

Vergaderjaar 2023–2024

26 643

Informatie- en communicatietechnologie (ICT)

Nr. 1145

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 12 maart 2024

De vaste commissie voor Digitale Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over de brief van 26 oktober 2023 over de voortgangsrapportage Europese Digitale Identiteit (Kamerstuk 26 643, nr. 1084).

De vragen en opmerkingen zijn op 30 januari 2024 aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties voorgelegd. Bij brief van 12 maart 2024 zijn de vragen beantwoord.

De fungerend voorzitter van de commissie,
Kathmann

De griffier van de commissie,
Boeve

Vragen en opmerkingen van de leden van de GroenLinks-PvdA-fractie en reactie van de bewindspersoon

De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van de voortgangsrapportage. Zij onderschrijven het grote belang van de zelfbeschikking van mensen en bedrijven over hun eigen gegevens. Mensen zijn de baas over hun data en dienen daar altijd zeggenschap over te bewaren. Deze digitale autonomie moet voorop staan in het beleid van Nederland en in Europa. Over de voortgangsrapportage hebben de leden enkele opmerkingen en vragen.

1)

Ten eerste hebben de leden van de GroenLinks-PvdA-fractie vragen over mogelijke alternatieven voor de Europese wallet. Is de Staatssecretaris bijvoorbeeld bekend met de open source wallet Yivi? Erkent de Staatssecretaris dat het van belang is om openbare, alternatieve wallets te ontwikkelen en ondersteunen zodat de Europese wallet niet de enige op de markt wordt? Wat doet zij om ook in het buitenland dergelijke alternatieve wallets geldig en functioneel te maken, zo vragen deze leden.

Ja, ik ben bekend met Yivi.

Er is geen sprake van een door de Europese Unie (hierna: EU) uitgegeven «Europese wallet». Wallets worden nationaal uitgegeven. Ik onderken het belang dat er meerdere wallets worden ontwikkeld. Ik steun dan ook dat onder het voorstel tot herziening van de eIDAS-verordening (hierna: verordening) iedere lidstaat wordt geacht zelf minstens één wallet (hierna: EDI-wallet) uit te geven of een onafhankelijk ontwikkelde wallet te erkennen als EDI-wallet. Op deze manier wordt geborgd dat lidstaten natuurlijke personen en rechtspersonen die dat willen de beschikking geven over een EDI-wallet. Deze EDI-wallets kunnen zij in de gehele EU gebruiken. Dit is onder meer mogelijk doordat certificering van EDI-wallets in de gehele EU plaatsvindt tegen dezelfde eisen. Daarnaast worden er onder meer technische standaarden voorgeschreven waaraan EDI-wallets moeten voldoen. Ook worden diverse publieke en private dienstverleners verplicht om EDI-wallets te accepteren voor hun dienstverlening, zodat gebruikers ook in andere lidstaten met hun EDI-wallet terecht kunnen bij dienstverleners.

2)

Ten tweede zijn de leden van de GroenLinks-PvdA-fractie benieuwd welk risico er is op «function creep». Dat wil zeggen: door het normaliseren van het gebruik van een Europese wallet, is het makkelijker om deze steeds breder in te zetten en de functionaliteit uit te breiden. Welke waarborgen zijn er dat de Europese wallet enkel dient voor het afgekaderde doel waar de lidstaten mee instemmen?

Hoe verzekert de Staatssecretaris dat het gebruik van een wallet niet verplicht wordt, direct of indirect (bijvoorbeeld als bedrijven geen andere mogelijkheden toestaan)? Kan de Staatssecretaris zich in Europees verband uitspreken voor dit recht en andere lidstaten vragen ditzelfde principe te hanteren, zodat Nederlanders in het buitenland ook niet (in)direct verplicht kunnen worden de Europese wallet te gebruiken? Kan de Staatssecretaris bedrijven ertoe dwingen om altijd alternatieven, waaronder niet- digitale, te accepteren? Staat dit geborgd in de huidige kaders van de eIDAS, vragen de leden.

De verordening bevat een overzicht van de functionaliteiten van EDI-wallets, zoals inloggen, het onder eigen regie ophalen en delen van gegevens en elektronisch ondertekenen. Een wallet kan pas gecertificeerd worden wanneer deze voldoet aan de met deze functionaliteiten samen-

hangende vereisten die voortvloeien uit de verordening. Door lidstaten aangewezen geaccrediteerde conformiteitsbeoordelingsinstanties voeren deze certificering uit. Mocht er in de toekomst nationaal of Europees behoefte ontstaan aan nieuwe functionaliteiten, dan kunnen dergelijke nieuwe functionaliteiten via democratische besluitvorming toegevoegd worden.

Uit de verordening volgt dat het gebruik van een EDI-wallet vrijwillig is en dat de toegang tot publieke en private diensten, toegang tot de arbeidsmarkt en ondernemingsvrijheid niet op enige wijze beperkt of belemmerd mag worden voor natuurlijke personen en rechtspersonen geen EDI-wallet gebruiken. Dienstverleners in de hele EU kunnen dus geen diensten aanbieden waarbij alleen een EDI-wallet kan worden gebruikt. Hier vloeit uit voort dat bedrijven die een EDI-wallet accepteren altijd een alternatief moeten bieden. Dit kan zowel een digitaal als een niet-digitaal alternatief zijn. De verordening schrijft ook voor dat het gebruik van andere bestaande identificatie- en inlogmiddelen mogelijk blijft.

Ik heb mij eerder tijdens de Raadsonderhandelingen hard gemaakt voor borging van vrijwillig gebruik van EDI-wallets zodat het beperken van toegang tot dienstverlening voor mensen die geen EDI-wallet kunnen of willen gebruiken voorkomen wordt. Ik ben dan ook tevreden dat dit nu in de verordening is opgenomen.

Bedrijven worden niet verplicht om altijd een niet-digitaal alternatief te bieden. Dit zou ook onwenselijk zijn omdat er bedrijven zijn die bijvoorbeeld volledig digitaal opereren, zoals webshops en appdienstverleners. Wel ga ik in het kader van het beschikbaar houden van voor burgers cruciale dienstverlening onder meer in gesprek met zorgverzekeraars en woningbouwcorporaties om een niet-digitaal alternatief te waarborgen. Banken hebben daarvoor al een programma «Commitment van banken voor beter toegankelijk betalingsverkeer». De aangesloten banken garanderen dat niet-digitale klanten gebruik kunnen blijven maken van niet-digitale basisbankdiensten, zolang als dat nodig is.

Ik hecht eraan te benadrukken dat er in het contact met de overheid altijd een niet-digitaal alternatief is. Met de Wet modernisering elektronisch bestuurlijk verkeer is in de Algemene wet bestuursrecht bepaald dat natuurlijke personen en rechtspersonen in het contact met de overheid het recht hebben om digitaal zaken te doen, maar niet de plicht.

3)

Ten derde vragen de leden van de GroenLinks-PvdA-fractie of de Nederlandse voorbeeldwallet actief wordt voorgelegd aan vertrouwde organisaties voor een zienswijze, met nadruk op privacywaakhonden en (digitale)rechtenorganisaties. Is de Staatssecretaris bereid dit te doen? Hoe zorgt de Staatssecretaris ervoor dat de reacties die worden opgehaald een goede afspiegeling geven van de ervaring van gebruikers, waakhonden, maatschappelijke organisaties en bedrijven? Tot slot vragen de leden hoe de Staatssecretaris de Kamer op de hoogte houdt van de resultaten van de grootschalige Europese pilots.

Ja. De Nederlandse publieke EDI-wallet (hierna: publieke wallet) wordt stapsgewijs en open source ontwikkeld. Dit betekent dat zowel belangenbehartigers als betrokken gebruikers in de gelegenheid zijn om feedback te geven op de ontwikkeling. Het programma EDI-stelsel NL, waartoe ik opdracht heb gegeven, organiseert regelmatig bijeenkomsten om professionals, burgers en ondernemers en belangenbehartigers, in staat te stellen een bijdrage te leveren. Het programma EDI-stelsel NL zorgt ervoor dat een brede afspiegeling en vertegenwoordiging van diverse

belanghebbenden is geborgd in de aanpak en aansturing. Verder zullen de beproevingen met de publieke wallet plaatsvinden met een representatieve groep testgebruikers. Tevens laat ik deze testen op onder andere gebruiksvriendelijkheid en toegankelijkheid.

Over de voortgang van de Europese pilots zal ik u periodiek informeren via de Verzamelbrief Digitalisering.

4)

Ten vierde willen de leden van de GroenLinks-PvdA-fractie onderstrepen dat digitale toegankelijkheid in een digitaliserende samenleving essentieel is. Wordt de winst in het gemak voor gebruikers uiteengezet voor verschillende bevolkingsgroepen? Wordt er expliciet gekeken naar de rol van een wallet voor gebruikers met een beperking, of mensen die onder bewind staan? Welke mogelijkheden hebben mensen om anderen te machtigen om hun wallet namens hen te gebruiken? Hoe gaat de Staatssecretaris ervoor zorgen dat hier niet dezelfde problemen ontstaan zoals bij DigiD, waar bewindvoerders moeilijk namens hun cliënt gebruik van kunnen maken? Legt de Staatssecretaris de voorbeeldwallet ook voor aan organisaties die zich inzetten voor digitale toegankelijkheid?

Digitale toegankelijkheid wordt geborgd in de verordening. Bij de ontwikkeling en beproeving van de publieke wallet en bij de aanpak van het programma EDI-stelsel NL worden nadrukkelijk ook de gebruikers (burgers en ondernemers) betrokken, waaronder ook gebruikers met een beperking. Het uitgangspunt is dat het voor iedereen die dat wil mogelijk moet zijn om een EDI-wallet te gebruiken. Over de mogelijkheden voor degenen die zelf geen publieke dienstverlening af kunnen of mogen nemen heb ik uw Kamer recentelijk geïnformeerd bij brief van 22 december 2023¹ en in mijn beantwoording van Kamervragen over dit onderwerp op 26 januari jl.² Als aanvulling op de mogelijkheid die vertegenwoordigers (gemachtigden en wettelijk vertegenwoordigers) hebben om met hun eigen inlogmiddel diensten af te nemen namens de personen die zij vertegenwoordigen, onderzoek ik of het voor vertegenwoordigers mogelijk is om middels een EDI-wallet aan te tonen dat zij namens een ander mogen handelen.

5)

Tot slot vragen de leden van de GroenLinks-PvdA-fractie op welke momenten de Kamer wordt geïnformeerd over de voortgang op de voorbeeld-wallet. Zij willen graag weten welke kwetsbaarheden er in de testfase worden gevonden en hoe deze worden gedicht. Kan de Staatssecretaris de Kamer hierover per kwartaal informeren? Wanneer ontvangt de Kamer een volgende update over de vorderingen in de Europese onderhandelingen over de verordening, zo vragen de leden van voornoemde fractie.

Ik zal u periodiek via de Verzamelbrief Digitalisering informeren over de voortgang van de publieke wallet. De tests, die naar verwachting in de tweede helft van dit jaar wordt uitgevoerd om de werking van de publieke wallet in de praktijk te beproeven, worden na afloop geëvalueerd. De bevindingen daarvan zal ik vervolgens met u delen.

De inhoudelijke onderhandelingen over de verordening zijn geëindigd. Nederland heeft, net zoals alle andere lidstaten, eerder in Coreper ingestemd met de definitieve compromistekst. Voorafgaand aan de stemming in Coreper bent u hierover geïnformeerd.³ Afgelopen weken

¹ TK 26 643, nr. 1112.

² Aangangsel Handelingen II 2023/24, nr. 878.

³ TK 21 501-33, nr. 1042.

hebben de juristen-linguïsten van de EU de verordening vertaald naar alle officiële talen van de EU. Het Europees Parlement heeft op 29 februari jl. plenair ingestemd met de definitieve compromistekst. De Raad zal naar verwachting binnenkort ook formeel stemmen op basis van een gekwalificeerde meerderheid. Na deze instemming wordt het akkoord kort erna gepresenteerd in het Publicatieblad van de EU. De verordening treedt 20 dagen na publicatie in het Publicatieblad in werking.

Vragen en opmerkingen van de leden van de VVD-fractie en reactie van de bewindspersoon

De leden van de VVD-fractie hebben kennisgenomen van de voortgangsrapportage Europese Digitale Identiteit. De leden hebben nog enkele vragen en opmerkingen.

De leden van de VVD-fractie lezen dat het kabinet is gestart met het opstarten van een veilig en betrouwbaar EDI-stelsel⁴ in Nederland. Zo lezen voornoemde leden dat binnen het EDI-stelsel Nederland veel waarde wordt gehecht aan gegevensbescherming, informatieveiligheid en toegankelijkheid. Welke concrete maatregelen zijn genomen en worden nog genomen om aspecten als gegevensbescherming en informatieveiligheid te borgen? Worden deze aspecten vervolgens ook getest? Zo ja, in welke mate? Zo nee, waarom niet, vragen de leden.

Het beschermen van gebruikers en hun gegevens, evenals van organisaties die op het EDI-stelsel vertrouwen, vraagt om een combinatie van juridische, organisatorische en technische maatregelen. Zo moeten EDI-wallets worden gecertificeerd conform de cybersecuritywetgeving en staan ze daarna onder doorlopend toezicht. Daarbij zullen periodiek kwaliteitsbeoordelingen en hercertificering van EDI-wallets plaatsvinden. Ze moeten bovendien voldoen aan het hoogste betrouwbaarheidsniveau. Ook worden mechanismen ingericht voor de identificatie en authenticatie van partijen die gegevens van gebruikers vragen via EDI-wallets. De publieke wallet wordt getest op mogelijke kwetsbaarheden voordat deze in gebruik wordt genomen als EDI-wallet. Nu al, in de fase van de ontwikkeling van de publieke wallet, vinden technische analyses, gebruikerstests en kwaliteitscontroles plaats, mede om de informatieveiligheid te borgen.

De leden van de VVD-fractie vragen voorts, hoewel ze de vrijwillige basis van deelname goed vinden, hoe de representativiteit van de testgroep voor de voorbeeld-wallet vormgegeven wordt. Wanneer verwacht het kabinet dat de verdere technische handelingen op EU-niveau om de kosten-batenanalyse uit te voeren tot stand gekomen zullen zijn, zo vragen deze leden.

Bij de gebruikerstesten die plaatsvinden voor het ontwerp van de publieke wallet en bij de beproevingen worden verschillende gebruikersgroepen benaderd.

Het geheel aan technische handelingen zal naar verwachting 12 maanden na inwerkingtreding van de eIDAS-revisie vastgesteld zijn.

Vragen en opmerkingen van de leden van de NSC-fractie en reactie van de bewindspersoon

De leden van de NSC-fractie hebben met interesse kennisgenomen van de voortgangsrapportage over het Europese Digitale Identiteitsbewijs en de bijbehorende Maatschappelijke Kosten-Batenanalyse (MKBA).

⁴ Deze leden refereren aan EDI als Electronic Data Interchange.

De leden van de NSC-fractie vragen om toelichting waarom ervoor is gekozen om het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties met geraamde ontwikkelkosten van € 32,3 miljoen zelf een EDI-wallet te laten bouwen, terwijl de Stichting Internet Domeinregistratie Nederland (SIDN) als maatschappelijke organisatie zonder winstoogmerk met Yivi reeds een privacyvriendelijke, open source identiteitswallet van Nederlandse bodem beschikbaar heeft gesteld. Zij vragen welke redenen eraan ten grondslag liggen om niet Yivi namens Nederland als nationale Digital Identity Wallet aan te dragen, aangezien deze wallet ook tegenwicht zou kunnen bieden tegen de potentiële dominantie van grote technologiebedrijven in de markt.

Om een gelijk speelveld tussen private aanbieders van EDI-wallets te creëren lag het niet voor de hand om parallel aan de onderhandelingen over de verordening een bestaande wallet, van een private partij of stichting, aan te dragen. Hiermee zou de ene walletontwikkelaar een voorsprong krijgen op de anderen. Bovendien is voortgebouwd op de ontwikkelingen van de afgelopen jaren binnen het domein inlogmiddelen, waarbij gebleken is dat de Kamer veel waarde hecht aan een publiek alternatief naast marktoplossingen. De publieke wallet wordt ontwikkeld ook met als doel inzichten op te doen over de vereisten van de herziene verordening.

De leden van de NSC-fractie spreken voorts hun zorgen uit over, zoals tijdens de technische briefing⁵ naar voren kwam, het feit dat dienstverleners die gebruik maken van de EDI, onder de eIDAS-verordening niet verplicht zijn daarnaast een analoog identiteitsbewijs te accepteren. Dit zou uitsluiting van dienstverlening van burgers die niet beschikken over een digitale identiteit tot gevolg kunnen hebben. Is de Staatssecretaris voornemens om bij de inwerkingtreding van de verordening middels additionele nationale wetgeving dit gat te dichten?

Ik wil bij de leden de indruk wegnemen dat sprake is van een gat. Zoals ik in het antwoord op de tweede vraag van GroenLinks-PvdA uiteen heb gezet blijven bestaande identificatie- en inlogmiddelen de standaard en vormen EDI-wallets een digitaal alternatief.

De leden van de NSC-fractie vragen de Staatssecretaris om een overzicht te geven van de beleidsmatige maatregelen die zij voor ogen heeft om het risico op overbevraging door dienstverleners in te perken, evenals welk handelingsperspectief burgers hebben wanneer dienstverleners toch onnodig veel gegevens verzamelen. Verwacht zij daarbij dat de toezichthouder voldoende geëquipeerd zal zijn om effectief voor de rechten van burgers op te komen? Met inachtneming van de recente DAC7-richtlijn – die particuliere verkopers op online handelplatforms als Marktplaats of Vinted verplicht om onder andere hun burgerservicenummer te delen met de platforms in kwestie – leeft er bij de leden van deze fractie de zorg dat er een onwenselijke normverschuiving aan het ontstaan is. De leden verzoeken de Staatssecretaris te reflecteren op het beeld dat nu ontstaat dat eerst het probleem gecreëerd wordt dat burgers door middel van wetgeving onder steeds meer omstandigheden verplicht worden om persoonlijke gegevens te delen, en vervolgens digitale identiteiten als oplossing voor dit probleem worden aangedragen.

Ik wil benadrukken dat de Algemene Verordening Gegevensbescherming (AVG) onverkort van kracht is binnen dit domein. De AVG schrijft voor dat

⁵ Technische briefing over Voortgangsrapportage Europese Digitale Identiteit d.d. 23 januari 2024; www.tweedekamer.nl/debat_en_vergadering/commissievergaderingen/details?id=2023A07878.

geen onnodige gegevensverwerking plaatsvindt. Daarnaast biedt de verordening aanvullende maatregelen om het risico op overvraging voor burgers te mitigeren.

Zo moeten dienstverleners zich registreren in een register in de lidstaat waar ze zijn gevestigd, voordat zij gebruikers van EDI-wallets om gegevens kunnen vragen. Daarbij worden de identiteits- en contactgegevens van dienstverleners vastgelegd. Ook moeten dienstverleners opgeven waar ze de EDI-wallet voor willen gebruiken en welke gegevens ze willen vragen. Deze registers zijn openbaar, zodat iedereen kan beoordelen of er sprake is van overbevraging. Bij tekenen van overbevraging kan een toezichthouder ingrijpen.

De gebruiker voert regie over zijn EDI-wallet en de gegevens die daarin opgenomen zijn. De EDI-wallet moet de gebruiker daartoe zo goed mogelijk ondersteunen, onder andere door de dienstverlener te authenticeren en de gebruiker op eenduidige en begrijpelijke manier te informeren. Ook laten EDI-wallets aan gebruikers zien van welke organisaties hij gegevensverzoeken heeft ontvangen en met welke organisaties hij welke gegevens heeft gedeeld. Vanuit dat overzicht kan de gebruiker vragen om de verwijdering van de gedeelde gegevens, of melding doen bij de gegevensbeschermingsautoriteit. Die autoriteit heeft onder de AVG de mogelijkheid om in te grijpen en boetes op te leggen.

De leden van de NSC-fractie vragen of de verwachting is dat de toezichthouder voldoende geëquipeerd zal zijn om effectief voor de rechten van burgers op te komen. Ja, dit zal het geval zijn. De verordening schrijft voor dat toezichthouders «de noodzakelijke bevoegdheden en toereikende middelen om hun taken doeltreffend, efficiënt en onafhankelijk te kunnen uitvoeren» krijgen.

Het beeld dat de leden schetsen, dat er een probleem wordt gecreëerd, herken ik niet. Voor zover er verplichtingen bestaan voor burgers om gegevens te delen, zijn dit wettelijke verplichtingen of contractuele verplichtingen waarbij de AVG de grenzen aangeeft. Ook herken ik het beeld niet van de verplichtingen als een probleem, met het oog waarop de EDI-wallet tot stand is gekomen.

Een EDI-wallet is bedoeld als een middel om veilig en betrouwbaar gegevens te delen, in die gevallen waarin de gebruiker dat wenst te doen. De EDI-wallet is «neutraal» ten aanzien van de doelen waarvoor deze wordt ingezet. De gebruiker bepaalt zelf voor welke doelen hij de wallet wil gebruiken.

De leden van de NSC-fractie verzoeken de Staatssecretaris om nader te beargumenteren of het indicatief voordeel van het gebruik van EDI-wallets voor eigenaren respectievelijk de gasten van hotels en campings, dat in de MKBA op € 8,6 miljoen en € 2,15 miljoen per jaar is geraamd, wel realistisch is. Dit zijn opvallend hoge bedragen, die hun oorsprong vinden in de geschatte cumulatieve tijdswinst voor het personeel, uitgaande van een minuut tijdswinst per transactie. Echter, deze potentiële tijdswinst zal slechts reële financiële winst worden als het gebruik van de EDI tot gevolg heeft dat hotels en campings ofwel meer gasten kunnen ontvangen, dan wel minder personeel hoeven in te zetten. Dit neigt in de ogen van deze leden naar een papieren werkelijkheid en zij vragen de Staatssecretaris of zij dit beeld deelt.

Hoewel de leden van de NSC-fractie er begrip voor hebben dat deze use-case nader uitgewerkt dient te worden, verzoeken zij de Staatssecretaris wel om toelichting waarom zowel het efficiencyvoordeel voor de dienstverlener, als het gebruikersgemak bij burgers in het geval van bezorging wordt geschat op bedragen in de orde van grootte van

tientallen miljoenen. Waar zou dit aanzienlijke financiële voordeel ten opzichte van de huidige situatie in zitten, zo vragen deze leden. Uit de MKBA blijkt dat het lastig is te bepalen of de invoering van de EDI-wallet een daadwerkelijk negatief effect zal hebben op identiteitsfraude, maar in de analyse wordt wel beschreven dat dit in potentie het geval kan zijn. Echter, indien er een manier gevonden wordt om EDI-wallets te spoofen of om de uitgifte ervan te beïnvloeden middels hacks dan wel klassieke methoden, dan biedt dit mogelijkheden tot identiteitsfraude of misbruik die eerder niet mogelijk waren. Deze leden verzoeken de Staatssecretaris om te beschrijven welke waarborgen hiertegen beschikbaar zullen zijn.

De onderzoekers hebben zich bij de analyse van de kosten en baten gebaseerd op de rijksbreed gehanteerde voorschriften voor maatschappelijke kosten-batenanalyses, van onder meer het Centraal Planbureau en Planbureau voor de leefomgeving. Daarbij hebben de onderzoekers aangegeven dat in het beginstadium van soortgelijke wetgevingstrajecten, het kenmerkend is dat het niet altijd mogelijk is om een volledig representatief beeld van de kosten en baten te geven.

In het geval van «bezorging» geven de onderzoekers aan dat het gaat om veelvoorkomende, alledaagse handelingen. Dat leidt ertoe dat de onderzoekers inschatten dat er cumulatief veel voordeel te realiseren is.

Veiligheid is een van de kernwaarden binnen de ontwikkeling van EDI-wallets en het stelsel. In mijn antwoord op de vraag van de leden van de VVD-fractie geef ik weer welke maatregelen getroffen worden om de informatieveiligheid te borgen. Binnen deze context heeft het risico op identiteitsfraude mijn voortdurende aandacht.

Ook zijn er maatregelen om in te kunnen grijpen als er onverhoopt toch sprake is van identiteitsfraude. Het is op dat moment mogelijk om de geldigheid van deze specifieke EDI-wallet in te trekken. Indien er een veiligheidsprobleem aan ten grondslag ligt dat de betrouwbaarheid van het soort EDI-wallet aantast, dan schort de verantwoordelijke lidstaat de uitgifte en de werking van die EDI-wallet onverwijld op en licht deze de gebruikers ervan, de Europese Commissie en andere lidstaten in.

De leden verzoeken de Staatssecretaris, tot slot, om enige toelichting te geven over de wijze van certificering van EDI-wallets die zal plaatsvinden door de Rijksinspectie Digitale Infrastructuur (RDI).

De Rijksinspectie Digitale Infrastructuur (RDI) is de beoogd toezichthouder voor het EDI-stelsel in Nederland. De RDI voert zelf geen certificering van EDI-wallets uit, maar heeft hierbij wel een rol als de Nationale Cybersecurity Certificering Autoriteit (NCCA).

De eisen waartegen gecertificeerd gaat worden zijn (op hoofdlijnen) vastgelegd in de verordening en worden nader uitgewerkt in een aantal technische uitvoeringshandelingen. De exacte wijze waarop certificering plaats gaat vinden is in afwachting van de uitkomsten van onderzoek door de Europese Commissie. Hierbij wordt onderzocht of en hoe een certificeringsschema voor de EDI-wallets past in het wettelijk kader van de Cybersecurity Act.

Door middel van een certificeringsschema kan door een geaccrediteerde en door de overheid aangewezen conformiteitsbeoordelingsinstantie worden getoetst of aan alle inhoudelijke eisen is voldaan. Deze conformiteitsbeoordelingsinstanties en de door hen uitgegeven certificeringen voor EDI-wallets komen onder toezicht van de Nationale Cybersecurity Certificering Autoriteit.

Vragen en opmerkingen van de leden van de D66-fractie en reactie van de bewindspersoon

De leden van de D66-fractie hebben met interesse kennisgenomen van de voortgangsrapportage en hebben geen verdere vragen.

Vragen en opmerkingen van de leden van de BBB-fractie en reactie van de bewindspersoon

De leden van de BBB-fractie hebben de stukken ter kennis aangenomen en hebben hierover enkele vragen.

De leden van de BBB-fractie vragen de Staatssecretaris waarom de functionaliteiten zoals het offline kunnen gebruiken van de id-wallet en een elektronische handtekening kunnen zetten met een id-wallet later worden ontwikkeld. Kan de Staatssecretaris aangeven hoe dit rijmt met de maatregelen die de overheid moet treffen om de privacy te waarborgen, zoals genoemd wordt op pagina 1 van de brief van de Staatssecretaris van 26 oktober 2023.

De publieke wallet zal op het moment dat deze breed beschikbaar wordt gesteld voorzien zijn van alle vereiste functies. Daar gaat een ontwikkelproces aan vooraf waarin ik stapsgewijs en beheerst functionaliteiten van de publieke wallet laat ontwikkelen, te beginnen met online identificatie en inloggen, en het online voeren van regie over eigen gegevens. Zodra een solide basis bestaat die deze eerste functies biedt, kunnen andere vereiste functies worden toegevoegd zoals het zetten van elektronische handtekeningen en het kunnen gebruiken van de wallet in offlinemodus (op fysieke locaties zonder dat internetverbinding vereist is).

Het borgen van de privacy is één van de belangrijkste aspecten bij de ontwikkeling van de (functionaliteiten van de) publieke wallet en heeft mijn voortdurende aandacht.

De leden van de BBB-fractie wijzen op de volgende passage uit de brief: «Wel geeft het onderzoek een beeld van de mechanismen die de kosten en baten van de EDI-wallet bepalen en beschrijft het de randvoorwaarden voor een succesvolle implementatie». De leden van deze fractie willen de Staatssecretaris vragen om te verduidelijken wat de randvoorwaarden die de succesvolle implementatie van het EDI-Wallet precies zijn, en deze randvoorwaarden puntsgewijs uit te werken.

De onderzoekers geven in het MKBA-rapport de volgende randvoorwaarden voor succesvolle implementatie aan:

- Om het gebruik van een nieuw stelsel van gegevensuitwisseling via de EDI-wallet mogelijk te maken, is meer nodig dan de realisatie van alleen één of meerdere EDI-wallets:
 - Er zijn ketenafspraken nodig over welke gegevens ontsloten worden, in welke vorm dat gebeurt en idealiter over de betekenis en waarde van de gegevens, zodat een ontvangende partij het gegeven ook daadwerkelijk kan verwerken.
 - Het moet mogelijk worden gemaakt dat gegevens worden ontsloten door de verschillende bronhouders. Deze zullen technische voorzieningen moeten treffen.
 - Het moet mogelijk worden gemaakt dat de gegevens kunnen worden ontvangen. Ook hiervoor moeten technische voorzieningen worden gemaakt.
- De onderzoekers beschrijven dat publieke partijen een rol hebben in het aanjagen van het vlieg wiel. Een initieel succes kan ertoe leiden dat

er meer succesvolle toepassingen ontstaan. Hiertoe kunnen publieke partijen het volgende doen:

- Het (stimuleren van het) ontsluiten van (overheids)attributen zodat deze opgenomen kunnen worden in EDI-wallets.
- Het realiseren van een voorbeeldwallet om daarmee voor private ontwikkelaars van een EDI-wallet inzichtelijk te maken hoe beoogde normen, eisen en publieke waarden meegenomen kunnen worden in een wallet.
- Het (stimuleren van het) uitwerken en implementeren van een aantal use cases met zowel publieke als private partijen, zodat de EDI-wallet al vroeg gebruikt kan worden en zo ook ervaring opgedaan kan worden met de ontwikkeling en werking van de EDI-wallet.

In de brief verwijst de Staatssecretaris op pagina 3 naar een document van het wetsvoorstel van de Europese Commissie voor een raamwerk voor een Europese Digitale Identiteit, onder punt 5. In dat document staat dat, zo citeren deze leden: «Gebruikers moeten niet worden verplicht de portemonnee te gebruiken om toegang tot particuliere diensten te krijgen, maar als gebruikers dat willen, moeten zeer grote online platforms de Europese portemonnee voor digitale identiteit daarvoor aanvaarden, met inachtneming van het beginsel van minimale gegevensverwerking.» De leden van voornoemde fractie vragen de Staatssecretaris of er wel rekening wordt gehouden met wat ze in het Engels «complexity by design» noemen, ofwel complexiteit door ontwerp toe te passen? Kan de Staatssecretaris garanderen dat deze methoden niet gebruikt worden als zo'n Europees id-wallet daadwerkelijk officieel uitgerold wordt? Kan de Staatssecretaris eisen van bedrijven dat ze geen «dark patterns» gebruiken om de onbewuste gebruikers te sturen naar de keuze om de digitale Wallet te gaan gebruiken, bijvoorbeeld door de knop groter te maken of de EU Wallet knop wel een kleur te geven en de overige opties niet? En wat kan de Staatssecretaris doen om het gebruik van dark patterns te voorkomen?

Indien platforms, in het ontwerp van hun diensten, het opzettelijk lastig maken voor de gebruiker om die diensten zonder EDI-wallet te gebruiken, kan gesproken worden van een «dark pattern». Dark patterns zijn reeds gereguleerd in EU-wetgeving. Zo vallen dark patterns onder de Europese richtlijn oneerlijke handelspraktijken – geïmplementeerd in Boek 6 van het Burgerlijk Wetboek –, de AVG en de Digital Services Act (hierna: DSA). De DSA zal vanaf 17 februari 2024 van toepassing zijn op alle tussenhandel-diensten. Sinds augustus 2023 is de DSA van toepassing op zeer grote online platformen en zeer grote online zoekmachines. De DSA kent een bepaling waarbij wordt voorgeschreven dat «aanbieders van online platforms hun online-interfaces niet zo ontwerpen, organiseren of beheren dat gebruikers worden misleid of gemanipuleerd of hun vermogen om vrije en geïnformeerde beslissingen te nemen wordt ondermijnd of verstoord». Deze bepaling is van toepassing in situaties die niet onder de reikwijdte van de Richtlijn oneerlijke handelspraktijken of de AVG vallen. Een toezichthouder, zoals de Autoriteit Persoonsgegevens of de Autoriteit Consument en Markt, kan optreden als zij van mening is dat een bedrijf de bovengenoemde wet- en regelgeving overtreedt.

De leden van de BBB-fractie vragen voorts de Staatssecretaris of het mogelijk is om als alternatief voor het Digitale EU Wallet ook de optie nationaal te faciliteren om het papieren bewijs mogelijk te maken als officiële optie naast de digitale EU Wallet.

In lijn met mijn antwoord op de eerste vraag van de leden van de fractie GroenLinks-PvdA benadruk ik nogmaals dat er geen door de EU uitge-

geven «Europese wallet» komt. Een EDI-wallet wordt nationaal uitgegeven.

Voor het antwoord op de vraag over het faciliteren van de optie om het papieren bewijs mogelijk te maken verwijs ik de leden graag door naar het antwoord op de tweede vraag van de leden van de fractie GroenLinks-PvdA.

De leden van de BBB-fractie vragen de Staatssecretaris vervolgens of er op voorhand voor de inschrijving in het register van betrouwbare partners er een controle wordt uitgevoerd over het desbetreffende bedrijf/organisatie?

Nee. De verordening sluit een voorafgaande autorisatieprocedure uit.

Hoe worden de risico's beperkt dat malafide bedrijven en organisaties gegevens kunnen vragen via de digitale EU Wallet?

Zoals toegelicht in mijn antwoord op de vraag van de leden van de NSC-fractie moeten bedrijven en organisaties die gegevens willen ontvangen uit EDI-wallets zich registreren. Doordat de EDI-wallet daarnaast bijhoudt met wie gegevens zijn gedeeld, zijn malafide bedrijven herleidbaar en kunnen toezichthouders ingrijpen.

De leden van de BBB-fractie vragen, tot slot, of het klopt dat de verordening niet gebruikt mag worden voor gezondheidsattesten zoals vaccinatiebewijzen.

De verordening stelt geen eisen aan welke gegevens gebruikers van EDI-wallets onder hun eigen regie kunnen brengen. Dit betekent dat de gebruiker zelf kan kiezen welke gegevens hij in zijn EDI-wallet zet, mits die gegevens door de bronhouder beschikbaar worden gesteld voor gebruik in EDI-wallets. De verordening verplicht bronhouders van gezondheids- en vaccinatiegegevens niet om deze beschikbaar te maken in EDI-wallets.

Een EDI-wallet is – zoals reeds is aangehaald in het antwoord op de vraag van de leden van de NSC-fractie – neutraal ten aanzien van de doelen waarvoor deze wordt ingezet. Dat betekent dat het gebruik voor gezondheidsattesten niet bij voorbaat is uitgesloten maar ook niet verplicht is. Gebruikers bepalen zelf of en waarvoor ze een EDI-wallet willen gebruiken. De verordening borgt dit via de vrijwilligheid van gebruik.

Vragen en opmerking van de leden van de SP-fractie en reactie van de bewindspersoon

De leden van de SP-fractie hebben kennisgenomen van de voortgangsrapportage Europese Digitale Identiteit, en hebben enkele vragen hierover.

De leden van de SP-fractie benadrukken dat een digitale identiteit nooit de enige manier van identificatie moet zijn. 20 procent van volwassenen in Nederland beschikt onvoldoende digitale vaardigheden, en veel mensen hebben simpelweg geen behoefte aan een digitale identiteit. Als overheden of private organisaties zoals banken en werkgevers papieren documentatie uitsluiten wanneer iemand zich moet identificeren of iets anders moet doen met data dat ook via een digitale route kan, zoals een sollicitatie of een aanvraag van een lening, wordt een grote groep buitengesloten. Een offline variant van de id-wallet is onvoldoende. Hoe gaat de Staatssecretaris garanderen dat het altijd mogelijk blijft voor mensen om via de papieren route zich te kunnen identificeren of zaken te doen met particuliere organisaties, zo vragen deze leden.

Voor het antwoord op deze vraag verwijs ik de leden graag naar de antwoorden op de tweede vraag van de leden van de GroenLinks-PvdA-fractie.

De leden van de SP-fractie hebben ook een aantal vragen over de opslag van persoonsgegevens die gebruikt worden door de id-wallet. Gebruikers mogen zelf bepalen welke gegevens betrokken mogen worden bij hun id-wallet, zoals een rijbewijs of diploma(s). Hoe heeft een persoon toegang tot deze data? Wordt alles lokaal opgeslagen op een computer of smartphone om offline gebruik te faciliteren, zo willen de leden weten. Of worden de gegevens uit een databank gehaald en krijgt de persoon tijdelijk inzage? Wat kunnen personen doen als informatie uit hun id-wallet toch op illegale wijze wordt gebruikt?

Gebruikers kunnen persoonlijke gegevens uit publieke en private bronnen in hun EDI-wallet laden.

Waar deze gegevens vervolgens precies staan is afhankelijk van het ontwerp van de wallet. In het ontwerp van de publieke wallet komen deze gegevens op de telefoon van de gebruiker, versleuteld en met een pincode beveiligd.

Het beschermen van burgers tegen ongeoorloofd of frauduleus gebruik van hun EDI-wallet is van groot belang voor het waarborgen van het vertrouwen in en voor de brede acceptatie van EDI-wallets. Gebruikers moeten effectieve bescherming tegen dergelijk misbruik krijgen. Na kennisname van oneigenlijk of frauduleus gebruik moeten toezichhoudende instanties de nodige maatregelen nemen om ervoor te zorgen dat de registratie van de vertrouwende partij en het kunnen delen van gegevens met de vertrouwende partij wordt ingetrokken of opgeschort.

Aangezien het om verwerking van persoonsgegevens gaat is de AVG onverkort van toepassing. Als sprake is van onrechtmatige gegevensverwerking blijft het daarom mogelijk om een verzoek tot inzage en verwijdering van gegevens te doen. Daarnaast bestaat de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens, waarna de toezichthouder kan handhaven. Als aan bepaalde voorwaarden is voldaan dan is het ook mogelijk om aanspraak te maken op vergoeding van de geleden schade.

Tot slot hebben burgers ook de mogelijkheid om als er sprake is van identiteitsfraude een melding te doen bij het Centraal Meldpunt Identiteitsfraude. Burgers kunnen hier terecht voor advies en ondersteuning.

Aangezien de id-wallet ook in de EU gebruikt kan gaan worden, is de EU verantwoordelijk voor het beschermen van de persoonsgegevens als iemand hun id-wallet in het buitenland gebruikt, of is dat aan de lidstaat, zo vragen de voornoemde leden.

De bescherming van persoonsgegevens is geregeld in de AVG. De AVG bepaalt wie verantwoordelijk is voor de verwerking van persoonsgegevens en aan welke eisen deze verwerking moet voldoen. De AVG-vereisten zoals doelbinding en dataminimalisatie gelden onverkort in de gehele EU. Bovendien moeten verwerkingsverantwoordelijken passende technische en organisatorische maatregelen treffen, zodat passende beveiliging van de gegevens gewaarborgd is. Als een gebruiker via zijn door Nederland uitgegeven EDI-wallet persoonsgegevens verstrekt aan een dienstverlener in een andere lidstaat, dan draagt die dienstverlener de verantwoordelijkheid voor de goede bescherming van die persoonsgegevens. Op het moment dat een

dienstverlener niet aan de AVG voldoet kan de toezichthouder van de desbetreffende lidstaat hiertegen optreden.

Vragen en opmerking van de leden van de CU-fractie en reactie van de bewindspersoon

De leden van de ChristenUnie-fractie danken de Staatssecretaris voor de toegestuurde voortgangsrapportage over de Europese Digitale Identiteit. Zij hebben hierover nog enkele vragen.

De leden van de ChristenUnie-fractie vragen de Staatssecretaris helder uiteen te zetten wat op grond van de Europese richtlijn de mogelijkheden zijn voor bedrijven en organisaties om gebruik te maken van de id-wallet en diensten aan te bieden exclusief voor gebruikers van een id-wallet.

Voor het antwoord op deze vraag verwijs ik de leden naar het antwoord op de tweede vraag van de leden van de GroenLinks-PvdA-fractie.

De leden van de ChristenUnie-fractie lezen dat de Staatssecretaris het van belang acht dat burgers digitaal autonoom kunnen zijn en zelf kunnen beschikken over hun digitale identiteit. De leden zien de ontwikkeling van de Europese Digitale Identiteit als een ultieme vorm van individualistisch samenleven, ontwikkeld vanuit het principe van verbeterde marktwerking. De Europese Digitale Identiteit is een id-wallet die technisch gezien goed kan werken voor personen en bedrijven.

Tegelijkertijd kan deze id-wallet op de langere termijn uitgroeien als cruciaal voor ieders digitale sociale bestaan. Nu steeds meer van ons sociale leven digitaal wordt is het, volgens de leden van deze fractie, verstandig om naar deze ontwikkeling niet alleen vanuit economisch of marktperspectief te kijken maar ook vanuit sociaal-maatschappelijk perspectief. Dit op het oog technisch vernuftige en handige instrument kan vorm gaan geven aan het sociaal-maatschappelijk verkeer. De leden vragen de Staatssecretaris te reflecteren op de mogelijke gevolgen van de ontwikkeling van de Europese Digitale Identiteit.

De ontwikkeling van EDI-wallets is onderdeel van een grotere digitaliseringsinslag. Deze biedt kansen voor onze samenleving en economie die het kabinet wil stimuleren en omarmen, op een manier waarop vertrouwen ontstaat en onze publieke waarden veilig worden gesteld. Welk effect EDI-wallets zullen hebben op onze samenleving zal afhangen van de toepassingen die in de praktijk ontstaan. Zo kunnen EDI-wallets meer grip geven op eigen gegevens en eigen digitale interacties en burgers meer autonomie geven bij het verkrijgen van toegang tot diensten. Het gaat bijvoorbeeld om het openen van een bankrekening of het aanvragen van een vergunning. Daarbij moeten we oog houden voor mogelijke risico's, negatieve effecten en publieke waarden als privacy, veiligheid en transparantie. Voor de ontwikkeling van de publieke wallet heb ik het programma EDI-stelsel ingericht. Dit programma heeft als taak de relevante stakeholders waaronder beoogde eindgebruikers (burgers en ondernemers) te betrekken bij de ontwikkelingen rondom digitale identiteit om de verschillende zienswijzen in acht te nemen. Ook worden diverse maatschappelijke organisaties betrokken. Het programma heeft daarnaast een community-platform ingericht⁶ en organiseert openbaar toegankelijke bijeenkomsten. Deze aanpak leidt ertoe dat er inzichten worden opgedaan vanuit verschillende perspectieven in de vorming van het EDI-stelsel in Nederland.

De NL voorbeeld-wallet wordt in de praktijk beproefd met een representatieve groep testgebruikers op basis van vrijwillige deelname. Ook vinden

⁶ <https://edi.pleio.nl/>.

er Large Scale Pilots plaats voor grensoverschrijdende implementatie. Deze tests zien op gebruiksvriendelijkheid en toegankelijkheid. De leden missen in deze tests de meer fundamentele aspecten aan het (groot-schalig) gebruik van de id-wallets. Klopt het dat er niet wordt getest op de sociaal-maatschappelijke aspecten van het (groot-schalig) gebruik van een id-wallet?

De Large Scale Pilots die door de Europese Commissie zijn uitgeschreven beproeven voornamelijk de technische, functionele en juridische aspecten voor een nationale en grensoverschrijdende werking van de verschillende wallets. De pilots worden uitgevoerd met testdata in een testomgeving met een gesloten groep testgebruikers (hetgeen voldoende is om de technische functionaliteiten te beproeven). Sociaal-maatschappelijke aspecten zijn in deze pilots niet meegenomen.

De leden van de ChristenUnie-fractie zouden het zeer verrijkend vinden als niet alleen technische risico's en de mate van gebruiksvriendelijkheid wordt onderzocht, maar ook een meer fundamentele risicoanalyse. Bijvoorbeeld een onderzoek naar de mogelijke gevolgen als een bepaalde dienst van een organisatie of bedrijf enkel toegankelijk is via het gebruik van een id-wallet. Is de Staatssecretaris het met deze leden eens dat bij de ontwikkeling van de Nederlandse variant van de Europese Digitale Identiteit dergelijke vragen ook een antwoord verdienen? Is de Staatssecretaris bereid dergelijke aspecten mee te nemen in de testen van de NL voorbeeld-wallet en de Large Scale Pilots? De leden geven de suggestie mee hierover nadrukkelijk het gesprek te voeren met ethici, filosofen en sociologen op het snijvlak van maatschappij en digitalisering.

Zoals aangegeven bij de beantwoording van de tweede vraag van de leden van de GroenLinks-PvdA-fractie stelt de verordening als eis dat het gebruik van de EDI-wallets vrijwillig is en dat het mogelijk blijft om via andere bestaande identificatie- en inlogmiddelen toegang te krijgen tot publieke en private diensten.

Bedrijven die gebruik willen maken van de id-wallets dienen zich te registreren in een register zodat openbaar toegankelijk is welke organisatie welke gegevens gebruikt. De leden van de ChristenUnie-fractie vragen hierover wat de verwachting is hoeveel bedrijven en organisaties hiervan gebruik willen maken. Bij welke organisatie wordt het beheer van dit register belegd?

Registratie is verplicht voordat dienstverleners gegevens bij gebruikers via een EDI-wallet mogen opvragen.

Iedere dienstverlener die gegevens bij gebruikers wil opvragen via een EDI-wallet dient zich te registreren. De verordening schrijft voor dat publieke dienstverleners, zeer grote onlineplatforms en bedrijven die diensten verlenen, waarbij «sterke gebruikersauthenticatie» voor online-identificatie op grond van een wettelijke of contractuele verplichting vereist is, op het gebied van bijvoorbeeld vervoer, energie, bankwezen, financiële dienstverlening, sociale zekerheid, gezondheidszorg, drinkwatervoorziening, postdiensten, digitale infrastructuur, onderwijs of telecommunicatie EDI-wallets moeten accepteren als de gebruiker daarom vraagt. Deze partijen dienen zich dus op voorhand te registreren.

Uiteraard zullen er ook bedrijven zijn die uit eigen beweging EDI-wallets accepteren en zich dus laten registreren. Om hoeveel bedrijven dit uiteindelijk zal gaan is op dit moment niet bekend.

Elke lidstaat moet een eigen register voor vertrouwende partijen inrichten. Het is nog niet besloten bij welke organisatie het Nederlandse register wordt belegd.

De leden van de ChristenUnie-fractie hebben ook vragen over op welke wijze de id-wallet wordt gefinancierd? Wordt het volledig publiek gefinancierd of dienen bedrijven en organisaties die gebruik willen maken van een id-wallet te betalen naar gebruik? Is de Staatssecretaris voornemens het id-wallet budget neutraal op te leveren? De leden van de ChristenUnie-fractie vragen de Staatssecretaris hierover nader uitleg te verschaffen.

De verordening bepaalt dat het uitgeven, gebruiken en intrekken van EDI-wallets voor natuurlijke personen gratis is. Voor rechtspersonen bestaat die verplichting niet.

Het is niet de bedoeling om de publieke wallet budgetneutraal te realiseren. Door deze open source te ontwikkelen wil ik vanuit de overheid bijdragen aan kennis en inzicht die publiek beschikbaar zijn en hergebruikt kunnen worden.