

Beantwoording door de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van de vragen van 16 juli 2021 van de vaste commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis van de Koning van de Eerste Kamer der Staten-Generaal naar aanleiding van het voorstel van de Europese Commissie voor een verordening inzake Europese digitale identiteit (COM(2021)281).

De leden van de **GroenLinks**-fractie vragen mij het risico te beoordelen dat private dienstverleners online overal de digitale identiteit op zullen vragen waar dat voorheen nog niet kon of op plaatsen waar in de offline wereld dit niet noodzakelijk wordt geacht. Deze leden vragen me tevens een oordeel te geven over de mate van bescherming van de privacy middels de hoogste standaarden voor cybersecurity.

Allereerst zijn noch het wetsvoorstel van de Commissie noch het wetsvoorstel digitale overheid (Wdo) bedoeld om grondslagen te bieden aan gegevensverwerkingen die nu niet noodzakelijk zijn. Gegevens mogen alleen verwerkt worden met inachtneming van de beginselen, zoals die inzake transparantie en doelbinding, op het terrein van de verwerking van persoonsgegevens op basis van de algemene verordening gegevensverwerking (AVG)¹ en aanvullende nationale wetgeving. Het risico bestaat altijd dat partijen gegevens verwerken op een wijze die niet is toegestaan, maar dit risico wordt door de voorgestelde voorschriften in het voorstel van de Commissie of in de Wdo niet groter of kleiner. Het voorstel van de Commissie beoogt juist, evenals de Wdo, met specifieke waarborgen te voorkomen dat elektronische identiteiten (eID's) en gegevens over personen en bedrijven oneigenlijk worden gebruikt.

Daarnaast is van belang dat in de uitwerking van de nieuwe Europese Digitale Identiteit (EDI) de voorschriften en standaarden worden opgenomen die borgen dat alle Europeanen digitale diensten veilig kunnen afnemen. Een betrouwbare koppeling met de nationale identiteit zoals door de overheid vastgelegd, is hierbij belangrijk. Dit noemen we de digitale bronidentiteit, zijnde een door de overheid uitgegeven, erkende en in de wet- en regelgeving verankerde, digitale identiteit voor gebruik in de publieke en private sector. Deze digitale bronidentiteit bevat een minimale set van identiteitsgegevens die nodig zijn in het maatschappelijk verkeer.² Burgers en ook bedrijven zouden, zoals de Commissie eveneens voorstelt, volledig inzicht en controle moeten hebben over de gegevens die ze delen. Gebruikers bepalen welke data met wie gedeeld worden en moeten vooraf geïnformeerd worden over de benodigde attributen en gegevens voor afname van een concrete dienst, die alleen gedeeld mogen worden als dit in overeenstemming is met nationaal recht en voor zover dit voor het gebruik van een bepaalde dienst nodig is. Aanbieders van digitale diensten en leveranciers van eID-middelen, zoals *'e-wallets'*, en van attributen mogen de gegevens van gebruikers niet combineren en aanwenden voor andere diensten. Ook verplicht het voorstel van de Commissie tot gescheiden opslag van gegevens en verbiedt het om de gegevens over de persoon of het bedrijf en de transacties te bewaren en te hergebruiken.

Tot slot dienen de eID's, bijvoorbeeld in de vorm van *'wallets'*, volgens het voorstel zelf beveiligd te zijn op het hoogste betrouwbaarheidsniveau. In het fiche is vermeld dat het kabinet bereid is om het idee van de Commissie te verkennen om certificering van Europees te erkennen eID's toe te laten onder de cyberbeveiligingsverordening³. Ook wil het kabinet het toezicht op aanbieders van middelen en gegevens en op dienstverleners in de publieke en private sector harmoniseren om

¹ Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

² Dit is verder toegelicht in de visiebrief digitale identiteit: Kamerstukken II, 2020/2021, 26643 nr. 743.

³ Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening).

de veiligheid en betrouwbaarheid van digitale dienstverlening en een gelijk speelveld binnen de interne markt te borgen. Tot slot is van cruciaal belang dat in de uitwerking van het voorstel en bij toekomstig gebruik van de Europese eID's de kennis van experts uit het domein van justitie, veiligheid en inlichtingen benut wordt om de veiligheid ervan zoveel mogelijk te borgen.

De leden van de GroenLinks-fractie vragen op welke onderdelen de voorstellen voor de Wdo eventueel moeten worden aangepast, zodat deze in lijn zijn met het voorstel van de Commissie, en vragen of onderdelen in het huidige voorstel voor de Wdo conflicteren met (de keuzes die zijn gemaakt binnen) het voorstel van de Commissie. De leden vragen mij tevens aan te geven welke keuzes die ik maak in de Wdo verschillen van de keuzes in het voorstel van de Commissie.

Het voorstel van de Commissie en het voorstel voor de Wdo zijn grotendeels in lijn met elkaar en conflicteren niet. Het voorstel van de Commissie regelt echter meer dan de voorgenomen eerste tranche van de Wdo en in dat opzicht verschillen beide voorstellen. In hoofdlijnen ziet het voorstel van de Commissie op meer functionaliteiten en heeft het een bredere reikwijdte. Daar waar de huidige eIDAS-verordening en in lijn daarmee de eerste tranche van de Wdo voorschriften bevat voor het veilig en betrouwbaar gebruik van eID's bij overheidsdiensten, regelt het voorstel van de Commissie het gebruik van eID's én attributen met een verplicht te introduceren *e-wallet* bij overheden én in de private sector onder regie van burgers en bedrijven.

Bij adoptie van dit voorstel zal de Wdo moeten worden aangevuld met voorschriften die nu beoogd zijn in de tweede tranche. In de Wdo dient opgenomen te worden een publiekrechtelijke systematiek voor toelating van één of meer *wallets*. Ook dient de acceptatieplicht voor eID's aangevuld te worden met de plicht om toegelaten *wallets* te accepteren bij online diensten. Daarnaast dient gebruik in het private domein gereguleerd te worden en dienen voorschriften opgenomen te worden in het kader van gegevensuitwisseling onder regie van burgers en bedrijven en voor de digitale bronidentiteit als minimale set van identiteitsgegevens in *wallets*. Tot slot zal bezien moeten worden hoe de voorgestelde nationale certificering van eID's door lidstaten zelf onder de Wdo geregeld kan worden en zal daarin het toezicht in het publieke en het private domein dienen te worden uitgewerkt. Ik doe dit in de tweede tranche van de Wdo, voortbouwend op het fundament dat hiervoor is gelegd in de eerste tranche. Ten overvloede merk ik op dat de Wdo, voor zover zij onderwerpen regelt die in de eIDAS-verordening zijn opgenomen, het karakter van een uitvoeringswet heeft.

De leden van de GroenLinks-fractie wijzen erop dat ik voornemens ben om in de tweede tranche van de Wdo de grondslag te verankeren voor het delen van gegevens in combinatie met een digitale bronidentiteit (voor de *wallet* waaraan 'attributen', zoals kwalificaties en bevoegdheden, gekoppeld kunnen worden). In het BNC-fiche bij het voorstel van de Commissie staat dat nationale uitvoeringsregelgeving nodig is vanwege de brede werkingssfeer van het voorstel. De leden vragen mij welke aanpassingen het betreft, die digitale transacties met nationale eID-middelen in het private domein mogelijk moeten maken, en welke verschillen er bestaan tussen de eerste tranche van de Wdo en de tweede tranche inzake gegevensuitwisseling onder regie van de burger. De leden vragen tevens op welke wijze maatregelen inzake inzage, correctie, bescherming van gebruikers, certificering, elektronische archivering, toezicht en handhaving zullen worden aangepast.

In de eerste tranche van de Wdo is een grondslag opgenomen voor de infrastructuur van de voorzieningen die het delen van, de inzage in en de correctie van gegevens – die de burger zelf betreffen – mogelijk maakt onder de regie van de burger. In de tweede tranche van de Wdo zal een dergelijke grondslag voor het delen van gegevens verder worden uitgewerkt in combinatie met de digitale bronidentiteit. Waar de eerste tranche ziet op het veilig inloggen, zal in de tweede tranche het veilig delen van gegevens – ook onder regie van burgers en bedrijven – in de Wdo meer centraal worden gezet. Welke aanpassingen precies gedaan moeten worden, zal afhankelijk zijn van de definitieve inhoud van de herziene verordening die uiteindelijk zal worden aangenomen.

Voor inzage, correctie en bescherming van gebruikers zijn geen specifieke aanpassingen in de Wdo nodig, omdat de rechten, regels en maatregelen daarvoor uit de AVG volgen. Wel is het zo dat in de Wdo eventueel voorzieningen moeten worden getroffen om burgers zo goed mogelijk in staat te stellen hun rechten ook daadwerkelijk te benutten, waarvoor het voorstel van de Commissie ook voorzieningen bevat. Voor de overige aspecten geldt dat de noodzaak om hiervoor nationale uitvoeringsregelgeving op te stellen zal moeten worden bezien op basis van de definitieve tekst van de verordening. Voor de volledigheid wordt opgemerkt dat elektronische archivering op dit moment buiten de reikwijdte van de Wdo valt.

De leden van de GroenLinks-fractie vragen mij specifiek in te gaan op de keuze voor het toelaten van private aanbieders en de verantwoordelijkheden die deze private aanbieders hebben.

Over de keuze om private aanbieders van inlogmiddelen toe te laten bestaat er geen verschil van inzicht met de Wdo. Ook het voorstel van de Commissie biedt de mogelijkheid om private aanbieders van inlogmiddelen toe te laten, zolang deze aanbieders voldoen aan de gestelde eisen, zoals die ten aanzien van privacy, betrouwbaarheid en veiligheid.

De leden van de GroenLinks-fractie vragen mij een oordeel te geven over de keuze van de Commissie om veel ruimte te laten aan lidstaten voor de ontwikkeling en benutting van de digitale identiteiten. De leden vragen me of ik het met hen eens ben dat als alle lidstaten een andere infrastructuur kiezen, deze niet of nauwelijks met elkaar zullen functioneren c.q. communiceren op de hoogste beveiligingsniveaus. De leden van GroenLinks-fractie zien de digitale identiteit die nu Europees wordt vormgegeven als het ware als een oprit naar de digitale snelweg, in dit geval de infrastructuur. In de optiek van de leden is het kwetsbaar als iedere oprit en snelweg van verschillende design is en er een andere controleur aanwezig is. De leden vragen mij dit te beoordelen.

Het voorstel van de Commissie is een herziening van de huidige eIDAS-verordening en laat, in lijn daarmee, ruimte aan lidstaten voor verplicht te ontwikkelen eID's en *wallets*, die na Europese erkenning binnen een geharmoniseerde Europese infrastructuur gebruikt kunnen worden voor digitale dienstverlening in andere lidstaten. Enerzijds constateert het kabinet in het BNC-fiche dat deze infrastructuur in technisch opzicht nog niet volmaakt is en ontwikkeling behoeft, anderzijds werkt wat nu in diverse lidstaten ontwikkeld is in het algemeen wel om eID's grensoverschrijdend te kunnen gebruiken. Tevens constateert het kabinet met de Commissie dat er in Europa te weinig eID-middelen, dienstverleners en diensten zijn aangesloten om te kunnen spreken van een succesvolle implementatie van de verordening. De oorzaak ligt bij de lidstaten zelf en daarom steunt het kabinet het idee in het voorstel om alle lidstaten te verplichten om minstens één eID, waaronder minstens één *wallet*, te laten erkennen. Daarnaast dringt het kabinet er bij de Commissie op aan om maatregelen te nemen om te bevorderen dat in de lidstaten meer dienstverleners en diensten aansluiten op de nationale koppelvlakken, die weer gekoppeld moeten worden aan de Europese infrastructuur. Zodoende groeit de behoefte en de noodzaak om de interoperabiliteit te blijven verbeteren en te komen tot een steeds meer geharmoniseerde infrastructuur, waarbij wel voldoende ruimte blijft voor nationale invulling en innovatie van de identiteitsinfrastructuur.

De leden van de GroenLinks-fractie vragen me of ik van mening ben dat commerciële benutting van de digitale identiteiten inzake gebruikersgedrag niet mag. Anders gezegd, dat meta-informatie over het gebruik dus nooit commercieel benut mag worden. De leden vragen hoe het antwoord op deze vraag zich verhoudt tot het verschil tussen het voorstel van de Commissie en de voorstellen van de Wdo en vragen aan mij aan te geven wat onder commerciële activiteiten wordt verstaan. Tot slot vragen de leden of ik kan verzekeren dat er op geen enkele wijze iets met de persoonlijke inlogdata gedaan kan worden.

Ik ben van mening dat commerciële benutting van digitale identiteiten inzake gebruikersgedrag inderdaad niet mag. Het gaat erom dat persoonsgegevens alleen gebruikt worden om inlogmiddelen veilig uit te kunnen geven en ten behoeve van het gebruik van het inlogmiddel door de burger, en dat de verwerking binnen deze doelbinding blijft, zoals bepaald in het voorstel voor de Wdo. Andersoortig commercieel gebruik, direct of indirect, van deze gegevens en gegevens die in het kader van de dienstverlening worden gegenereerd (logging met meta-informatie c.q. gebruikersgedrag) wordt in de Wdo expliciet verboden en wordt als verhandelverbod op verzoek van uw Kamer nu ook via een novelle op wetsniveau geregeld. Onder commerciële activiteiten versta ik in dit verband activiteiten die niet vallen onder activiteiten waartoe de private aanbieders op grond van de doelomschrijvingen in de Wdo gerechtigd zijn.

In het voorstel van de Commissie is het verhandelverbod niet expliciet, in ieder geval niet zoals in de Wdo, opgenomen. Wel is voor de *wallet* artikel 6a, lid 7, opgenomen dat aanbieders van *wallets* verbiedt om persoonsgegevens – die gerelateerd zijn aan de *wallet* of het gebruik daarvan – te combineren met data van andere diensten van zichzelf of derden. De gegevens mogen op grond van deze bepaling dus niet voor andere, niet *wallet*-gerelateerde, dienstverlening worden ingezet. Het verbod om de gegevens commercieel in te zetten staat niet met zoveel woorden in het voorstel van de Commissie, maar de ratio achter deze bepaling lijkt dezelfde te zijn als het verhandelverbod in de Wdo.

Volledig uitsluiten van risico's van ongeoorloofd gebruik, is helaas nooit mogelijk. Met het instrumentarium in het voorstel voor de Wdo verwacht ik het risico daarop tot een minimum te kunnen beperken. In de Wdo worden, naast het verhandelverbod in de wet zelf, in de uitvoeringsregels ook nadere voorschriften gesteld om andersoortig gebruik dan op grond van de Wdo onmogelijk te maken. Denk aan het gescheiden opslaan van gebruiks- en gebruikersgegevens, waardoor de koppeling niet meer of alleen geclausuleerd mogelijk is, en aan maatregelen om waar mogelijk met versleutelde gegevens te werken. Aanbieders van private inlogmiddelen worden hier niet alleen bij de toelating op gecontroleerd, maar ook tussentijds, als onderdeel van het doorlopende toezicht op de inlogmiddelen. Bij overtreding van deze regels kan in voorkomende gevallen worden overgegaan tot schorsing, en uiteindelijk ook uitsluiting van de dienstverlening, waarbij de toelating wordt ingetrokken en de aanbieder zijn dienstverlening moet stoppen. Overigens zal een dergelijk gebruik van persoonsgegevens ook een overtreding van de AVG inhouden, waarvoor tevens de daarbij behorende sanctieringsmogelijkheden open staan.

De leden van de GroenLinks-fractie zouden tot slot graag van mij een appreciatie ontvangen van de keuze van Duitsland inzake de digitale identiteit. Hoe verhoudt zich de Duitse structuur ten opzichte van het voorstel van de Commissie en van de Wdo en welke specifieke verschillen zijn er?

De Duitse federale overheid ziet, zoals het kabinet, de digitale (bron)identiteit als een fundamentele bouwsteen voor succesvolle digitalisering. Duitsland zet daarom in op de ontwikkeling van een infrastructuur waarbinnen eID's met attributen veilig en betrouwbaar uitgewisseld en grensoverschrijdend gebruikt kunnen worden door zowel burgers als bedrijven op basis van '*self-sovereign Identity*' (SSI) technologie. Duitsland en Spanje hebben recent een gezamenlijke verklaring uitgebracht, waarin ze hun samenwerking bevestigen en een grensoverschrijdende pilot initiëren op het terrein van digitale identiteiten.⁴ Ik volg dit initiatief met interesse en ben in goed overleg met zowel Duitse als Spaanse initiatiefnemers over kennisuitwisseling en samenwerking.

Het kabinet wil dat alle ingezetenen en bedrijven in Nederland en in andere Europese landen op een veilige, betrouwbare, toegankelijke en gebruiksvriendelijke manier zoveel mogelijk digitaal transacties kunnen verrichten in het publieke en in het private domein, ook over de grens. Op dit moment zorgt de snelheid van de digitale innovatie ervoor dat mensen veelal zonder alternatieven onder regie van overheden afhankelijk zijn van grote, niet-Nederlandse bedrijven ('*Big tech*').

⁴ <https://www.bundesregierung.de/breg-en/news/digital-identity-ecosystem-1947474>

Hierbij zien we te vaak diensten die zogenaamd 'gratis' zijn, waarbij mensen eigenlijk 'betalen' met hun (transactie)gegevens. Dit vraagstuk wil het kabinet adresseren. De Wdo is het beoogde fundament voor regulering en doorontwikkeling van een dergelijk eID-stelsel en het kabinet wil in de tweede tranche de grondslag verankeren voor het delen van gegevens in combinatie met een digitale bronidentiteit. Die zal op termijn gebruikt kunnen worden in oplossingen zoals een *wallet*, waaraan allerlei attributen gekoppeld kunnen worden onder toezicht van de overheid en onder regie van de burgers en bedrijven die hun gegevens zelf ter beschikking stellen.

De leden van de **PvdA-fractie** vragen hoe het voorstel van de Commissie voor een raamwerk voor een Europese digitale identiteit zich precies verhoudt tot de voorstellen van de Wdo, waarvan de eerste tranche momenteel in behandeling is in de Eerste Kamer. Kunnen de voorziene wettelijke verankering van privacy by design, het handelverbod van gegevens en open source in de Wdo in stand blijven wanneer het voorstel van de Commissie van kracht zou worden?

Het voorstel van de Commissie is, zoals de huidige eIDAS-verordening, gebaseerd op de interne markt en heeft tot doel met harmonisatie de interoperabiliteit van eID's, *wallets* en daarin opgenomen attributen te verbeteren. Om te bereiken dat middelen uit verschillende lidstaten grensoverschrijdend gebruikt kunnen worden, moeten de eisen die aan middelen in lidstaten gesteld worden, zoveel mogelijk gelijk zijn. Privacy by design is op grond van de AVG al een ontwerpeis en is als zodanig overgenomen in het voorstel, alsmede in de Wdo, waarbinnen hierop expliciet zal moeten worden getoetst. Over het handelverbod heb ik u in het voorgaande geïnformeerd. Het voorstel van de Commissie gaat niet expliciet in op het gebruik van open source, maar staat daaraan dus ook niet in de weg. Vanuit Nederland zal, indien opportuun, worden gekoerst op een bepaling zoals die ook in de novelle is opgenomen, met de argumentatie zoals ik die met uw Kamer heb gewisseld in het kader van de behandeling van de Wdo.

De leden van de PvdA-fractie vragen of het voorstel van de Commissie toestaat dat de Nederlandse (digitale) overheid uitsluitend gebruik maakt van decentrale opslag van gegevens.

De Wdo maakt zowel centrale als decentrale opslag van gegevens mogelijk. Ik heb uw Kamer hier in eerdere beantwoording op vragen over de Wdo over geïnformeerd. Het voorstel van de Commissie spreekt evenals de Wdo geen voorkeur voor de ene of andere manier uit. Het voorstel kiest net als de Wdo voor een benadering van adequate bescherming van persoonsgegevens, waarbij het scala aan maatregelen breder reikt dan de wijze en de locatie van opslag van gegevens.

De leden van de PvdA-fractie verwijzen naar de volgende passage in het BNC-fiche: 'Het kabinet streeft ernaar onder de Wet Digitale Overheid een regiem van open toelating te introduceren, waarbij marktwerking wordt ingezet binnen de kaders voor veilige en betrouwbare digitale interactie.' De leden vragen of het voorstel van de Commissie toestaat dat nationale wetgeving over de digitale overheid (de Wdo) ook zonder marktpartijen wordt vormgegeven.

Het voorstel van de Commissie schrijft voor dat lidstaten ten minste één *wallet* moeten uitgeven. Dit kan geschieden door de lidstaat zelf, onder mandaat van de lidstaat of onafhankelijk maar erkend door de lidstaat. Het voorstel staat dus toe een *wallet* zonder marktpartijen uit te geven en dit als zodanig in nationale wetgeving vorm te geven.

De leden vragen mij om gedetailleerd uiteen te zetten wat volgens mij de genoemde 'kaders voor veilige en betrouwbare digitale interactie' inhouden en aan te geven of daar privacy by design, het handelverbod van gegevens, open source, en decentrale opslag onder vallen.

De kaders voor inlogmiddelen, waar de vragen ten aanzien van privacy by design, het handelverbod van gegevens, open source en decentrale opslag in dit verband op zien, worden gevormd door de eIDAS verordening, die de eisen stelt aan de betrouwbare uitgifte en werking van inlogmiddelen, en door de AVG, die vereist dat de te verwerken persoonsgegevens goed

beschermd zijn. Privacy by design en het verhandelverbod van gegevens vallen hier zeker onder. Dit zijn uitwerkingen van de AVG-beginselen. Open source kan bijdragen aan transparantie. Ik heb daarom in de novelle bij de Wdo opgenomen dat open source een wegingsfactor wordt bij de toelating van inlogmiddelen, zodat verantwoord naar inzet van open source wordt toegewerkt. Privacy by design is eveneens als criterium in de novelle opgenomen, waardoor dit als criterium wordt gesteld voor de toelating van middelen. Ook het verhandelverbod is, zoals hiervoor beschreven is, expliciet opgenomen in de novelle.

Decentrale opslag kan een bijdrage leveren aan de bescherming van persoonsgegevens, maar is geen op zichzelf staand middel voor privacybescherming. Het is een maatregel die er in samenhang met andere maatregelen voor kan zorgen dat persoonsgegevens beschermd zijn.

De leden van de PvdA-fractie vragen mij tot slot of ik dit ook aan de Commissie heb medegedeeld.

Het betreft een nieuw wetsvoorstel van de Commissie dat nog niet op het niveau van bewindspersonen is besproken. De Nederlandse positie zoals beschreven in het BNC-fiche wordt op dit moment naar voren gebracht in de ambtelijke werkgroepen van de Telecomraad. De agenda van de eerstvolgende Telecomraad is nog niet vastgesteld en evenmin de daaraan deel te nemen bewindspersonen en de daarin in te nemen posities.