Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2020–2021

34 972 Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid)

P

NADERE MEMORIE VAN ANTWOORD

Ontvangen 2 juni 2021

1. Inleiding

De memorie van antwoord heeft de **commissie** aanleiding gegeven tot het gezamenlijk maken van enige opmerkingen en het stellen van enige vragen. Deze staan in de volgende paragraaf opgesomd, waarna de leden van enkele hier na te noemen fracties daarnaast of in aanvulling daarop nog opmerkingen en vragen aan de regering willen voorleggen. Deze zijn gerangschikt in aparte paragrafen.

De leden van de fractie van het **CDA** hebben kennisgenomen van de beantwoording door de regering.
Zij hebben nog enkele nadere vragen en opmerkingen.
De leden van de fracties van **GroenLinks**, de **PvdA** en de **ChristenUnie** hebben kennisgenomen van de beantwoording door de regering en hebben gezamenlijk nog nadere opmerkingen en vragen.
De leden van de fractie van **D66** danken de regering voor de beantwoording en zijn blij met de toezegging om open source en privacy by design wettelijk te verankeren als toelatingscriteria. Zij hebben nog enkele aanvullende vragen.
De leden van de fractie van de **PVV** hebben kennisgenomen van de beantwoording door de regering. Zij hebben nog nadere opmerkingen en vragen.
e leden van de fractie van de **SP** bedanken de regering voor de uitgebreide beantwoording. Ze merken op dat de regering de zorgpunten van deze leden goed gehoord heeft. Ze waarderen de inzet van de regering om hieraan tegemoet te komen, maar vinden een aantal zaken nog onduidelijk. Daarom hebben zij nog een aantal vragen.
De leden van de fractie van de **ChristenUnie** hebben kennisgenomen van de beantwoording door de regering en hebben naast de gezamenlijke vragen nog enkele opmerkingen en vragen.

kst-34972-P
ISSN 0921 - 7371
's-Gravenhage 2021

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 zoveel mogelijk aangehouden, met dien verstande dat vergelijkbare vragen zijn geclusterd.

2. Vragen en opmerkingen van de commissie

De commissie dankt de regering voor de memorie van antwoord, de toezeggingen en de keuze om naar aanleiding van de vragen van de leden van de fracties van de Eerste Kamer tot een novelle over te gaan. Zou de regering kunnen aangeven op welke termijn zij verwacht deze novelle aan de Tweede Kamer aan te bieden? Kan zij op basis van de toezeggingen in de memorie van antwoord uiteenzetten hoe deze novelle eruit gaat zien? Gaat de regering in de opmaat naar de novelle nog een consultatieronde houden bij partijen die gespecialiseerd zijn in open source en privacy by design? De commissie vraagt ook hoe de open source en privacy by design uit de novelle zich tot de toekomstige tranches in het kader van de Wdo verhoudt?

In reactie op de vragen van de commissie wordt opgemerkt dat inmiddels een novelle aan de Afdeling advisering van de Raad van State is voorgelegd. Na verwerking van het advies, zal deze aan de Tweede Kamer worden gezonden. Naar verwachting zal dat nog voor de zomer zijn. De novelle bevat formeel-wettelijke verankering van privacy by design, het verhandelverbod van gegevens en open source. Meer specifiek wordt ter zake van (private) inlogmiddelen voor burgers en bedrijven bepaald dat de Minister van BZK een erkenning weigert indien het ontwerp van het identificatiemiddel of de ontsluitende dienst onvoldoende voorziet in de bescherming van gegevens, de aanvrager niet aannemelijk heeft gemaakt dat met de erkenning geen inkomsten worden verkregen uit het verhandelen of verstrekken van gegevens over gebruikers of authenticatie van gebruikers, of bij de voor de werking van het identificatiemiddel of de ontsluitende dienst noodzakelijke processen naar zijn oordeel onvoldoende gebruik wordt gemaakt van software die onder een open source licentie is gepubliceerd.
In de opmaat naar de novelle is geen afzonderlijke consultatieronde gehouden bij marktpartijen. De afgelopen jaren zijn bij de voorbereiding van het wetsvoorstel marktpartijen en andere – private en publieke – stakeholders regulier en intensief betrokken. Hierdoor bestaat een goed beeld van kansen, risico's en belangen. De in de novelle geregelde onderwerpen zullen naar verwachting onverkort relevant blijven in toekomstige tranches van de Wdo.

Open source

Hoewel het beginsel open source nu in de wet zal worden opgenomen, roepen de antwoorden in de memorie van antwoord op pagina's 19 en 22 de vraag op hoe positief de regering hierover nu precies is.[1] Bovendien wordt in de memorie van antwoord over «open source» gesproken als «toelatingscriterium», «principe» of «hoofdelement», maar nooit expliciet als toelatingseis. Kan de regering bevestigen dat open source een vereiste is voor toelating? En om wat voor open source-licentie gaat het dan?

In reactie op de vragen van de commissie merk ik op dat de regering de voordelen van open source software en de bijdrage, die openbaarheid van de broncode kan leveren aan transparantie en aan veiligheid, onderschrijft. De regering staat positief tegenover open source en heeft om die reden ervoor gekozen het beginsel in de wet op te nemen. Bij de leden

[1] Kamerstukken I, 2020/21, 34 972, L.

bestaat kennelijk twijfel over het enthousiasme van de regering, omdat open source niet als toelatingseis wordt opgenomen maar als wegingsprincipe. Laat ik voorop stellen dat het gebruik van open source de weg is die de regering wil opgaan. Het feit dat dit als wegingscriterium is opgenomen heeft derhalve niets te maken met enige twijfel over de waarde of nut van open source, maar alles met het mogelijk maken van een beheerste en verantwoorde toegroei naar meer open source. Deze formulering beoogt dus op geen enkele wijze afbreuk te doen aan het vertrouwen in open source, maar beoogt het gebruik van open source beheerst mogelijk te maken, waarbij ook de continuïteit van middel, waarvan in de praktijk miljoenen burgers en bedrijven direct afhankelijk zijn voor hun contact met de overheid, op korte termijn te borgen en op een verstandige manier meer open source te maken. Dat resulteert erin dat open source als wegingsprincipe wordt gehanteerd en niet als «harde» toelatingseis.

Opensourcelicenties zijn er in vele soorten en maten. Bepalingen over gebruik, hergebruik, aanpasbaarheid, wijze van inzet (commercieel of niet commercieel) of afbakening naar doelgroep (bijvoorbeeld onderwijsdoeleinden) kunnen enorm variëren. Een van de criteria die kenmerkend is voor de bepaling over een licentie (of beter gezegd: de software) open source is, is dat de broncode openbaar toegankelijk is. Het is dit criterium dat in de weging voor open source in dit verband bepalend is, omdat daaruit de ook door de leden beoogde voordelen transparantie en veiligheid – mits goed geregeld – kunnen voortvloeien.

De regering schrijft op pagina 22 dat open source software die niet actief ondersteund en onderhouden wordt dan zelfs een veiligheidsrisico kan worden in plaats van een veiligheidsmaatregel. Hoe bedoelt de regering dit? Alle software die niet onderhouden wordt, vormt een risico; dat geldt niet alleen voor open source. Welke specifiek en uniek kenmerk van open source is onveiliger, zoals de regering lijkt te suggereren. Of ziet de commissie dat verkeerd? Is de regering het eens dat er een brede consensus is dat de openheid van open source software juist bijdraagt aan goede beveiliging?

In reactie op de vragen van de commissie merk ik op dat de voordelen van open source niet worden gerealiseerd door het enkele feit dat software open source wordt aangeboden. Zoals is aangegeven in de Memorie van antwoord is het doel dat aan de eisen van veiligheid en betrouwbaarheid wordt voldaan. De openbaarheid van de broncode – door het «meer-ogen-principe» – kán bijdragen aan veiligheid. Hierdoor kunnen meer mensen kijken of de software werkt zoals bedoeld, en of er geen veiligheidsproblemen in zitten. Dit voordeel onderken ik. De kracht of sterkte van open source is echter primair afhankelijk van de sterkte en activiteit van omvang van de gemeenschap en ontwikkelaars die dit «dragen». De eigenschap open source als zodanig biedt niet de garantie voor transparantie en veiligheid. Om het principe te laten gelden zal een voldoende omvangrijke en actieve gemeenschap moeten bestaan en in stand worden gehouden.

Zoals is opgemerkt in de memorie van antwoord biedt open source software kansen, de reden waarop dit als criterium in de novelle wordt opgenomen. De kracht en de veiligheid die worden geboden ligt in de mensen erachter die de software maken en de context waarin de software wordt ingezet. Op het moment dat die kracht wegvalt, vallen ook de voordelen weg. De regering is het overigens eens met de leden dat dat ook voor andere dan opensourcesoftware geldt. Echter daar zal veeleer sprake zijn van een aanspreekbare organisatie, waarmee afspraken worden gemaakt en zekerheden worden verkregen over de ontwik-

kelkracht, de updatesnelheid en van mensen achter de software. Dat laatste zou in principe ook bij open source software gerealiseerd kunnen worden, maar vergt een actieve en aanspreekbare ontwikkelgemeenschap, en de mogelijkheid om daar afspraken /continuïteitsgaranties over af te spreken.

In de memorie van antwoord wordt gesproken van «de beweging naar open source in te zetten» en over een «transitieproces».[2] Kan een closed source inlogmiddel wel aanvankelijk toegelaten worden, en dan pas na zeg 3 jaar open source worden, zo vraagt de commissie. Waarom wordt niet van begin af aan een heldere norm gesteld met een open source vereiste, zonder uitzonderingen en transitieproces van 3 jaar?
Kan de regering aangeven waarom zij een transitieperiode noodzakelijk acht? Hoewel de commissie allesbehalve overtuigd is van de noodzakelijkheid van een dergelijke periode, zou deze in ieder geval beperkt moeten zijn. Als open source verplicht wordt in de wet of onderliggende AMvB's is er geen noodzaak langer te wachten en er is ook geen transitieruimte nodig. De norm voor open source is helder en elke partij die aspiraties heeft om toegelaten te worden als privaat middel kan zijn broncode eenvoudig publiceren. De commissie ontvangt hierop graag een reactie.

In reactie op de vragen van de commissie merk ik op dat ik, zoals hierboven is uiteengezet, kies voor een transitieproces, oftewel voor een beweging naar open source. Ik herhaal hier de inzet dat meer open source het doel is, als belangrijk middel om transparantie en veiligheid te borgen. De optie om open source per direct als «harde» eis te stellen is serieus onderzocht. Essentiele voorwaarde voor de regering is dat dat uitvoerbaar moet zijn en niet leidt tot ongewenste consequenties voor burgers en bedrijven. Dat lijkt wel het geval te zijn, omdat middelen waar burgers nu gebruik van maken om veilig bij de overheid in te loggen, gebruik maken van closed source.,Door de stap te snel te maken kan de continuïteit van het gebruik van de inlogmiddelen in gevaar kan komen. Dat moet worden voorkomen. Zoals ik eerder aangaf, begrijp ik de wens van uw Kamer om open source in te zetten. Dit begrip wordt ook gedeeld, maar tegelijkertijd bestaat ook breed de zorg voor veilige inlogmiddelen op de korte termijn. Ik wil daarom in de novelle tot uitdrukking brengen dat we de beweging naar open source gaan maken, maar dan geformuleerd als een beoordelingscriterium voor toe te laten inlogmiddelen, waarbij ik de beoordelingsruimte houd om inlogmiddelen op hun merites te beoordelen. Daarmee brengt de novelle expliciet tot uitdrukking dat open source de richting is die we inslaan, zonder dat de gesignaleerde uitvoerbaarheidsproblemen optreden. Tot slot merk ik op dat gelet op het bovenstaande het sec verplicht stellen bij wet of AMvB weliswaar zou kunnen, maar dat dat leidt tot negatieve consequenties, met name voor burgers en bedrijven die van de continuïteit van middelen afhankelijk zijn. Zo'n verplichting zou dan slechts symboolregelgeving zijn met een op korte termijn averechts effect op de mogelijkheid voor mensen om veilig hun zaken te doen.

Op p. 20 van de memorie van antwoord staat: «Dit kan er in voorkomend geval op neerkomen dat de inzet van open source niet in de rede ligt en dat (op onderdelen) voor closed source kan – en moet – worden gekozen omdat veiligheid met open source niet gegarandeerd kan worden.» Kan de regering uiteenzetten welke uitzonderingsmogelijkheden zij ziet onder welke omstandigheden voor de open source vereiste? Wie beslist er over of er al of niet sprake kan zijn van een uitzondering, op welke gronden? Gaat de regering de software die gebruikt wordt voor het inloggen met de

[2] Kamerstukken I, 2020/21, 34 972, L, p. 27 en 31.

DigiD app van de overheid, en voor het inloggen met een identiteitskaart (met behulp van de DigiD app), ook open source maken?

In reactie op de vragen van de commissie merk ik op dat de Minister van BZK als bevoegd gezag – hij beoordeelt de aanvraag voor een erkenning – degene is die beslist over het toepasselijk zijn van de uitzondering. In reactie op de vragen van de commissie t.a.v. de software van DigiD merk ik op dat er onderzocht zal worden wat hierin mogelijk is. Daarbij is het van belang te kijken naar de technische en juridische mogelijkheden alsook de wenselijkheid in relatie tot eventuele beveiligingsrisico's bij het publiceren van deze software. Daar kunnnen derhalve ook uitzonderingen op bestaan. Zo is het denkbaar dat het zondermeer publiceren van dergelijke overheidsapps phishing met namaakapps in de hand kan werken, waarmee fraudeurs onrechtmatig inloggegevens kunnen verkrijgen.

Decentraal en centraal

De regering zegt in de memorie van antwoord, onder andere op p. 25, dat zowel centrale als decentrale oplossingen binnen de Wet digitale overheid passen. Maar is de regering het met de commissie eens dat het risico van een hack op een centrale architectuur groot is?

In reactie op de vraag van de commissie merk ik op dat het risico op een hack altijd aanwezig is. Of er nu met centrale of decentrale systemen wordt gewerkt – een hack kan nooit volledig kunnen worden voorkomen. Datalekken vinden immers plaats vanwege meerdere factoren, technische maar ook menselijke. Zij kunnen nooit volledig worden voorkomen, maar als het gebeurt moet er alles aan gedaan worden om dat zo snel mogelijk te ontdekken en de gevolgschade zo klein mogelijk te houden. Ik ben het met uw kamer eens dat een plek waar veel te halen is, een aantrekkelijker plek kan zijn om gehackt te worden, dan een plek waar weinig of niets te halen is. Daar is in de architectuur rekening mee gehouden door bij het inloggen bij overheden enkel het burgerservicenummer te verwerken en dit versleuteld te versturen en op te slaan. Andere persoonsgegevens (attributen) worden er naast de logging niet geregistreerd, dat wil zeggen niet op andere plekken waar dat nu reeds plaatsvindt.

Zoals ik in de memorie van antwoord al aangaf wordt door decentrale oplossingen logging geregistreerd. Dat is nodig en belangrijk om problemen te kunnen oplossen. Het risico van een hack op de centrale oplossing acht ik dan ook niet groter. En mocht deze toch plaatsvinden, dan zal door de getroffen maatregelen de impact hiervan niet aanzienlijk zijn.

Kan zij daarom in de wet vastleggen dat centrale verwerking van persoonsgegevens minimaal is?

In reactie op de vraag van de commissie merk ik op dat dataminimalisatie als beginsel, naast andere belangrijke privacybeginselen, reeds geldt op grond van de AVG. Ook in het wetsvoorstel is neergelegd dat persoonsgegevens alleen voorzover noodzakelijk verwerkt mogen worden. Dat geldt voor centrale opslag van gegevens, maar evenzeer voor decentrale oplossing. Op verzoek van uw Kamer heb ik bovendien de verplichting tot privacy by design op wetsniveau opgenomen. Dit vereiste geldt zowel voor centrale als decentrale oplossingen. Hoe authenticatiediensten hier uitvoering aangeven, is binnen de door mij gestelde kaders, aan hen. Ik hecht eraan om voldoende ruimte te laten aan deze implementatie om innovatie mogelijk te maken en een zekere wendbaarheid in de uitvoering mogelijk te maken.

Dat kan betekenen dat centraal alleen (logs)gebruiksgegevens worden, maar niet de gebruikersgegevens die gebruikt worden bij het inloggen zelf. Die gebruikersgegevens kunnen dan decentraal, op het inlogmiddel opgeslagen worden. Gaat de regering inzetten om gebruikersgegevens decentraal op te slaan en centraal alleen de logs?

Nee, zoals ik hierboven al aangaf is de implementatie van de gestelde eisen vrij. Bij de implementatie is een centrale, maar ook een decentrale opzet mogelijk; beide zijn geen doel op zich. Waar het om gaat is de mate van privacybescherming van de oplossing die een aanbieder van een inlogmiddel realiseert. Een keuze voor centrale of decentrale opslag van gegevens acht ik daarom niet opportuun. Ik hecht eraan om voldoende ruimte te laten aan deze implementatie om innovatie mogelijk te maken en een zekere wendbaarheid in de uitvoering mogelijk te maken.

Is de regering het met de commissie eens dat als dit zo bij het ontwerp bij de GGD zo was geweest, een dergelijk datalek niet had kunnen voorkomen?

In reactie op de vraag van de commissie merk ik op dat het voorval bij de GGD een andere situatie betrof. Bij de GGD was sprake van datadiefstal door GGD-medewerkers. Het is niet met zekerheid te zeggen dat, als de gegevens bij de GGD decentraal waren opgeslagen, het niet mogelijk geweest om een grote hoeveelheid data te stelen. Deze datadiefstal kon onder andere plaatsvinden door een print- en exportfunctionaliteit op één van de systemen; deze is naderhand meteen uitgezet. Daarnaast controleert de GGD verdachte patronen en verdacht gedrag nu continu. De GGD slaat gegevens op die in het kader van de virusbestrijding praktisch en juridisch noodzakelijk zijn. De medewerkers die deze gegevens gestolen hebben, hadden toegang tot deze gegevens om hun werkzaamheden goed uit te kunnen voeren. Indien deze gegevens decentraal waren opgeslagen dan hadden deze medewerkers nog steeds toegang tot deze gegevens gehad.

De regering geeft aan dat er nadelen kleven aan decentrale oplossingen. Het ontwerp van decentrale oplossingen zorgt ervoor dat een lek of hack zich beperkt tot een individu en niet de hele user-base. Binnen welk afwegings- en toetsingskader worden de voor- en nadelen tegen elkaar afgewogen van decentraal en centraal of een combinatie daarvan?

In reactie op de vraag van de commissie merk ik op dat bij de weging wat in een specifiek geval adequate privacybeschermende maatregelen zijn, alle beginselen uit de AVG worden betrokken. Dat is breder dan waar en hoe gegevens worden opgeslagen. Zoals ik eerder antwoordde op de vraag van de fractie van de ChristenUnie, zijn in de architectuur privacybeschermende maatregelen genomen door bij het inloggen enkel het burgerservicenummer te verwerken en dit versleuteld te versturen en op te slaan. Daarnaast is voorzien in gescheiden opslag van gebruiks- en gebruikersgegevens waardoor koppeling van loggegevens aan personen niet mogelijk is. Reden voor het opslaan van logging is dat het in geval van problemen of misbruik nodig is om te kunnen reproduceren en de gebruiker te helpen.

En hoe verhoudt zich dit tot de toetsende en toezichthoudende rol van de overheid?

Zoals ik in de Memorie van antwoord aangaf (p. 36) is of een inlogmiddel op een centrale of decentrale manier beheerd wordt, als zodanig niet van belang zolang er voldaan wordt aan de wettelijke veiligheids- en betrouwbaarheidseisen, die bij AMvB en ministeriële regeling nader worden

ingevuld. 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. Er is dus sprake van toetsing en controle door de overheid.

Wat betekent het privacy by design-vereiste voor logging, versleuteling tegen hacks en voor functiescheiding en pseudonimiseren van gebruiksgegevens? Gaat het om het bijhouden van welke gebruiker waar op welk moment inlogt, of moet daarbij door de aanbieder van een inlogmiddel ook geregistreerd worden welke gebruikersgegevens bij dat inloggen onthuld worden? Moeten deze loggegevens versleuteld worden, niet alleen als bescherming bij eventuele aanvallen, maar ook ter versterking van de vereiste functiescheiding? Moeten centraal opgeslagen gebruikersgegevens gepseudonimiseerd worden?

In reactie op de vragen van de commissie merk ik op, dat privacy by design betekent dat er in het ontwikkelproces van ICT diensten rekening wordt gehouden met privacy verhogende maatregelen. Dat is een weging op grond van alle AVG beginselen. Dit betekent onder meer dat er niet meer gegevens verwerkt mogen worden dan nodig en dat de gegevens die verwerkt moeten worden, zo goed mogelijk afgeschermd worden. Dit kan bijvoorbeeld bereikt worden via versleuteling en pseudonimisering en door gescheiden opslag van gegevens. Er is voor gekozen om het burgerservicenummer te versleutelen, waarmee het onherleidbaar is tot de gebruiker en in geval van misbruik. Daarnaast worden gegevens gelogd om in geval van problemen of misbruik te kunnen achterhalen wat er is gebeurd en om zo de gebruiker te kunnen helpen. In de logging wordt bijgehouden wie op welk moment waar heeft ingelogd. Loggegevens (gebruiksgegevens) worden gescheiden van de gebruikersgegevens (BSN) opgeslagen.

Kan de regering bevestigen dat de open source-vereiste niet alleen geldt voor het inlogmiddel, maar ook geldt voor de software die een aanbieder van zo'n inlogmiddel gebruikt voor logging en monitoring, net als voor andere centrale verwerkingen van persoonsgegevens?

In reactie op de vraag van de commissie merk ik op dat het vereiste om waar mogelijk gebruik te maken van open source software in principe geldt voor alle software onderdelen die zorgen voor een goede werking van het middel. Ook wordt geen onderscheid gemaakt in de open source eis in relatie tot de wijze waarop persoonsgegevens worden verwerkt. Wel is het zo dat er op onderdelen – met gegronde redenen – beperkingen kunnen zijn ten aanzien van de openbaarheid van bepaalde handelingen. Wanneer in het belang van burgers op een systeem – centraal of decentraal – wordt gemonitord om te zorgen dat zij geen slachtoffer worden van fraude en misbruik, vervalt het hele nut ervan op het moment dat openbaar is – ook voor fraudeurs – waarop wordt gecontroleerd.

Kan de regering het privacy by design-vereiste concreet maken met een aantal voorbeelden van ontwerpen die niet aan privacy by design voldoen en dus tot niet-toelating leiden? In het bijzonder vraagt de commissie of een centrale architectuur met de bijbehorende privacy risico's aan privacy by design voldoet?

In reactie op de vragen van de commissie merk ik op dat er niet een one-size fits-all stramien is voor het inrichten van privacy by design. Dat hangt van verschillende factoren af, waarbij privacy by design in ieder geval breder is dan de vraag waar en hoe gegevens worden opgeslagen. De eisen die ik aan middelen stel zorgen ervoor dat voldaan wordt aan de eIDAS-verordening en de AVG en daarmee ook aan privacy by design. Of

een inlogmiddel op een centrale of decentrale manier beheerd wordt, is als zodanig niet van belang. Zoals ik heb opgenomen in de Privacyvisie eID die ik eind januari 2019 naar de Tweede Kamer stuurde (bijlage 871284 bij Kamerstukken 26 643, nr. 590), ga ik uit van integrale privacybescherming, waarbij op basis van privacyrisico's maatregelen genomen moeten worden. Er kunnen meerdere maatregelen genomen worden om privacyrisico's te verlagen. Hier bestaat niet één oplossing voor.

Buitenlandse wederzijds erkenning door eIDAS-verordening

Ingevolge de AVG is een nationaal-wettelijke grondslag nodig om mogelijk te maken dat private partijen bijvoorbeeld het burgerservicenummer kunnen verwerken. De eIDAS-verordening gaat uit van het beginsel van wederzijdse erkenning. Een inlogmiddel dat in een andere lidstaat is toegelaten, moet in Nederland geaccepteerd worden voor de toegang tot overheidsdienstverlening. Kan de regering nader toelichten wat de gevolgen hiervan zijn voor de keuzen die de regering maakt inzake dit wetsvoorstel, waaronder de keuze van openstelling voor private aanbieders? Is een van de gevolgen van de eIDAS-verordening dat wanneer in een lidstaat een partij binnen of buiten de EU toelaat deze ook in Nederland is toegelaten? Klopt het dat de stelling van de regering dat Nederland inlogmiddelen van een andere lidstaat moet toelaten, alleen opgaat als Nederland zijn markt ook daadwerkelijk openstelt voor private aanbieders? En als wij in Nederland private aanbieders toelaten, wat zijn dan de gevolgen voor de kaderstellende, toetsende en toezichthoudende rol van Nederland? Overweegt de regering in de novelle om de keuze van drie jaar geleden voor toegang voor private aanbieders te heroverwegen, ook in het licht van de technologische ontwikkelingen in de laatste jaren op het gebied van systemen die veilige, open source, decentrale en privacy by design zijn?

In reactie op de vragen van de commissie wordt opgemerkt dat het primaire gevolg van de eIDAS-verordening, zoals uw kamer terecht aangeeft, is gelegen in de verplichte acceptatie van Europees erkende inlogmiddelen in de grensoverschrijdende dienstverlening binnen de EU/EER. Het wetsvoorstel expliciteert dit in de bepalingen over de acceptatieplicht van inlogmiddelen (artikelen 7 en 15 Wdo). De keuze van openstelling voor private aanbieders heeft tot gevolg dat private middelen die door de Minister van BZK toegelaten (erkend) en bij de Europese Commissie aangemeld zijn, in andere lidstaten van de Europese Unie kunnen worden gebruikt. Omgekeerd moeten in andere lidstaten toegelaten – publieke en/of private, dat is aan de desbetreffende lidstaat – en bij de Europese Commissie aangemelde middelen ook in Nederland gebruikt kunnen worden. Dat Nederland inlogmiddelen van een andere lidstaat moet toelaten staat dus geheel los van de openstelling voor private aanbieders. Het stelsel van de Wdo, dat naast publieke middelen ook ruimte biedt voor private middelen, voorziet in strenge kaders en vergaande veiligheids-, betrouwbaarheids-, en privacybeschermingseisen; partijen worden hierop vooraf getoetst door het bevoegd gezag (de Minister van BZK) alsmede gedurende de looptijd van de erkenning door het Agentschap Telecom en de Autoriteit Persoonsgegevens. Het wettelijke stelsel voorziet bovendien ultimo in bevoegdheden voor de Minister van BZK om de toegang tot publieke dienstverlening te (doen) onderbreken. Met dit geheel wordt voldoende zicht en grip op private aanbieders gerealiseerd en worden voldoende waarborgen geschapen voor het veilig en betrouwbaar inloggen bij de overheid. In dit licht bezien is het verantwoord – juist ook om ruimte te bieden voor innovatie en toepassing van technologische ontwikkelingen – om private aanbieders toe te laten wanneer zij aan de gestelde eisen voldoen.

3. Vragen en opmerkingen van de leden van de fractie van het CDA

Wetswijziging

De leden van de fractie van het CDA zijn positief dat de regering aangeeft dat open source de norm wordt, privacy by design extra zal worden benadrukt en het verhandelen van gegevens wordt verboden door een wetswijziging. Dit geldt ook voor de toevoeging dat bij het aanvragen van een erkenning duidelijk moet worden gemaakt dat het verdienmodel een directe relatie moet aantonen tussen de vergoeding en de geleverde dienst: het inlogmiddel. Deze leden vragen de regering welke aanpak en timing zij in deze voor ogen heeft: eerst de novelle laten goedkeuren door de Tweede Kamer en dan het voorliggende wetsvoorstel inclusief de novelle te behandelen, of het voorstel van de Wet digitale overheid met een toezegging inzake de genoemde wijzigingen in de Eerste Kamer te bespreken? En welke overwegingen liggen daaraan ten grondslag, juist tegen de achtergrond dat de leden van genoemde fractie de wijzigingen van essentieel belang achten.

In reactie op de vragen van de CDA-fractie wordt opgemerkt, dat het de voorkeur heeft om zo snel mogelijk na het uitbrengen van de onderhavige nota het wetsvoorstel met een toezegging inzake de genoemde wijzigingen in de Eerste Kamer te bespreken. Indien uw kamer op korte termijn instemt met het wetsvoorstel – hoewel het dan nog niet inwerking treedt en de novelle nog niet door uw kamer is behandeld – verschaft dit een grote mate van duidelijkheid en rechtszekerheid aan betrokkenen (zij weten dan waar ze aan toe zijn), waardoor met de voorbereiding van de uitvoering kan worden gestart. Ook kunnen dan de voorgehangen AMvB's aan de Afdeling advisering van de Raad van State worden voorgelegd, waardoor de voortgang daarvan geen verdere vertraging oploopt en deze AMvB's gelijktijdig met het wetsvoorstel in werking kunnen treden.

Gegevensverwerking door private partijen

In de memorie van antwoord wordt aangegeven dat de partijen, die toegelaten zijn om een inlogmiddel te vervaardigen en aan te bieden, regelmatig zullen worden gecontroleerd. Soms wordt er ook gesproken over continue monitoring. Kan de regering aangeven of er nu sprake is van continue monitoring dan wel van regelmatige controle. Aan welke inzet wordt gedacht bij regelmatige controle? En zo ja, waarom?

In reactie op de vragen van de CDA-fractie wordt opgemerkt dat onderscheid gemaakt moet worden tussen soorten controle: toezicht en monitoring. Ik richt beide in. Toezicht is extern belegd en betreft de naleving van de toelatingseisen door partijen die inlogmiddelen aanbieden; dit wordt uitgeoefend door het Agentschap Telecom (AT). Het AT toetst vooraf (dat wil zeggen bij de aanvraag om toelating/erkenning) en tijdens de dienstverlening. Daarnaast richt ik intern beheersmatige en continue monitoring in op het gebruik van inlogmiddelen om technische problemen te signaleren en op ongebruikelijke handelingen die op misbruik kunnen duiden. Dit betreft monitoring van gegevensverkeer om problemen voor burgers zo vroeg mogelijk te signaleren, hen te helpen met het oplossen ervan en negatieve gevolgen voor hen zoveel mogelijk te voorkomen.

Ook wordt in de memorie van antwoord aangegeven dat bij misbruik besloten kan worden om de vergunning in te trekken.[3] In hoeverre is het niet meer toestaan van een inlogmiddel daadwerkelijk te realiseren?

In reactie op de vraag van de CDA-fractie wordt opgemerkt dat in geval van zwaarwegende redenen zal worden besloten om een vergunning in te trekken. Hiervan is sprake in geval ernstig gevaar bestaat voor de cyberveiligheid of staatsveiligheid of in geval ernstig gevaar bestaat dat de erkenning mede zal worden gebruikt om strafbare feiten te plegen of uit strafbare feiten verkregen of te verkrijgen voordelen te benutten of anderszins de betrouwbaarheid en veiligheid van het Nederlandse stelsel voor elektronische dienstverlening in gevaar komt. In dat geval zal ik niet aarzelen om een vergunning van een middel in te trekken. Uiteraard zal ik hierbij bezien of een intrekking permanent moet zijn of dat een tijdelijke opschorting volstaat.

Welke effecten kan dit hebben voor de burgers en bedrijven die juist van dat inlogmiddel gebruikmaken?

Het effect voor burgers en bedrijven hiervan is dat een middel (eventueel tijdelijk) niet meer gebruikt kan worden. Ik realiseer mij daarbij dat dit voor burgers en bedrijven ongemak kan veroorzaken, echter dit weegt in dergelijke gevallen – ook voor hen – op tegen blootstelling aan het risico dat aan continuering van het middel kleeft.

Wat is hiertoe de aanpak en welke afspraken worden daartoe gemaakt met de geselecteerde aanbieders?

Partijen die een aanvraag tot erkenning van een inlogmiddel indienen zullen voorafgaand geïnformeerd worden over de voorwaarden die gelden en de over de mogelijkheid tot opschorten en intrekken van het inlogmiddel. (zie ook AMvB en MR burgermiddelen).

Hebben deze leden de memorie van antwoord goed begrepen dat als commerciële online-aanbieders ook van dit inlogmiddel gebruik willen maken, het verboden is om daarnaast een «eigen», meer commercieel inlogmiddel aan te bieden met aantrekkelijke voorwaarden voor de gebruikers, die hiervoor kiezen, waardoor er als het ware concurrentie tussen de inlogmiddelen ontstaat?

Het wetsvoorstel beperkt zich tot elektronische dienstverlening door (semi-)overheidsdienstverleners. Toegelaten private inlogmiddelen moeten hiervoor gebruikt kunnen worden. 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. Dit valt buiten de reikwijdte van het wetsvoorstel en buiten mijn verantwoordelijkheid.

4. Vragen en opmerkingen van de leden van de fracties van GroenLinks, de PvdA en de CU gezamenlijk (onder aansluiting van de leden van de fractie van 50Plus)

Gegevensverwerking door private partijen

Naast de gezamenlijke commissievragen zouden de leden van de fracties van GroenLinks, de PvdA en de CU nogmaals met de regering van gedachten willen wisselen over de fundamentele keuze van de regering om private aanbieders toe te laten met toegang en beschikking over

[3] Kamerstukken I, 2020/21, 34 972, L, p. 15.

persoonsgegevens van burgers. De leden van de fractie van 50Plus sluiten zich bij deze vragen aan. Twijfelt de regering weleens aan de gemaakte keuze van drie jaar geleden om dit mogelijk te maken? «Meer partijen biedt een voordeel voor wat betreft beschikbaarheid en het hebben van een terugvaloptie. Dat is een belangrijke reden geweest om te kiezen voor een open stelsel, waarbij meerdere middelen kunnen worden toegelaten, waaronder private», antwoordt de regering.[4] Kan de regering uitgebreider en puntsgewijs ingaan op de toegevoegde waarde van private aanbieders in het licht van de noodzakelijkheid, proportionaliteit en doelmatigheid?

Ik sta nog steeds achter de keuze die ik in 2018 heb gemaakt om naast het publieke middel DigiD ook private inlogmiddelen toe te laten. De redenen hiervoor die er destijds waren gelden onverminderd. Naast de terugvaloptie zorgt de komst van private middelen voor vitaliteit in het stelsel, omdat door concurrentie – binnen het strenge publiekrechtelijke kader waarmee de overheid op veiligheid en privacy stuurt en controleert – de prikkel naar vernieuwing en daarmee de inzet van steeds betere beschermingsmethoden (innovatie) wordt aangejaagd. Bovendien zorgt de aanwezigheid van meerdere middelen gezamenlijk voor het sneller bereiken van een grotere dekkingsgraad van middelen met een hogere betrouwbaarheid.

Heeft de regering overwogen om zelf een tweede systeem te (laten) ontwikkelen? Zo nee, waarom niet?

Er is niet overwogen zelf een tweede systeem te ontwikkelen. Onderdeel van de *fall back* is ook dat er verschillende systemen en verschillende beherende organisaties zijn. Die diversiteit maakt dat als er één (type) systeem onbeschikbaar raakt (bijvoorbeeld door een veiligheidslek), niet direct alle terugvalopties met hetzelfde probleem te maken hebben.

De regering geeft aan dat tijdens marktconsultaties met private partijen grote variëteit bestaat aan aanbieders, waarbij het vooral kleinere innovatieve bedrijven zijn die zich toeleggen op het aanbieden van betrouwbare authenticatie, en dat derhalve niet als een bijproduct, maar als «core business« zien. Met welke partijen heeft de regering allemaal gesproken tijdens de marktconsultaties en wat is hiervan de invloed geweest op de inhoud van de wet?

De marktconsultaties waren voor eenieder toegankelijk. Betrokken waren zowel grote als kleinere partijen die ofwel actief zijn op de markt voor inlogmiddelen of daar voornemens toe hebben. Daarbij gaat het om partijen uit op dit moment reeds middelen aanbieden binnen eHerkenning, om partijen uit banken- en telecomsector maar ook om innovatieve start ups. Deze marktconsultaties heeft de regering gebruikt om zich een beeld te vormen van het praktisch aanbod aan inlogmiddelen, de verschillende (technische en functionele) oplossingsrichtingen en toepassing. En aldus een inschatting te kunnen maken van de mogelijkheid en uitvoerbaarheid om met meerdere aanbieders te kunnen werken en de regels techniek-neutraal te kunnen formuleren en geen oplossingen uit te sluiten. De marktconsultaties hebben geen invloed de inhoud van de aan partijen gestelde toelatingseisen, daar deze voorvloeien uit de eIDAS-verordering, de AVG en nationale privacyregels.

De regering bevestigt dat de keuze voor private aanbieders betekent dat zij meer moet investeren in onderhoud en toezicht.[5] Kan de regering schetsen wat hiervoor voor nodig is van overheidswege? Hoeveel kosten

[4] Kamerstukken I, 2020/21, 34 972, L, p. 37.
[5] Kamerstukken I, 2020/21, 34 972, L, p. 37.

deze inspanningen? De regering zegt dat de extra inspanningen gerechtvaardigd zijn omdat de private middelen zich niet alleen uitstrekken tot het overheidsdomein maar ook tot het commerciële domein. Op basis waarvan is vastgesteld dat hier behoefte aan en noodzaak voor was vanuit de burger? Is er naast marktpartijen ook voorafgaand met andere organisaties gesproken en zo ja, met wie allemaal? De regering geeft aan dat burgers juist beter worden beschermd dankzij de private aanbieders, omdat zij nu buiten het publieke domein deze sleutels kunnen gebruiken.[6] Kan de regering dit nader toelichten? Hoe beoordeelt de regering het risico voor burgers die bij één partij een inlogmiddel voor alle diensten gaan gebruiken met alle persoonsgegevens van de desbetreffende persoon? Hoe beoordeelt de regering het risico van hacks en aanvallen, ook in verhouding tot de veronderstelde winst van beschikbaarheid? Zorgen van de leden over de grootte van ons zogenoemde «aanvalsoppervlak» -dat beduidend groter wordt door het toelaten van private aanbieders- tracht de regering weg te nemen door te benadrukken dat alle partijen voorafgaand aan toelating worden onderworpen aan strenge controles en toezicht. Hoe zit dat met partijen die al door andere lidstaten zijn goedgekeurd?

Het werken met meerdere partijen betekent dat meer inspanning geleverd moet worden op te zorgen dat partijen kunnen samenwerken binnen de gestelde kaders van de WDO. Dat zelfde geldt voor monitoring en toezicht. Meer partijen controleren betekent meer inspanning. De kosten zullen mede afhangen van de hoeveelheid partijen die zich voor toelating aanmeldt. Dat is niet op voorhand te bepalen. Het feit dat private middelen ook buiten het overheidsdomein te gebruiken zijn, betekent dat burgers en bedrijven ook bij commerciële dienstverleners gebruik kunnen maken van hun door de overheid gecontroleerde en goedgekeurde inlogmiddelen. Hierdoor is het maatschappelijke profijt groter dan veilige toegang tot de overheid alleen. In dat licht ziet de regering haar inspanningen als gerechtvaardigd. Vanuit de praktijk (webwinkels (thuiswinkel.org) en deskundigen (cybersecurityraad) wordt al langere tijd gepleit voor een rol van de overheid in het private domein.

Het feit dat er meerdere inlogmiddelen komen kan juist bijdragen aan het feit dat burgers niet voor alle diensten één sleutel gebruiken, maar kunnen kiezen en variëren. Ten aanzien van het aanvalsoppervlak het volgende. Enerzijds kan betoogd worden dat meerdere middelen het aanvalsoppervlak groter maken. Anderzijds wijzen de leden op het risico van de beschikbaarheid van een enkel middel. Het is belangrijk daar een middenweg in te kiezen. Daarbij speekt het voor zich dat de veiligheidsmaatregelen die worden getroffen moeten zijn toegerust op de dreigingen die er bestaan. Dat zal niet statisch zijn, maar net als de dreigingen zelf veranderen en constant moeten meegroeien.

Lagere regelgeving

De regering schrijft op pagina 2 van de memorie van antwoord dat alleen de hoofdelementen in beginsel opname in de wet behoeven. Mogen deze leden concluderen dat de regering elementen als informatieveiligheid, het beheer van de infrastructuur, de toelating en erkenning van de aanbieders, de rechten en plichten die zij hebben, het beschermen van persoonsgegevens en het doorberekenen van kosten géén hoofdelementen vindt?

---

[6] Kamerstukken I, 2020/21, 34 972, L, p. 28.

De regering schrijft: «De heer van Lochem concludeerde tijdens de deskundigenbijeenkomst van 30 juni jl. dat bij dit type wetgeving, dat op het terrein ligt van technologie en innovatie, de argumenten om daarin behoorlijk wat te delegeren, voor minstens een flink deel wel valide zijn. Hij adviseerde uw Kamer er minder op aan te dringen om toch nog zoveel mogelijk in de wet onder te brengen, maar wat meer dan normaal mee te kijken met de uitvoerende regelgeving en als Kamer vinger aan de pols te houden. In aansluiting daarop merk ik op, dat om die reden het wetsvoorstel voorziet in (zware) voorhang bij het parlement, waardoor van gecontroleerde delegatie sprake is.»[7] Tijdens de deskundigenbijeenkomst in de Eerste Kamer op 30 juni 2020 waren er ook diverse deskundigen (een meerderheid) die juist kritischer waren op deze keuzen van het kabinet. Zou de regering, net als bij de heer Van Lochem, in aansluiting op die andere deskundigen haar appreciatie willen geven van de mate van delegatie naar lagere regelgeving? En zou de regering in de memorie van antwoord van pagina 3 tot 7, waar zij op verzoek van diverse partijen per artikel aangeeft of het in de wet, per AMvB of ministeriële regeling wordt geregeld, hierbij ook de argumentatie per artikel kunnen toelichten op de elementen waar ook subdelegatie («bij of krachtens algemene maatregel van bestuur») is toegestaan? De Raad van State wees ook duidelijk op dit punt in relatie tot centrale onderdelen van de generieke digitale infrastructuur (GDI).[8] Kan de regering dit ook betrekken in haar antwoord?

In reactie op de vragen van de leden van de fracties van GroenLinks, de PvdA en de CU gezamenlijk (onder aansluiting van de leden van de fractie van 50Plus) wordt opgemerkt dat informatieveiligheid, het beheer van de generieke digitale infrastructuur, de toelating en erkenning van de aanbieders, het beschermen van persoonsgegevens en het doorberekenen van kosten wel degelijk als hoofdelementen worden beschouwd, aangezien deze behoren tot de voornaamste duurzame normen van de materie. Om die reden zijn deze onderwerpen in het wetsvoorstel zelf verankerd. Dat op onderdelen nadere uitwerking in lagere regelgeving plaatsvindt, doet hieraan niet af. De mate waarin delegatie en subdelegatie wordt voorgesteld, is volledig in lijn met het uitgangspunt van het primaat van de wetgever. Ingevolge dit uitgangspunt behoeven namelijk niet alle normen in een formele wet te worden opgenomen, maar is delegatie toegestaan – soms zelfs aangewezen – ter uitwerking van de hoofdelementen. In casu geschiedt dit met name in AMvB's, die bij uw kamer worden voorgehangen (gecontroleerde delegatie). Er worden slechts enkele ministeriële regelingen voorzien, primair de Regeling nadere eisen toelating identificatiemiddelen (op basis van de artikelen 9, 11, 13, 20 en 22 van het wetsvoorstel) en de Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening (op basis van artikel 6 van het wetsvoorstel). Reden hiervoor is dat het voorschriften betreft van administratieve aard, de uitwerking van (technische en organisatorische) details en de verwerking van uit de Europese eIDAS-verordening voortvloeiende eisen die geen ruimte laten voor het maken van keuzen van beleidsinhoudelijke aard.

In lijn met het advies van de Afdeling advisering van de Raad van State bevat het wetsvoorstel de taken, verantwoordelijkheden en functionaliteiten met betrekking tot een aantal belangrijke voorzieningen van de generieke digitale infrastructuur (de centrale onderdelen), waarbij concretisering en uitwerking bij lagere regelgeving plaatsvindt. De grondslagen hiervoor worden in artikel 5 van het wetsvoorstel ingekaderd en begrensd. Zo is de taak van de Minister van BZK voor de uitgifte van publieke identificatiemiddelen wettelijk verankerd in het eerste lid, onder

[7] Kamerstukken I, 2020/21, 34 972, L, p. 10.
[8] Kamerstukken II, 2017/18, 34 972, nr. 4.

a, van het wetsvoorstel en nader uitgewerkt in twee voorgenomen AMvB's, te weten het Besluit digitale overheid (voor wat betreft de bescherming van persoonsgegevens) en het Besluit identificatiemiddelen voor natuurlijke personen WDO (voor wat betreft de eisen waaraan publieke middelen moeten voldoen).

Toezicht

De Autoriteit Persoonsgegevens (AP) zal toezicht houden op de uitvoering van de Wet Digitale Overheid en vormt daarmee een belangrijke pijler rondom de handhaafbaarheid. Is de regering het met deze leden eens dat dit een verzwaring zal betekenen voor werkdruk van de AP? Is zij bereid de AP financieel meer te ondersteunen? De toezichthouder Agentschap Telecom (AT) heeft aangegeven dat harmonisatie van de domeinen burgers en bedrijven vanuit oogpunt van uitvoerbaarheid en handhaafbaarheid wenselijk is. Hoewel het momenteel werkbaar wordt geacht, is het niet wenselijk, zo blijkt uit het verhaal van de toezichthouder. Kan de regering het proces van harmonisatie schetsen in tijd en inhoud?

In reactie op de vragen van de leden van de fracties van GroenLinks, de PvdA en de CU gezamenlijk (onder aansluiting van de leden van de fractie van 50Plus) kan ik bevestigen dat de AP een van de instanties is die een toezichtstaak heeft terzake van de Wdo. Dit betekent een verzwaring van de werkdruk. In lijn met het kabinetsbeleid (Kamerstukken 2020–2021, 25 268, nr. 192) zal middels een uitvoeringstoets inzichtelijk worden gemaakt wat de financiële gevolgen zijn van de nieuwe wettelijke taak voor de AP en zal de financiële dekking worden geregeld.

In reactie op de wens van toezichthouder AT tot harmonisatie van de domeinen burgers en bedrijven, merk ik op deze wens te onderschrijven. Ik ben voornemens dit te realiseren in de tweede tranche van de Wdo, welk wetsvoorstel naar verwachting de komende kabinetsperiode zal worden ingediend. Harmonisatie behoeft naar aard en inhoud – mede vanuit een oogpunt van uitvoerbaarheid en handhaafbaarheid – de nodige voorbereiding, omdat de bestaande regimes voor burgers en bedrijven op onderdelen (juridisch en technisch) essentieel van elkaar verschillen. Met name het feit, dat inlogmiddelen voor burgers op basis van BSN functioneren en tot op heden alleen publiek worden aangeboden en inlogmiddelen voor bedrijven niet, maakt dat het naar elkaar toe brengen van systemen tijd en aandacht vergt.

Toekomstig beleid

De regering geeft aan dat in de toekomst (met tranches) «wordt gedacht over verbetering van de persoonlijke informatiepositie van burgers (regie op gegevens), een door de overheid gevalideerde online identiteit die breed bruikbaar is – dat wil zeggen voor het afnemen van diensten bij publieke en private (commerciële) organisaties –, het verder integreren van het burger- en bedrijvendomein, bredere toepassing van standaarden voor digitale dienstverlening en machtigen. Over deze onderwerpen vindt de gedachtenvorming momenteel volop plaats.»[9] Betreft dit slechts voorbeelden waarover wordt nagedacht of zijn er meer onderwerpen in de gedachtenvorming? Hoe ziet deze gedachtenvorming eruit? Wie is hierbij betrokken? Deze leden zouden graag een schets krijgen van de gedachtenvorming die volop gaande is. In hoeverre houdt dit verband met de aanstaande novelle?

[9] Kamerstukken I, 2020/21, 34 972, L, p. 13.

In reactie op de vragen van de leden van de fracties van GroenLinks, de PvdA en de CU gezamenlijk (onder aansluiting van de leden van de fractie van 50Plus) wordt opgemerkt dat de genoemde onderwerpen, alsmede het gebruik van basisregistraties, een plek zullen krijgen in de volgende tranche van de Wdo; op dit moment worden geen andere onderwerpen voorzien. De gedachtenvorming vindt multidisciplinair plaats, dat wil zeggen dat de voorbereiding in nauwe samenwerking tussen beleid, wetgeving en uitvoering plaatsvindt. De voorbereiding van de tweede tranche Wdo staat los van de novelle, die betrekking heeft op de voorliggende, eerste, tranche Wdo.

De regering schrijft dat België Wdo-achtige wetten kent. Deze leden vragen naar aanleiding van de antwoorden om een casusschets van de situatie in België. Waarom stelt de regering dat België dergelijke wetgeving kent? Welke overeenkomsten zijn er en welke verschillen? Zou de regering hierbij specifiek kunnen ingaan op de rol die private aanbieders spelen op de Belgische markt? Wat gaat daar goed en wat kan er beter? Is er structurele samenwerking en/of uitwisseling?

In reactie op de vragen van de leden van de fracties van GroenLinks, de PvdA en de CU gezamenlijk (onder aansluiting van de leden van de fractie van 50Plus) wordt opgemerkt dat in België diverse wetten en regelingen inzake de elektronische identiteitskaart kent.[10] Het Belgische systeem voorziet, evenals het Nederlandse stelsel, in identificatie en authenticatie van burgers en bedrijven door publieke en erkende private inlogmiddelen. In België kunnen met eID overheidsdiensten worden afgenomen, maar kan het ook voor commerciële diensten worden gebruikt bijvoorbeeld voor toegang tot webshops, casino's etc. Er is momenteel, naast de van overheidswege (door gemeenten) uitgegeven e-kaart, sprake van een erkende private aanbieder: Itsme, een initiatief van een aantal banken in samenwerking (consortium) met providers en de federale overheid. Itsme heeft ruim twee miljoen gebruikers, kost enkele euro's en is genotificeerd bij de EU-Commissie op betrouwbaarheidsniveau hoog en daarmee compliant met eIDAS. Samen met de publieke e-kaart – die, evenals de Nederlandse eNIK, ook ID en reisdocument is – is sprake van een ruim bereik; met beide zijn de ervaringen goed.

5. Vragen en opmerkingen van de leden van de D66-fractie

Gegevensverwerking door private partijen

Deze leden zijn verheugd dat wettelijk zal worden vastgelegd dat partijen gegevens niet mogen verwerken voor andere doeleinden dan vervaardiging en werking van het inlogmiddel. Er is natuurlijk, zoals de regering zelf ook aangeeft, een verschil tussen gebruikers- en gebruiksgegevens. De regering stelt in de memorie van antwoord dat «persoonsgegevens» niet commercieel uitgenut mogen worden, niet gebruikt mogen worden voor profilering en niet verhandeld mogen worden.[11] Deze leden zouden graag een bevestiging ontvangen dat deze «persoonsgegevens» zowel gebruikers- als (alle denkbare vormen van) gebruiksgegevens omvatten.

In reactie op de vraag van de leden van de fractie van D66 merk ik op dat het bij persoonsgegevens om alle persoonsgegevens gaat: gebruiks- en gebruikersgegevens en eventuele andere categorieën persoonsgegevens die verwerkt worden. Voor al deze gegevens geldt dat zij niet gebruikt mogen worden voor andere doeleinden dan de vervaardiging en werking van het inlogmiddel.

---

[10] Zie voor een overzicht Wetgeving – eID – IBZ Instellingen en Bevolking (fgov.be).
[11] Kamerstukken I, 2020/21, 34 972, L, o.a. p. 11.

Toezicht

De leden van de D66-fractie blijven daarnaast zorgen houden over de facilitering van toezichthouders. De regering geeft aan dat alle partijen die inlogmiddelen willen aanbieden alle vereisten aantoonbaar moeten naleven. Hier wordt zowel voorafgaand aan toelating op gecontroleerd als ook gedurende hun dienstverlening. Het Agentschap Telecom (AT) en (voor aspecten aangaande de bescherming van persoonsgegevens) de Autoriteit Persoonsgegevens (AP) houden toezicht en handhaven. Deze leden zijn ervan overtuigd dat sterk toezicht essentieel is. Zij begrijpen dat de AP zelf haar prioriteiten bepaalt en dat de regering hier dus geen uitspraken over kan doen, maar als de toegekende middelen simpelweg niet toereikend zijn, zal toezicht tekortschieten. Op dit moment kan de AP al maar slechts bij een deel van alle gemelde datalekken in actie komen door een tekort aan budget[12]. In de Tweede Kamer is recentelijk een motie aangenomen over verhoging van het budget van de AP[13] waar Minister Dekker o.a. op antwoordde[14] dat het niet aan het demissionaire kabinet is om ongedekte moties uit te voeren. De leden van de D66-fractie hebben hier begrip voor, maar vragen zich sterk af of het geen recept voor ongelukken is om deze wet aan te nemen zonder dat de facilitering van de toezichthouders gewaarborgd is – sterker nog, terwijl we weten dat de facilitering van de AP op dit moment niet afdoende is.

In reactie op de vraag van de leden van de fractie van D66 verwijs ik kortheidshalve naar hetgeen over toezicht door AP is opgemerkt bij punt 4, in reactie op de vragen van de leden van de fracties van GroenLinks, de PvdA en de CU gezamenlijk (onder aansluiting van de leden van de fractie van 50Plus).

Closed source

De leden van de D66-fractie vinden het goed dat aan open source zal worden getoetst bij het behandelen van een toelatingsaanvraag, omdat open source het uitgangspunt zou moeten zijn. Volgens de memorie van antwoord is het echter denkbaar dat closed source software ook aan de orde zal komen, vanwege de mogelijke veiligheidsargumenten die de regering aanhaalt in haar beantwoording. De regering stelt dat er in zo'n geval «nadrukkelijk door anderen dan de leverancier zelf» zal moeten worden vastgesteld dat de closed software werkt zoals beschreven en veilig is. Deze leden vragen zich af wie deze «anderen» zullen zijn. Zal dit ook worden getoetst door het Agentschap Telecom?

In reactie op de vraag van de leden van de fractie van D66 merk ik op, dat bij de toetsing van de toelatingsaanvraag het van belang is dat een onafhankelijke oordeel wordt verkregen, waarin wordt vastgesteld dat er gegronde redenen zijn om closed source in te zetten. Een voorbeeld daarvan is hiervoor aangehaald ten aanzien van de monitoring ter bescherming van burgers en bedrijven tegen fraude en misbruik. Bij de toelating (erkenning) zal ook het Agentschap Telecom zich een oordeel vellen over de aangevoerde redenen.

---

[12] Zie bijvoorbeeld Trouw (1 maart 2021): *Datadiefstal is explosief gegroeid. Het gevaar? «Mensen kunnen al hun spaargeld kwijtraken»* https://www.trouw.nl/binnenland/datadiefstal-is-explosief-gegroeid-het-gevaar-mensen-kunnen-al-hun-spaargeld-kwijtraken~b1e95096/.

[13] Motie van het lid Hijink c.s. over verhoging van het budget van de Autoriteit Persoonsgegevens, Kamerstukken II, 2020/21, 27 529 nr. 240.

[14] Kamerstukken II, 2020/21, 25 268/32 761, nr. 197.

6. Vragen en opmerkingen van de leden van de PVV-fractie

Open source – closed source

De regering geeft in de memorie van antwoord enerzijds aan in te willen zetten op open source, maar geeft tegelijkertijd aan op pagina 19: «De eigenschap open source als zodanig biedt niet de garantie voor transparantie en veiligheid» en op pagina 22: «Open source software die niet actief ondersteund en onderhouden wordt kan dan zelfs een veiligheidsrisico worden in plaats van een veiligheidsmaatregel.» Kan de regering verduidelijken welke concrete eisen gesteld zullen worden aan open source en welke vormen van open source licenties er toegestaan zullen worden en/of op basis van welke criteria open source licenties beoordeeld zullen worden voor toelating? Kan de regering aangeven welke criteria gehanteerd zullen worden ten aanzien van het actief ondersteunen en onderhouden van open source software?

In reactie op de vraag van de leden van de fractie van de PVV ten aanzien van de licentievormen verwijs ik kortheidshalve naar hetgeen over open source is opgemerkt bij punt 2. Ten aanzien van actief onderhoud en ondersteuning zal bepalend zijn of zekerheid kan worden verkregen dan wel kan worden geboden over de betrouwbaarheid en veiligheid van de software, en dat een organisatie daarop aanspreekbaar kan zijn. Eventuele problemen dienen snel en adequaat te worden opgelost. Het (maatschappelijk) belang daarvan is zeker bij breed gebruik, immers groot. Het zal daarbij gaan op soortgelijke eisen die ook aan aanbieders van closed source worden gesteld.

Verder geeft de regering aan de beweging naar open source in te zetten in een transitieproces; kan de regering verduidelijken welke stappen in deze «beweging naar open source» concreet gezet zullen gaan worden, op basis van welke criteria en indicatoren en wat de termijn van dit transitieproces wordt?
Daarnaast geeft de regering aan in voorkomende gevallen voor closed source te kiezen, omdat veiligheid met open source niet gegarandeerd kan worden. Kan de regering concreet aangeven op basis van welke criteria deze gevallen bepaald zullen worden en bij wie deze bevoegdheid komt te liggen? Kan de regering tevens aangeven in hoeverre in dergelijke gevallen alsnog tot open source oplossingen kan worden overgegaan indien de veiligheid wel gewaarborgd kan worden en of hier (periodiek) op getoetst zal worden?

In reactie op de vraag van de leden van de fractie van de PVV verwijs ik kortheidshalve naar hetgeen over open source is opgemerkt bij punt 2. Bij een aanvraag van een private partij om toelating (erkenning) is open source het uitgangspunt. De bevoegdheid tot behandeling en besluitvorming inzake aanvragen om een erkenning ligt bij de Minister van BZK. Een erkenning wordt door mij geweigerd indien de aanvragende partij onvoldoende gebruik maakt van open source software.
Ik zal een reeds verleende erkenning die gebaseerd was op closed source, wijzigen, schorsen of intrekken wanneer open source redelijkerwijs beschikbaar is geworden. De betreffende partij zal dan alsnog tot open source moeten overgaan.

Ten aanzien van de criteria die worden gehanteerd om te bepalen of open source redelijkerwijs beschikbaar is geldt dat, zoals ik hierboven ten aanzien van het beheer en onderhoud aangaf, bepalend zal zijn of zekerheid kan worden verkregen dan wel kan worden geboden over de betrouwbaarheid en veiligheid van de software, en dat een organisatie daarop aanspreekbaar kan zijn. Eventuele problemen dienen snel en

adequaat te worden opgelost. Het (maatschappelijk) belang moet worden geborgd. Daar bij geldt dat in het algemeen steeds meer software open source, voor meer functionaliteiten beschikbaar komt met deze achterliggende zekerheid. Dat is waar periodiek op zal worden getoetst. Daarbij geldt: als voor een betreffende functionaliteit software open source met geboden zekerheid ter beschikking is, daarvoor dient te worden gekozen. De verwachting is dat dit in de tijd zal toenemen, waardoor de beweging naar open source gestalte zal krijgen.

Veiligheid, privacy by design

Kan de regering aangeven op welke wijze risico's op (grootschalige) hacks ondervangen zullen worden als gekozen wordt voor centrale oplossingen?

In reactie op de vraag van de leden van de fractie van de PVV verwijs ik kortheidshalve naar hetgeen over hacks in relatie tot centrale – decentrale opslag is opgemerkt bij punt 2.

Kan de regering tevens nader ingaan wat de ervaringen hiermee zijn bij bestaande systemen, zoals de elektronische patiëntengegevens? Zo concludeert een rapport van de Autoriteit Persoonsgegevens (AP) over toegang tot digitale persoonsgegevens in het HagaZiekenhuis: «De AP constateert dat het Haga Ziekenhuis onvoldoende passende maatregelen heeft getroffen ten aanzien van de beveiligingsaspecten «authenticatie» en «controle van de logging». Het Haga Ziekenhuis handelt hierdoor in strijd met artikel 32, eerste lid, aanhef, van de AVG.»[15]

In reactie op de vraag van de leden van de fractie van de PVV kan ik melden, dat het door het Haga gebruikte systeem geen centraal systeem is. Voorts is van belang op te merken dat het Haga een private instantie is. Op het punt van onder meer informatiebeveiliging valt het Haga dus niet onder overheidsverantwoordelijkheid. Ik volsta ermee hier te benadrukken dat het Haga gehouden is de AVG na te leven.

Kan de regering concreet aangeven hoe de beveiligingsaspecten authenticatie en controle van logging binnen de kaders van dit wetsvoorstel worden geregeld? Kan de regering meer specifiek aangeven welke privacy by design-middelen zij wil verplichten en of het hierbij gaat om het loggen van middelen waarbij gebruikers inloggen, of loggen zij ook de specifieke persoonsgegevens waarmee wordt ingelogd?

In reactie op de vragen van de leden van de fractie van de PVV merk ik op dat informatiebeveiliging en verwerking van persoonsgegevens worden gereguleerd in het Besluit digitale overheid. Deze AMvB, waarin te nemen maatregelen zoveel mogelijk functioneel worden voorgeschreven, hangt momenteel bij uw kamer voor. Meer specifiek wordt onder meer tot versleutelingsmethodes verplicht, waardoor het bsn niet meer direct herleidbaar is. De specifieke persoonsgegeven, dat wil zeggen de attributen die aan een overheidsdienstverlener worden verstrekt worden niet gelogd. Ook wordt verplicht tot gescheiden opslag van gebruiks- en gebruikersgegevens. Dit laat overigens onverlet dat ook andere privacybeschermende maatregelen kunnen worden toegepast.

Zoals ik eerder aangaf is het nodig om burgers die in de problemen komen te kunnen helpen. Daarvoor is het nodig dat gegevens worden gelogd en worden gecontroleerd, zodat problemen zoveel mogelijk

---

[15] Autoriteit Persoonsgegevens, Toegang tot digitale patiëntdossiers door medewerkers van het HagaZiekenhuis, Onderzoeksrapport maart 2019, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/haga_rapport_def.pdf.

kunnen worden voorkomen of snel hersteld kunnen worden. Dit vormt het herstelvermogen. De wijze waarop dat plaatsvindt en de verwerkingen die daarvoor plaatsvinden dienen onverkort aan de AVG te voldoen. In de WDO en het besluit digitale overheid is dat nadrukkelijk ingekaderd. Zo zijn de doeleinden, verstrekkingsmogelijkheden en bewaartermijnen nauwkeurig omschreven.

Voorts heeft SIDN aangegeven dat onduidelijk is wat de technische veiligheidsrichtlijnen in dit kader zijn. Kan de regering aangeven of deze gegevens versleuteld zijn en apart opgeslagen ten behoeve van functiescheiding? Gaat het om het bijhouden van welke gebruiker waar op welk moment inlogt, of moet door de aanbieder van een inlogmiddel ook geregistreerd worden welke persoonsgegevens bij dat inloggen onthuld worden? Moeten deze loggegevens versleuteld worden, niet alleen als bescherming bij eventuele aanvallen, maar ook ter bekrachtiging van de vereiste functiescheiding (persoonsgegevens/gebruikersgedrag)?

In aansluiting op het voorgaande geldt dat de voorschriften in het kader van monitoring en logging niet anders zijn dan voor andere verwerkingen van persoonsgegevens binnen het stelsel. Zo wordt niet bijgehouden welke gegevens door een gebruiker worden verstrekt, maar wel op welk moment waar wordt ingelogd, om ingeval de gebruiker problemen ondervindt hem te kunnen helpen. Voorts gelden ook voorschriften als functiescheiding en gescheiden opslag, en dat gegevens waar mogelijk versleuteld worden opgeslagen. Ik wijs er voor de volledigheid nog op dat voor mij bepalend is dat een adequaat beschermingsniveau van persoonsgegevens wordt bereikt. Kern is dat de AVG wordt nageleefd, en dat kan op verschillende wijzen. Dat betreft implementatie, waarbij meerdere maatregelen mogelijk zijn. Deze implementatieopdracht is breder dan enkel de vraag welke techniek wordt gebruikt of de wijze waarop gegevens zijn opgeslagen.

eID op Europees niveau en in andere landen

De EU werkt momenteel aan de introductie van een eID op Europees niveau. Kan de regering aangeven hoe dit wetsvoorstel zich verhoudt tot de introductie van de eID en in hoeverre er al rekening wordt gehouden met interoperabiliteit? Acht de regering een dergelijke eID wenselijk? Kan de regering bovendien aangeven wat de introductie van een eID betekent voor de persoonsgegevens van Nederlandse burgers en in hoeverre de EU hier over zou kunnen beschikken?

De Noordse en Baltische staten hebben in het kader van het NOBID-project een Nordic-Baltic eID ontwikkeld. Kan de regering aangeven in hoeverre de plannen voor de Wdo vergelijkbaar zijn met dit project?

In reactie op de vragen van de leden van de fractie van de PVV, merk ik op dat de EU een wijziging van de zgh. eIDAS-verordening voorbereidt. Naar verwachting presenteert de Europese Commissie eind mei van dit jaar haar voorstel en wordt er geen Europees eID geïntroduceerd. Het voorstel beoogt verbetering van de effectiviteit van de huidige verordening, waarbij interoperabiliteit een belangrijk aspect is. Zie ook hetgeen bij punt 2 is opgemerkt. Nadat het voorstel is gepubliceerd, zal de regering haar standpunt formuleren in het BNC-fiche. Het wetsvoorstel sluit aan bij de huidige en komende EU-wetgeving. Zo zijn de toelatingseisen terzake van (publieke en private) inlogmiddelen gebaseerd op de eIDAS-eisen. De verwerking en beveiliging van persoonsgegevens voor de identificatie terzake van grensoverschrijdende elektronische dienstverlening binnen de EU, die plaatsvindt door tussenkomst van de zgh. eIDAS-voorziening

(artikel 5, leden 2 en 3, Wdo) wordt nader geregeld in het Besluit digitale overheid, dat bij uw kamer is voorgehangen.

De ontwikkeling van een Nordic-Baltic eID behelst de implementatie van de eIDAS-verordening in de Scandinavische en Baltische staten. Het wetsvoorstel Wdo sluit daar nauw bij aan.

7. Vragen en opmerkingen van de leden van de SP-fractie

Open source

Als eerste willen de leden van de SP-fractie opmerken dat de beantwoording in de memorie van antwoord niet altijd even consistent is. En al zijn deze leden blij dat de regering nu ook open source omarmt, conform het kabinetsbeleid, het is natuurlijk niet zo dat open source minder veilig is. Integendeel. Zeker is het zo dat open source onderhouden dient te worden, evenals alle andere software, en dat daar aandacht voor dient te zijn. Deze leden nemen aan dat dit meegenomen wordt in de verdere uitrol van de Wdo.

In reactie op de vraag van de leden van de fractie van de SP kan ik bevestigen dat beheer en onderhoud van alle software, gelet op de veiligheid en betrouwbaarheid van de toegang tot overheidsdiensten, wordt meegenomen bij de verdere uitrol van de Wdo.

Verheugd zijn de leden van de SP-fractie over de toezegging dat er een wetswijzing nodig is om open source, evenals privacy by design en een wettelijk verbod op verhandelen van gegevens te verankeren in de Wdo. Uit de memorie van antwoord was het deze leden niet duidelijk welke route bewandeld zou worden, inmiddels begrijpen zij dat hiertoe een novelle zal worden ingediend. Hoe de open source zal worden ingezet is nog vaag. Kan de regering ingaan op wat voor soort open source-licentie opgenomen gaat worden in de wetswijziging? En is de open source dan ook echt een vereiste voor toelating? Deze leden willen benadrukken dat dit laatste voor hen een belangrijk punt is.

In reactie op de vragen van de leden van de fractie van de SP verwijs ik kortheidshalve naar hetgeen over open source is opgemerkt bij punt 2. Voor wat betreft de licentievorm is de openbaarheid van de broncode relevant omdat die bepalend is voor transparantie en veiligheid door hantering van het «meer ogen» principe.

De leden van de SP-fractie begrijpen uit de beantwoording dat de regering streeft naar open source voor de aanbieders, maar onduidelijk is hoe het streven zijn beslag zal krijgen. Zij begrijpen dat de druk groot is van gevestigde bedrijven die van nature misschien niet allemaal gewend zijn om dit traject van open source in te gaan. Toch willen deze leden ervoor waken dat deze bedrijven een voorlopige toetreding krijgen, waarin ze met closed source kunnen beginnen. Een dergelijk stap zal er voor zorgen dat deze bedrijven ook de omschakeling in een latere fase zullen vertragen. Bovendien, wanneer deze bedrijven niets te verbergen hebben, dan hoeft men toch niet met closed software te beginnen? Deze leden vragen om een helder standpunt van de regering in dezen.

In reactie op de vragen van de leden van de fractie van de SP verwijs ik kortheidshalve naar hetgeen over open source is opgemerkt bij punt 2. Hierbij zij opgemerkt dat niet de belangen van gevestigde bedrijven leidend zijn, maar de belangen van burgers en bedrijven voor wie continuïteit van middelen essentieel is. Voorts benadruk ik dat bij een aanvraag van een private partij om toelating (erkenning) open source het

uitgangspunt is. Ook bepaalt het wetsvoorstel dat erkende middelenaanbieders de omschakeling naar open source moeten maken wanneer dit redelijkerwijs beschikbaar is.

Decentraal en centraal

De regering geeft in de beantwoording aan niet te willen afdwingen dat de gegevens decentraal worden opgeslagen. De argumenten die zij hiervoor aandraagt, liggen met name in de uitvoering: problemen oplossen met gebruikers is lastiger als alles decentraal is opgeslagen. Tegelijkertijd is decentraal wel de trend, zo constateren de leden van de fractie van de SP. Deze leden begrijpen echter de denkrichting van de regering, maar zouden ervoor willen pleiten om wettelijk af te dwingen dat de gebruikersgegevens wel decentraal moeten worden opgeslagen. Daarmee wordt de kans op het stelen van gevoelige gegevens aanmerkelijk verkleind.

In reactie op de vraag van de leden van de fractie van de SP merk ik op dat in de huidige opzet, behalve een versleuteld burgerservicenummer, geen inhoudelijke gebruikersgegevens worden opgeslagen. Overige gebruikersgegevens die mogelijk voor het verwerven en gebruik van een inlogmiddel op basis van toestemming van de gebruiker worden verwerkt, worden verwerkt voor administratieve doeleinden (denk aan NAW-gegevens en contactgegevens zoals een e-mailadres). Deze gegevens kunnen door een aanbieder van een inlogmiddel worden opgeslagen, maar moeten dan worden gescheiden van de gegevens die gegenereerd worden door het gebruik (gebruiksgegevens, logging waaronder versleuteld bsn).

Privacy by design

Dan de toezegging om de principes van privacy by design in de wet op te nemen. Ook hierover zijn deze leden verheugd. Wel vragen zij zich af wat er precies opgenomen gaat worden. Kan de regering nader omschrijven welke elementen van privacy by design in de wet meegenomen gaan worden?

In reactie op de vraag van de leden van de fractie van de SP merk ik op dat het wetsvoorstel er in zal voorzien dat een erkenning (toelating) van een privaat inlogmiddel wordt geweigerd indien het ontwerp (design) onvoldoende voorziet in de bescherming van gegevens. Hierbij is de actuele stand van processen en technieken leidend. Ook wordt geborgd dat na verlening van een erkenning nieuwe technieken en processen door erkenninghouders worden geïmplementeerd.

Kenbaar maken van voornemens

De leden van de SP-fractie willen de regering vragen om over haar voornemens naar buiten toe helder te communiceren. Nog weinigen zijn op de hoogte van het voornemen om de wet op deze punten aan te scherpen, terwijl wel al een fors aantal partijen voorsorteren op de Wdo. Zo worden systemen van de apotheker aangesloten op een koppelvlak om aan de eisen van inloggen te voldoen. Ook zij moeten op de hoogte zijn van de nieuwe vereisten die in de wet gaan komen. Op welke wijze wil de regering dit kenbaar maken aan de betrokken partijen, zo vragen deze leden. Bovendien wordt door de vertraging ook de verplichting van HTTPS op overheidswebsites uitgesteld, evenals de toegankelijkheidseisen. Dit zou echter overheden er niet van moeten weerhouden hun websites veilig en toegankelijk te houden. Is de regering bereid om de overheden hier nogmaals op te wijzen?

In reactie op de vragen van de leden van de fractie van de SP, wordt opgemerkt dat kenbaarheid van het wetsvoorstel en van de novelle van elkaar moeten worden onderscheiden. Het wetsvoorstel en de voorgenomen AMvB's zijn sinds indiening respectievelijk voorhang bij het parlement openbaar en voor een ieder kenbaar en beschikbaar. Hierdoor zijn de stakeholders (burgers, publieke dienstverleners, private partijen, toezichthouders) geruime tijd in de gelegenheid zich op het nieuwe stelsel voor te bereiden. De novelle zal openbaar en breed toegankelijk zijn wanneer deze bij de Tweede Kamer wordt ingediend. Dit zal naar verwachting voor de zomer zijn. Deze voorgenomen wetswijziging behelst aanvulling van slechts enkele artikel(onderdel)en van de Wdo en is bovendien relevant voor een beperkte doelgroep, te weten (publieke en private) aanbieders van inlogmiddelen. Zij zullen door mij afzonderlijk op de hoogte worden gesteld, vanzelfsprekend onder voorbehoud van de parlementaire behandeling.

Vertraging van inwerkingtreding van de Wdo heeft, zo ben ik met uw kamer eens, tot gevolg dat de verplichte toepassing van HTTPS op overheidswebsites ook vertraging oploopt. De toepassing van open (veiligheids)standaarden, waartoe HTTPS behoort, is evenwel uitgangspunt voor en veelal reeds staande praktijk bij overheidsinstanties. Dit wordt door mij gemonitord. In dit verband zij gewezen op de brief van 18 maart 2021, waarin ik de Monitor Open Standaarden 2020 naar het parlement heb gestuurd als onderdeel van de rapportage over de voortgang van informatieveiligheid bij de overheid. Hieruit blijkt dat het gebruik van de open standaarden gestaag is toegenomen. De toepassing van toegankelijkheidseisen inzake overheidswebsites is sinds september 2020 verplicht, daar deze implementatie van EU-recht behelzen (Besluit digitale toegankelijkheid overheid, Stb. 2018, 141).

8. Vragen en opmerkingen van de leden van de ChristenUnie-fractie (onder aansluiting van de leden van de fractie van 50Plus)

Toegankelijkheid burgers

Een mogelijk gevaar van het gebruik van veilige middelen om elektronisch met de overheid en publieke diensten te communiceren is dat deze middelen niet toegankelijk zijn voor sommige burgers vanwege de kosten of vanwege het vereiste kennisniveau. Is de regering het eens met de leden van de fractie van de ChristenUnie, met aansluiting van de leden van de fractie van 50Plus, dat in principe elke burger toegang moet hebben tot de genoemde veilige middelen? Welke maatregelen neemt de regering om dit te realiseren?

In reactie op de vraag van de leden van de fractie van de ChristenUnie benadruk ik dat een primair doel van het onderhavige wetsvoorstel is dat elke burger toegang heeft tot veilige inlogmiddelen. De publieke middelen op de betrouwbaarheidsniveaus substantieel en hoog zullen tegen legeskosten te verkrijgen zijn, opdat hiermee laagdrempelig zaken kan worden gedaan met de overheid. Daarnaast kunnen private partijen inlogmiddelen aanbieden. Het staat hen vrij om zelf de prijs te bepalen voor het inlogmiddel dat zij aanbieden. Daar stel ik geen regels voor.

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