodzaak is er en staat los van de eIDAS-verordening. Daarnaast is het – ook in de herziene eIDAS-verordening – aan de lidstaten zelf om nadere regels te stellen aan het toelaten van inlogmiddelen, waarbij rekening kan worden gehouden met de nationale situatie, zoals voor Nederland bijvoorbeeld de regels ten aanzien van het BSN. Nationale lidstaten zijn en blijven verantwoordelijk voor het gebruik van onder hun verantwoordelijkheid toegelaten c.q. gecertificeerde inlogmiddelen. Ook de zaken die in de novelle geregeld worden, zoals het hanteren van privacy by design als toelatingseis, specifieke invulling van het verhandelverbod en de beweging naar open source zijn zaken die aanvullend op eIDAS worden geregeld. De regering is bekend met de wijze waarop andere lidstaten de eIDAS-verordening hebben geïmplementeerd. Daarbij zitten er verschillen in de systemen. Sommige landen kennen open toelating zoals de Wdo die beoogt; andere landen kiezen om inlogmiddelen in te kopen. Waar het in alle gevallen om gaat is dat de veiligheid en betrouwbaarheid van de middelen zijn geborgd. De eerste tranche van de Wdo legt – naast andere verplichtingen die buiten de werkingssfeer van eIDAS vallen – daarvoor de basis, en geeft waar nodig nationale invulling aan de (huidige) eIDAS-verordening. Met de gekozen systematiek in de Wdo kies ik voor een systematiek die de basis vormt waarop de eIDAS-revisie kan voortbouwen.

Toezicht en handhaving

De leden van de GroenLinks-fractie merken op dat uit antwoorden van de regering blijkt dat verschillende zaken in de Wet digitale overheid moeten worden gehandhaafd. De leden vragen de regering of er voor handhaving voldoende middelen zijn en zo ja, om dat nader toe te lichten.

Voor de toezichts- en handhavingstaken zoals geregeld in artikel 17 van het wetsvoorstel zijn door mij middelen gereserveerd. Het betreft toezicht op de naleving van de toelatingseisen door aanbieders van inlogmiddelen door het Agentschap Telecom, interbestuurlijk toezicht op het naleven van de Wdo en toezicht op naleving door bestuursorganen en aangewezen organisaties van de eisen inzake informatieveiligheid en de in dit verband opgelegde auditverklaring.

Wat betreft het toezicht door de Autoriteit Persoonsgegevens op de uitvoering van de Wdo, heb ik uw Kamer in de nadere memorie van antwoord van 2 juni 2021 geïnformeerd dat in lijn met het kabinetsbeleid (Kamerstukken 2020–2021, 25 268, nr. 192) middels een uitvoeringstoets inzichtelijk gemaakt zal worden wat de financiële gevolgen zijn van deze nieuwe wettelijke taak voor de AP. Financiële dekking zal worden geregeld.

Het lid van de BBB-fractie heeft kennisgenomen van het voorliggende wetsvoorstel. In het wetsvoorstel Wet digitale overheid is opgenomen dat de provincies het interbestuurlijk toezicht uitoefenen in het kader van deze wet op gemeenten en indien van toepassing op gemeenschappelijke regelingen. De provincies geven aan op zichzelf bereid te zijn om deze taak op zich te nemen, maar zij wensen op korte termijn duidelijkheid over de reikwijdte van het toezicht, welke eisen aan de taakuitvoering door gemeenten mogen worden gesteld, en de compensatie die het Rijk de provincies zal verschaffen voor deze nieuwe taak. Extra taken zonder budget is namelijk een resultaat voor mislukking. Op 18 augustus 2021 heeft Bureau Berenschot een kritisch rapport uitgebracht over de uitvoering van de Wdo. Eén van de eindconclusies luidt: «De specifieke toezichtstaak (artikel 17, lid 3) voor provincies op de naleving van de Wdo is nu niet uitvoerbaar. Er is wat ons betreft nog niet voldoende duidelijk wat van provincies wordt verwacht en het lijkt niet voldoende doordacht hoe deze taak zich verhoudt tot de generieke toezichtstaak van provincies». Het lid van de BBB-fractie vraagt de regering om aan te geven hoe zij deze eindconclusies weegt en hoe zij de compensatie voor extra taken vorm gaat geven.

Het klopt dat op dit moment gesproken wordt over de exacte invulling van de toezichthoudende taak door de provincies in relatie tot de Wdo. Ik ben hierover in gesprek met de provincies en het IPO en zal hier binnenkort samen met hen uitwerking aan geven. Mocht deze toezichthoudende taak aanleiding geven tot het bieden van compensatie, dan zal hier binnen de hiervoor geldende kaders gevolg aan worden gegeven.

Privacy by design

De leden van de D66-fractie halen de memorie van toelichting bij de novelle aan waarin staat dat voor het gebruik van privacy by design de actuele stand van processen en technieken leidend zal zijn. De leden vragen welke eisen hier momenteel aan voldoen en in hoeverre dit verschilt of aanvullend is aan de *General Data Protection Regulation (GDPR)*. In het verlengde daarvan vragen de leden wanneer volgens de regering gegevens onvoldoende beschermd zijn en er dus reden tot het weigeren van toelating is.

Ik hecht eraan dat het voldoen aan privacy by design niet betekent dat een lijstje van specifieke maatregelen moet worden afgelopen. Privacy by design betreft de wijze waarop bij de inrichting van verwerkingen van persoonsgegevens die nodig zijn om een inlogmiddel aan te bieden een brede afweging wordt gemaakt en rekening wordt gehouden met het ontwerp van verwerkingen van persoonsgegevens. Daarbij zal het gaan

het om het samenstel van verschillende maatregelen dat ervoor zorgt dat persoonsgegevens goed beschermd zijn en blijven. Dit kan techniek zijn, maar dit kunnen ook maatregelen van personele of organisatorische aard zijn.

Kortom, een lijst met eisen op basis waarvan privacy by design kan worden vastgesteld is niet op voorhand te geven en is bovendien per oplossing verschillend.
Voor de beoordeling of sprake is van privacy by design worden de richtsnoeren gebruikt die de koepel Europese privacy toezichthouders heeft opgesteld om invulling te geven aan artikel 25 van de AVG (het privacy by design-artikel).[1]

Inhoudelijk verschilt de wijze waarop privacy by design wordt benaderd daarom niet van de wijze waarop dit in de AVG wordt geregeld. Ingevolge de EU-regels mag dat ook niet, omdat verordeningen direct gelden. Wat door de regels in de Wdo wordt toegevoegd is dat privacy by design expliciet als toelatingscriterium kan worden gehanteerd.

De leden van de Volt-fractie onderschrijven het belang van privacy by design en privacy by default uit de Algemene Verordening Gegevensbescherming (AVG). De leden lezen dat de wijzigingen in het gewijzigde voorstel ervoor moeten zorgen dat partijen nieuwe methoden en technieken (kunnen) toepassen, zonder dat daarbij de rechtszekerheid in het geding komt. De leden stellen de vraag wiens rechtszekerheid daarbij gediend is: die van de partijen die nieuwe methoden en technieken toepassen en reeds een erkenning hebben gekregen, of de rechtszekerheid van de gebruikers van de door die partijen aangeboden elektronische identificatiemethoden (burgers). De leden vragen welke afweging is gemaakt tussen de belangen van beide partijen.

Het doel om privacy by design in de novelle op te nemen is om de privacybelangen dan wel de rechtszekerheid van burgers te dienen bij het gebruik van inlogmiddelen. Om dat te bewerkstelligen wordt aan aanbieders van inlogmiddelen de verplichting opgelegd om maatregelen te treffen naar de stand van techniek, zodat de beschermingsmaatregelen adequaat zijn en blijven. Ten overvloede merk ik op dat het nadrukkelijk niet zo is dat partijen door de inzet van nieuwe methoden en technieken gegevens van burgers en bedrijven voor andere doelen zouden mogen gebruiken. De ratio achter de opname van privacy by design is bescherming van burgers. Daarnaast is het ook zo dat aan partijen die inlogmiddelen aanbieden zekerheid wordt geboden: zij weten waaraan hun inlogmiddelen dienen te voldoen. Van een afweging tussen belangen is in dit verband mijns inziens dan ook geen sprake.

De leden van de Volt-fractie vragen welk beoordelingskader de Minister van Binnenlandse Zaken en Koninkrijksrelaties aanhoudt bij het beslissen of de erkenning van de reeds erkende partijen in stand wordt gehouden of wordt gewijzigd, geschorst of ingetrokken.

Voordat een partij wordt erkend wordt getoetst of de partij en het middel dat die partij wil aanbieden voldoen aan de toelatingseisen. Die eisen blijven gelden nadat een partij is erkend. Verder gelden aanvullende eisen vanaf het moment dat een partij is erkend. Het gaat om eisen die niet vooraf kunnen worden getoetst, bijvoorbeeld een te behalen beschikbaarheidsniveau. Het totaal van toelatingseisen en aanvullende eisen aan toegelaten partijen is het toetsingskader. Wanneer in het kader van

[1] https://edpb.europa.eu/system/files/2021–04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_nl.pdf

toezicht wordt geconstateerd dat niet langer aan de eisen wordt voldaan kan worden overgegaan tot het schorsen of intrekken van de erkenning, maar ook tot het opleggen van een bestuurlijke boete of een last onder dwangsom. Wijziging van een erkenning is mogelijk zonder een nieuwe aanvraag te doen en zal vooral plaatsvinden op verzoek van de houder, bijvoorbeeld wanneer deze wijzigingen wil doorvoeren in het authenticatieproces of in de organisatie. Een dergelijk verzoek wordt afgewezen wanneer de erkenningshouder met het doorvoeren van de wijziging niet langer voldoet aan de toelatingseisen. Intrekking van een erkenning kan ook op verzoek plaatsvinden. In dat geval wordt getoetst of partijen een exitplan hebben waarin de belangen van gebruikers voldoende zijn geborgd. Daarbij is van belang dat verwerkte persoonsgegevens worden vernietigd en of gebruikers voldoende tijdig worden geïnformeerd over de beëindiging.

Open source

Leden van verschillende fracties hebben vragen gesteld over het onderwerp open source. In de volgende antwoorden ga ik achtereenvolgens onder meer in op de mogelijke voordelen van open source, de noodzakelijke weging ten aanzien van andere relevante belangen, het groeimodel dat ik voornemens ben te hanteren en de wijze waarop ik voornemens bent te zorgen dat partijen weten waaraan zij moeten voldoen wanneer zij een aanvraag willen indienen. Doelstelling is om de beweging naar open source op een verantwoorde manier te maken.

De leden van de fractie van VVD vragen waarom ervoor is gekozen om een erkenning te weigeren als onvoldoende gebruik wordt gemaakt van software die onder een open source licentie is gepubliceerd.

Het gebruik van open source software heeft als voordeel dat gebruikers en andere geïnteresseerden de werking van deze software kunnen inzien. Deze transparantie geeft hen de mogelijkheid om te controleren of de software werkt zoals is voorgesteld en of deze veilig is. Meer ogen zorgen in dat geval voor toename van de veilige werking van de software en de mogelijkheid om bijvoorbeeld sneller beveiligingsproblemen te ontdekken. Open source kan daarmee een bijdrage leveren aan de veiligheid en innovatie.

De mate waarin daadwerkelijk sprake is van dit voordeel is echter afhankelijk van het onderhoud van de broncode. De mate waarin dit onderhoud plaatsvindt kan sterk verschillen per open source softwarepakket. De kracht en meerwaarde van open source is daarmee vooral afhankelijk van de sterkte, activiteit en omvang van de gemeenschap en ontwikkelaars die dit «dragen». Een goede community is noodzakelijk om te zorgen dat veiligheidslekken snel gedicht kunnen worden, voordat kwaadwillenden deze kunnen opmerken en benutten.
Gelet op deze voordelen die open source kan hebben, wordt het gebruik ervan gestimuleerd, waarbij een afweging wordt gemaakt tussen factoren zoals de veiligheid en continuïteit van middelen. Daarom wordt met deze novelle voorgesteld vast te leggen dat een erkenning niet wordt verleend, wanneer onvoldoende gebruik wordt gemaakt van software die onder een open source licentie is gepubliceerd. Daarmee wordt van partijen geëist dat zij een beweging inzetten naar het gebruik van open source.

De leden van de D66-fractie vragen wat de criteria zijn op basis waarvan een weging kan worden gemaakt over het wel of niet verplicht gebruiken van open source. Zij vragen verder of dit afhankelijk is van een bepaalde hoeveelheid aanbieders en of daar een limiet voor geldt.

Bij de vaststelling of voldoende dan wel onvoldoende gebruik wordt gemaakt van open source software zijn de volgende overwegingen van belang. Ten eerste wordt gekeken naar de beschikbaarheid van open source software voor de verschillende functies van een inlogmiddel. Het aantal aanbieders is niet relevant, het gaat om de kwaliteit van de beschikbare open source-producten. Wat wel van belang is, is dat de broncode openbaar is. Dat biedt immers de nagestreefde transparantie. Wanneer voor een bepaalde functie geen open source software beschikbaar is die goed wordt onderhouden en ondersteund, is het gebruik van closed source gerechtvaardigd.
Ten tweede wordt gewogen of de veiligheid gewaarborgd wordt bij het gebruik van open source software. Als de veiligheid onvoldoende wordt ondersteund, is het gebruik van closed source software ook gerechtvaardigd.

Overigens hecht ik eraan om op deze plaats te benadrukken dat de inzet van open source, mits goed onderhouden en gedragen door een goede en kundige groep ontwikkelaars, juist ook kan bijdragen aan de veiligheid, doordat meer mensen meekijken en sneller beveiligingsproblemen kunnen worden ontdekt en opgelost.

Ten derde wordt meegewogen of het gebruik van open source software voor partijen uitvoerbaar is. Dit doe ik om te voorkomen dat een te snelle omschakeling naar open source tot continuïteitsrisico's kan leiden, omdat de partijen die nog voor een belangrijk deel closed source werken, die niet kunnen opvangen. Een product van closed source als open source aanbieden heeft namelijk meer voeten in de aarde dan enkel de aanpassing van de licentie. Het raakt ook de manier waarop de aanbieders nu de beveiliging ingericht hebben. De maatschappij is er immers niet bij gebaat wanneer toepassing van dit criterium ertoe leidt dat er hierdoor geen inlogmiddelen beschikbaar zijn om toegang tot digitale dienstverlening te krijgen of deze niet meer veilig zijn.

Op deze factoren is ingegaan in de memorie van toelichting bij de novelle in de paragraaf «Open source». Daarin is tevens uiteengezet dat sprake is van een groeimodel, waarmee wordt toegewerkt naar inzet van meer open source software waar dat mogelijk is. Een dergelijk groeimodel is nodig om te voorkomen dat voor gebruikers geen inlogmiddelen beschikbaar zijn om toegang te krijgen tot digitale dienstverlening.

De leden van de VVD-fractie vragen of de regering de mening deelt dat het allerbelangrijkste is dat technische oplossingen aan de veiligheidseisen en -waarborgen voldoen, dat open source niet per definitie de veiligste optie is en dat closed source oplossingen niet uitgesloten mogen worden.

Ik deel deze mening van deze leden. Dat is ook de reden dat ik in eerdere beantwoording heb aangegeven dat ik middelen op hun merites wil kunnen beoordelen, waarbij veiligheid voor burgers en betrouwbaarheid van middelen uiteindelijk de doorslag geven. Echter ik wil óók de beweging naar de inzet van meer open source maken bij de in te zetten middelen. Daarbij geldt dat het een het ander niet uitsluit en dat, zeker als de randvoorwaarden ten aanzien van open source goed worden ingevuld, open source juist ook een bijdrage kan leveren aan de veiligheid van inlogmiddelen. Het gebruik van open source software kan belangrijke voordelen hebben voor gebruikers. Op die voordelen ben ik in het voorgaande ingegaan.
Het gebruik van deze software mag echter niet in onaanvaardbare mate ten koste gaan van de factoren veiligheid of de beveiliging van de processen die voor de werking van een inlogmiddel noodzakelijk zijn.

Wanneer het gebruik van open source software die factoren wel op onaanvaardbare wijze aantast is het gebruik van closed source software wenselijk. Gedacht kan worden aan gevallen waarin het gebruik van software waarvan de broncode openbaar is, leidt tot een hogere kwetsbaarheid voor aanvallen op de beveiligingsprocessen. Ik deel dus de mening van de VVD-fractie en ben voornemens vast te leggen dat bij toelating rekening wordt gehouden met verantwoord gebruik van open source software gelet op de veiligheid van de inlogmiddelen.

Kort en goed dient als voor een functionaliteit een in alle opzichten gelijkwaardige open source oplossing voorhanden is, deze te worden ingezet. Daarbij houd ik zoals hierboven aangegeven rekening met de continuïteit en veiligheid van huidige middelen en een redelijke toegroeitermijn.

De leden van de D66-fractie vragen een nadere toelichting over verschillende aspecten op het gebied van open source waaronder de transitietermijn richting open source. Deze leden vragen of dezelfde termijn ook geldt voor DigiD. Ook de leden van de Volt-fractie stellen vragen over de praktische uitwerking van dit toetsingscriterium.

Zoals in het voorgaande is aangegeven wil ik een groeimodel hanteren. Dit betekent dat (potentiële) aanbieders van inlogmiddelen stap voor stap steeds meer open source moeten inzetten. Dat kan naarmate er meer veilige en bruikbare open source oplossingen beschikbaar komen. Zo wordt de beweging naar open source in gang gezet en gehouden. Ook wil ik aan aanbieders een verplichting opleggen om openbaar te maken welke open source software ze al gebruiken. Hiermee wordt inzichtelijk hoe ver het gebruik van open source gevorderd is.
In de uitvoeringsregelgeving waarin de toetsing van open source software wordt uitgewerkt, zal ik een minimumniveau vastleggen waaraan een middel moet voldoen. Dat minimumniveau zal ik, afhankelijk van de beschikbaarheid van open source, periodiek bijstellen. Zo borg ik dat het groeien naar open source niet ten koste gaat van de veiligheid van gebruikers of van hun mogelijkheden om toegang te krijgen tot digitale overheidsdiensten.
Een dergelijk groeimodel zorgt er ook voor dat de verplichtingen voor deelnemende partijen op verantwoorde wijze meegroeien met het aanbod van open source. Op deze manier wordt het gehele aanbiedersveld in beweging gebracht richting open source, zonder dat de koplopers in hun mogelijkheden worden beperkt.

Een termijn waarbinnen de transitie richting open source is voltooid, is dus niet te geven. Deze is onder meer afhankelijk van de ontwikkelingen op het gebied van open source software en de mate waarin deze wordt ondersteund.

Voor een publiek identificatiemiddel, DigiD, zal hetzelfde minimumniveau gelden als voor identificatiemiddelen van private aanbieders.

De leden van de D66-fractie vragen waarom de regering open source niet heeft verankerd in de wet in plaats van met een wegingsfactor.

Zoals in het antwoord op de vorige vraag is aangegeven is het wenselijk een door middelenaanbieders te halen minimumniveau vast te stellen van open source software of andere software waarvan de broncode openbaar is gemaakt. Daarbij heb ik beargumenteerd waarom een absolute verplichting om open source te gebruiken niet wenselijk is vanuit maatschappelijk perspectief. Het toetsingscriterium voor open source, zoals dat in de voorliggende novelle is opgenomen, maakt het mogelijk

om een groeimodel te hanteren, waarbij de norm periodiek opnieuw wordt vastgesteld aan de hand van de stand der techniek en met inachtneming van de relevante belangen. Het ligt vervolgens voor de hand dat de norm niet bij wet, maar bij lagere regeling wordt vastgesteld.

De leden van de VVD-fractie vragen de regering nader op in te gaan op de rechtszekerheid voor aanvragers en op de vraag wanneer sprake is van voldoende gebruik van open source.

Naar mijn mening komt het systeem dat ik voor ogen heb, een minimumniveau dat door partijen moet worden gehaald, de uitvoerbaarheid en de rechtszekerheid ten goede. Potentiële aanvragers en deelnemende partijen kunnen op basis van het systeem dat in lagere regelgeving op grond van de wet wordt uitgewerkt concluderen aan welke norm zij op een bepaald moment moeten voldoen en wat zij moeten doen om die norm te halen.

De leden van de D66-fractie vragen op welke manier het gebruik van open source wordt gehandhaafd.

Aanvragers van een erkenning moeten in hun aanvraag aangeven welke van de door hen gebruikte softwarecomponenten open source zijn of waarvan de broncode openbaar is. Bij de aanvraag wordt getoetst of met die componenten het op dat moment geldende minimumniveau wordt gehaald. Wordt het minimumniveau niet gehaald, dan wordt de aanvraag afgewezen. Wanneer een erkenning wordt verleend is de erkende partij verplicht de in de aanvraag genoemde softwarecomponenten ook daadwerkelijk te gebruiken. Daarop vindt toezicht plaats en bij overtreding kunnen handhavingsinstrumenten worden ingezet.

Wanneer het minimumniveau wordt bijgesteld, krijgen reeds erkende partijen een termijn om aan de nieuwe norm te voldoen. Van partijen wordt gevraagd te onderbouwen op welke wijze zij aan die norm voldoen en zij zijn gehouden de in die onderbouwing genoemde softwarecomponenten ook daadwerkelijk te gebruiken.

De leden van de VVD-fractie vragen hoe het onderwerp open source is geregeld in het wetsvoorstel Wet digitale overheid dat nu in de Eerste Kamer ligt.

Het wetsvoorstel Wet digitale overheid dat nu bij de Eerste Kamer ligt bevat geen inhoudelijke erkenningseisen. Volgens de systematiek van dat wetsvoorstel worden die eisen vastgelegd in regelgeving die op dat wetsvoorstel wordt gebaseerd. Met deze novelle wordt beoogd om daar verandering in te brengen en wordt een aantal basiseisen, waaronder een toets op het gebruik van open source software, vastgelegd in de wet. De novelle zorgt aldus voor een formele/procesmatige versteviging van de open source eis. De wijze waarop daar inhoudelijk mee wordt omgegaan verandert niet.

De leden van de D66-fractie vragen of de regering problemen of oneerlijke concurrentie voorziet als er voor Nederlandse aanbieders andere eisen bestaan op het gebied van open source dan andere Europese aanbieders die toegang krijgen tot de Nederlandse markt.

De eIDAS-verordening stelt Europese lidstaten in de gelegenheid om een eigen stelsel in te richten voor toegang tot digitale overheidsdienstverlening. Daarbij kunnen lidstaten bepalen welke eisen zij hanteren voor eventuele private partijen die binnen hun stelsel diensten aanbieden. Het wetsvoorstel digitale overheid bevat de randvoorwaarden voor het

Nederlandse stelsel, zoals de verplichting om open source software te gebruiken. Deze eisen zijn binnen de Nederlandse context gerechtvaardigd en noodzakelijk, in het geval van het gebruik van open source omdat dit bijdraagt aan de transparante werking en de veiligheid van de desbetreffende middelen. Partijen die willen worden toegelaten tot het Nederlandse stelsel moeten aan die verplichtingen voldoen.

Het is inderdaad op grond van de eIDAS-verordening mogelijk om in Nederland ook inlogmiddelen te gebruiken die in andere lidstaten zijn uitgegeven. Het gebruik van deze middelen zal waarschijnlijk een uitzondering blijven, zoals ook nu al het geval is. Om toegang te krijgen tot de eigen overheid zullen burgers en bedrijven in de praktijk een middel in het eigen land aanschaffen.
De leden van de D66-fractie vragen of voor de onderdelen waar gebruik van open source niet gewenst is, wel de mogelijkheid bestaat van het stimuleren van open standaarden, bijvoorbeeld ter bevordering van interoperabiliteit.

Het gebruik van open standaarden staat los van het gebruik van open source software door aanbieders van inlogmiddelen. Open standaarden zijn bedoeld om ervoor te zorgen dat iedereen dezelfde taal spreekt en open source is ervoor bedoeld dat de broncode voor software die gebruikt wordt openbaar is.

De Wdo biedt zeker de mogelijkheid om standaarden te verplichten ter bevordering van interoperabiliteit en informatiebeveiliging. Een voorbeeld hiervan is het thans actuele vraagstuk ter voorkoming van ransomwareaanvallen. Op grond van de Wdo zouden bijvoorbeeld informatieveiligheidstandaarden voor e-mail kunnen worden verplicht, waarmee de veiligheid en betrouwbaarheid van e-mail van de overheid verhoogd wordt.

Overige onderwerpen

De leden van de CDA-fractie hebben gevraagd naar de uitwerking van de motie-Van der Molen[2]. Deze motie is gericht op het herstellen van een weeffout die is ontstaan in de aanloop van het gehele wetstraject. Deze leden vragen waarom de uitvoering van de motie niet nu al via deze novelle geregeld kan worden, en niet zoals ik de Kamer eerder heb bericht, pas in de tweede tranche van de Wet digitale overheid.

Ik heb in mijn brief van 14 juli 2021 uw Kamer geïnformeerd hoe ik uitvoering zal geven aan de motie-Van der Molen. Ik heb daarin aangegeven dat ik gefaseerd beheerst toewerk naar een duurzaam en integraal stelsel van toegang voor burgers en bedrijven met inachtneming van de huidige praktijk en de systematiek van de eerste tranche. Dat het burger- en bedrijvendomein gescheiden is in de eerste tranche betreft nadrukkelijk geen weeffout maar een bewuste keuze. Het realiseren van een geïntegreerd burger- en bedrijfsmiddel en organisatiemiddel is een proces dat tijd kost en impact heeft voor zowel partijen binnen het stelsel als voor burgers en bedrijven die van de diensten gebruikmaken, en is daarom een te grote wijziging om binnen het bestek van deze novelle verantwoord te kunnen doen.

In het rapport «Digitalisering in wetgeving en bestuursrechtspraak» doet de Raad van State zes aanbevelingen[3], zo geven de leden van de

[2] Kamerstuk 34 972, nr. 32
[3] Digitalisering wetgeving en bestuursrechtspraak, publicatie van de Raad van State d.d. 28 juni 2021

SP-fractie aan. Deze zien onder andere op de gevolgen van automatisering voor burgers. Zo adviseert de Raad onder andere om «goede en inzichtelijke afspraken te maken over onderwerpen als verantwoordelijkheid, datagebruik, eigendom van data en techniek, onderhoud en knowhow.» Ziet de regering ook mogelijkheden om in deze wet ruimte te vinden voor de aanbevelingen van de Raad van State en hierover met een visie te komen, zo vragen deze leden.

Het rapport bevat een herbevestiging van eerdere adviezen van de Raad van State over bijvoorbeeld techniekonafhankelijk formuleren. Hierop wordt ingegaan in de paragraaf «Techniekonafhankelijk wetgeven». Daarnaast bevat het rapport een aantal denkrichtingen, vastgelegd in – zoals de leden van de fractie van de SP naar voren brengen – 6 aanbevelingen over bijvoorbeeld het gebruik van algoritmen door de overheid in besluitvorming die buiten het kader van dit wetsvoorstel in overheidsbeleid en mogelijk ook in wetgeving nadere uitwerking behoeven. Dit valt buiten het kader van het nu voorliggende wetsvoorstel. In interdepartementaal verband wordt bekeken hoe gegarandeerd kan worden dat de noties uit het rapport breed in de voorbereiding van beleid en wetgeving worden meegenomen, en wordt onderzocht hoe de denkrichtingen nader kunnen worden uitgewerkt.
Een aantal van de door uw leden aangehaalde onderwerpen zoals datagebruik en de mogelijkheid om regie te voeren op de eigen gegevens wordt in de tweede tranche van de Wdo in het kader van de wettelijke regeling van regie op gegevens opgepakt. Een aantal andere onderwerpen die de Raad adresseert, zoals onder andere het gebruik van algoritmen bij besluitvorming door de overheid, horen niet thuis in de Wdo. Dit betreft namelijk niet de inkadering van voorzieningen, maar de wijze waarop overheden hun besluitvorming inrichten. Hier moet eventueel op andere wijze nadere uitwerking aan gegeven worden in de Algemene wet bestuursrecht. Ik werk hier samen met de Minister van Justitie en Veiligheid aan.

De leden van de SP-fractie lezen dat het in algemene zin reguleren van alle vormen van commerciële uitnutting van persoonsgegevens buiten de werkingssfeer van dit wetsvoorstel valt. Zij vragen waarom daarvoor is gekozen en niet voor een ruimere definitie waarbij elke vorm van commerciële uitnutting van persoonsgegevens wordt uitgesloten.

Het wetsvoorstel regelt het inloggen bij (semi-)overheidsdiensten door burgers en bedrijven met publieke en private toegelaten inlogmiddelen en de randvoorwaarden die specifiek in die context gelden. Dit is waar de Minister van Binnenlandse Zaken bevoegd voor is. De definitie reikt daarmee zo breed als dat binnen diens bevoegdheid mogelijk is. Het regelen van de wijze waarop commerciële organisaties, die geen connectie hebben met het verlenen van digitale toegang tot de (semi-)overheid, met persoonsgegevens omgaan valt daarbuiten. De regels waaraan aanbieders van inlogmiddelen moeten voldoen zien daarom ook op het inloggen bij overheidsdiensten en niet bij commerciële diensten. Het gebruik van persoonsgegevens bij het inloggen bij commerciële diensten is elders geregeld, onder meer in de Algemene verordening gegevensbescherming.

De leden van de D66-fractie zien graag in een tijdslijn uiteengezet wat de novelle betekent voor de verdere behandeling en uitvoering van de Wet Digitale Overheid.

Ik begrijp de wens voor een tijdlijn. Deze is echter mede afhankelijk van de data waarop de novelle door uw Kamer zal worden behandeld en aangenomen, en de datum waarop vervolgens de behandeling van het

oorspronkelijke wetsvoorstel met de novelle door de Eerste Kamer plaats zal vinden. In beginsel is het nog mogelijk dat het wetsvoorstel op 1 juli 2022 in werking kan treden, als uw Kamer de behandeling voor eind januari 2022 afrondt. Ik spreek de hoop uit dat dit mogelijk is. Daarmee kunnen de waarborgen die het wetsvoorstel samen met de novelle biedt, van kracht worden, kunnen hogere betrouwbaarheidsniveaus voor inloggen worden afgedwongen en wordt de overheidsdienstverlening veiliger. Ik zeg toe dat uw Kamer voor het einde van het jaar geactualiseerde concepten ontvangt van de, nu bij uw Kamer in voorhang zijnde, algemene maatregelen van bestuur over inlogmiddelen die uitwerking geven aan de novelle.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
R.W. Knops