Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2022–2023

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

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

AB[1]

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 24 januari 2023

Hierbij bied ik u in kopie de antwoorden aan op de schriftelijke vragen met kenmerk 2022D47220 die aan mij zijn gesteld door de leden van de fracties van de VVD, D66, CDA en SP van de vaste commissie voor Digitale Zaken van de Tweede Kamer naar aanleiding van de brief Voortgangsrapportage domein Toegang (Kamerstuk 26 643, nr. 914), de brief Ministeriële Regeling met eisen aan inlogmiddelen voor burgers en bedrijven (Kamerstuk 35 868, nr. 17) en de brief interbestuurlijk toezicht onder de Wet digitale overheid (Kamerstuk 35 868, nr. 16).

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, Digitalisering en Koninkrijksrelaties
A.C. van Huffelen

[1] De letters AB hebben alleen betrekking op 34 972.

kst-34972-AB
ISSN 0921 - 7371
's-Gravenhage 2023

Beantwoording

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de stukken die staan geagendeerd voor het schriftelijk overleg «Toegang, toezicht en eisen inlogmiddelen onder de Wet digitale overheid (Wdo)» en hebben hierover nog enkele vragen en opmerkingen.

Ministeriële regeling

De leden van de VVD-fractie lezen dat wordt gewerkt met voorschriften voor het versturen van burgerservicenummers door aanbieders van inlogmiddelen. Deze voorschriften bestaan uit het werken op basis van pseudoniemen. Deze leden vragen waarom niet is gekozen voor end-to-end encryptie. Ziet de Staatssecretaris dit net als deze leden als veiligere optie? Zo ja, waarom is dan niet voor deze optie gekozen? Zo nee, waarom niet?

Ik ben het met de leden eens dat end-to-end versleuteling een veilige optie is. Dat is dan ook de optie die wordt ingezet, zodat BSN's van begin tot het eind versleuteld (als pseudoniem) worden verstuurd. Daarbij komt dat BSN's ook nu al nooit onversleuteld worden verzonden.

De leden van de VVD-fractie lezen dat aanbieders van inlogmiddelen moeten borgen dat de wijze waarop informatie aan de burger wordt getoond niet door een derde partij kan worden gemanipuleerd. Op welke manier moeten deze aanbieders de veiligheid borgen? Welke veiligheidseisen worden gesteld aan deze aanbieders?

Er worden veiligheidseisen gesteld om te zorgen dat de verbinding tussen de gebruiker, de aanbieder van het inlogmiddel en de dienstverlener veilig is. Dat gebeurt bijvoorbeeld met de eis voor een beveiligde verbinding door het gebruik van technische certificaten waardoor de systemen onderling herkenbaar zijn. Dat betekent dat de systemen van de publieke dienstverlener kunnen controleren dat gegevens ook daadwerkelijk van het systeem van de betreffende aanbieder van een inlogmiddel afkomstig zijn, en niet van een derde partij. Ook kan daardoor verzekerd worden dat de informatie die wordt uitgewisseld niet tussentijds is aangepast. Burgers en bedrijven kunnen zeker zijn (het slotje op websites), dat zij daadwerkelijk contact hebben met de dienstverlener waarmee zij zaken willen regelen en dat de informatie zoals zij die te zien krijgen juist is.

Deze leden lezen dat aan aanbieders van inlogmiddelen de verplichting wordt opgelegd om mogelijk misbruik te kunnen herstellen en herkennen. Op welke manier wordt dit getoetst? Wanneer kan een aanbieder misbruik in voldoende mate herkennen?

Het is belangrijk dat burgers en bedrijven beschermd worden op het moment dat zij slachtoffer worden van misbruik. Op dat moment moeten zij worden geholpen. Het komt voor dat zij slachtoffer worden zonder dat zij dit zelf in eerste instantie merken. Daarom is het van belang, en daarop wordt getoetst, dat aanbieders van inlogmiddelen in de systemen maatregelen hebben getroffen om fouten te kunnen reproduceren (audittrail) en signalering hebben ingericht om afwijkend (netwerk)verkeer te kunnen constateren. Dit zijn maatregelen waarop vooraf kan worden getoetst.
Misbruikbestrijding is in feite een doorlopende operationele taak. Monitoring zal doorlopend moeten worden aangepast, omdat partijen die misbruik maken voortdurend oude en nieuwe vormen van misbruik

toepassen. Ook zal in onderling overleg tussen de partijen binnen het stelsel hiernaar gekeken worden. Misbruik kan zich immers over de verschillende partijen heen uitspreiden. Hierbij zal ik als verantwoordelijke voor het stelsel ook zelf betrokken zijn.

De leden van de VVD-fractie lezen dat de Staatssecretaris gaat aansturen op dat er daadwerkelijk een community komt voor open source. Op welke manier gaat de Staatssecretaris dit aansturen? Wat als het niet lukt om een community te krijgen voor open source? Aan welke criteria moet een community doen? Kan de Staatssecretaris hierbij onder andere ingaan op het kennisniveau van de community, uit hoeveel mensen de community moet bestaan en wanneer een community goed genoeg is?

De totstandkoming van een community ga ik stimuleren, als onderdeel van mijn werkagenda. De community voor inlogmiddelen, waarnaar de leden in dit verband vragen, maakt daar onderdeel van uit, maar mijn inzet is breder. Conform de werkagenda zal daar waar dat kan, gewerkt worden met open source, met open data, open algoritmen en open beleidsregels. Rondom alle activiteiten, of het nu bijvoorbeeld om de wallet, het algoritmeregister of inlogmiddelen gaat, zullen mensen uit de buitenwereld betrokken worden. Online, maar ook met fysieke ontmoetingen. Daar ben ik al mee gestart als het gaat om de Europese digitale identiteit. Ik zal ervoor zorgen dat die communities geen losse eilandjes zijn, maar onderling verbonden worden. Dat zogenaamde communitymanagement zal actief vanuit het ministerie worden opgepakt.
Met deze maatregelen borg ik dat er een community ontstaat rond de bij inlogmiddelen gebruikte open source softwarecomponenten.

De leden van de VVD-fractie lezen dat per component van de inlogdienstverlening besloten wordt of en wanneer een component open source moet zijn. Hiervoor is een redelijke termijn nodig om de software om te zetten in open source. Hoe ziet deze overgangstermijn eruit?

Burgers moeten over een inlogmiddel kunnen blijven beschikken in deze overgangsfase. In de bijlage bij de ministeriële regeling wijs ik softwarecomponenten van inlogmiddelen aan waarvan de broncode gepubliceerd moet zijn. Dit betreft de componenten die persoonsgegevens verwerken. Elke aanwijzing voorzie ik van een ingangsdatum. Vanaf dat moment moeten partijen die een erkenning aanvragen of al over een erkenning beschikken, voor dat component gebruik maken van gepubliceerde broncode.
Voor het bepalen van de ingangsdatum hanteer ik het redelijkheidscriterium. Wat een redelijke overgangstermijn is, verschilt per component. Ik win hiervoor kennis in bij experts. Het uitgangspunt is dat de overgangstermijn per component zo kort mogelijk is, maar voldoende ruimte biedt om de voornoemde doelstellingen te realiseren.

Op welke manier wordt voorkomen dat burgers en bedrijven zonder hun middelen komen te zitten als gevolg van deze overgang?

De overgangsperiode dient om te voorkomen dat burgers zonder inlogmiddelen komen te zitten. Dat doe ik door – op basis van advies van experts en in overleg met de aanbieders – redelijke termijnen te stellen zodat de overgang vloeiend en realistisch kan verlopen. De continuïteit van deze inlogmiddelen, en daarmee het belang van burgers en bedrijven die er gebruik van maken, weeg ik mee bij het bepalen van de redelijke overgangstermijn.

De leden van de VVD-fractie lezen in artikel 4.5 dat beveiligingsincidenten gemeld moeten worden bij de Minister van Binnenlandse Zaken en

Koninkrijksrelaties. Is overwogen om beveiligingsincidenten te melden bij zowel de Minister als het Agentschap Telecom? Zo nee, waarom niet?

In het kader van het toezicht zijn bedrijven gehouden om zaken die de goede werking raken te melden bij de toezichthouder. Dat is gedaan om te zorgen dat naar de toekomst toe verbeteringen kunnen worden doorgevoerd. De toezichthouder kan indien nodig maatregelen nemen. Daarnaast is het nodig om beveiligingsincidenten te melden bij de Minister van BZK, omdat incidenten bij een schakel in het stelsel, gevolgen kunnen hebben voor andere schakels in het stelsel. Dat betekent dat ook de Minister van BZK vanuit zijn stelselverantwoordelijkheid maatregelen moet en zal nemen als dat nodig is.

Voortgangsrapportage domein toegang

De leden van de VVD-fractie lezen dat sms-authenticatie voorlopig behouden blijft. In welke gevallen blijft het mogelijk om middels sms-authenticatie in te loggen bij de overheid? Denkt het kabinet na over andere mogelijkheden dan sms-authenticatie gezien de risico's die daaraan verbonden zijn?

Zoals ik uw Kamer eerder heb gemeld, onder andere op 5 oktober jl,[2] blijft inloggen met sms-authenticatie (tweefactorauthenticatie) mogelijk in de gevallen dat authenticatie bij dienstverleners op niveau laag plaatsvindt. Zoals u bekend wordt ook tweefactorauthenticatie door eIDAS geclassificeerd als niveau laag. Naast sms-authenticatie is het ook mogelijk om in te loggen via de DigiD-app. Ook dit gebruik van de DigiD-app is tweefactorauthenticatie en daarmee niveau laag. Met de DigiD-app kan ook op een hoger betrouwbaarheidsniveau (substantieel of hoog) ingelogd worden, mits aangevuld met een eenmalige controle van een wettelijk identiteitsdocument. De betrouwbaarheidsniveaus substantieel en hoog bieden een betere beveiliging dan inloggen met gebruikersnaam en wachtwoord, ook als dit wordt aangevuld met tweefactorauthenticatie. Als burgers hulp nodig hebben bij het gebruik van de genoemde middelen, dan kunnen zij onder andere terecht bij de Informatiepunten Digitale Overheid in bibliotheken.[3]

De leden van de VVD-fractie weten dat het voor veel wettelijk vertegenwoordigers belangrijk is om digitaal zaken te doen namens een ander. De planning is erop gericht om dit in het jaar 2024 gereed te hebben. Wanneer in 2024 zal dit het geval zijn? Het zou mooi zijn als dit begin 2024 zo ver kan zijn en niet pas aan het einde van 2024, want dat is nog twee jaar van nu. Graag krijgen deze leden een reactie.

Mensen die onder curatele of bewind staan, of een mentor hebben of minderjarig zijn, mogen niet in alle gevallen zelf diensten afnemen van de overheid. Hun wettelijk vertegenwoordigers doen dit namens hen. Dit moet ook digitaal kunnen. Samen met de Rechtspraak werk ik aan het digitaal ontsluiten van informatie over curatele, bewindvoering en mentorschap. De Rechtspraak benoemt in dezen de wettelijk vertegenwoordiger en houdt hier toezicht op. Om in dat kader digitaal te kunnen communiceren met de curator, bewindvoerder of mentor realiseert de Rechtspraak in stappen een centraal systeem (systeem Toezicht). In dit systeem worden onder meer de unieke identificerende gegevens

---

[2] Antwoord op vragen van het lid Leijten over het nieuws dat de SMS-controle van DigiD wordt uitgefaseerd, 2022Z09543, 8 juli 2022 en Kamerbrief Voortgangsrapportage domein Toegang, Kamerstuk 26 643, nr. 914, 26 september 2022.

[3] Kamerbrief Informeren burgers over verhoging authenticatieniveau, Kamerstuk 26 643, nr. 942, 22 november 2022.

vastgelegd die nodig zijn om een wettelijk vertegenwoordiger en de vertegenwoordigde te kunnen identificeren. In het begin van 2023 zijn alle bewindvoerders (professioneel en particulier) voor zover zij digitaal communiceren met de Rechtspraak opgenomen in dit systeem. De planning is dat later dit jaar ook de curatoren zijn opgenomen en vanaf begin 2024 ook de mentoren.
Voor het ontsluiten van informatie over ouderlijk gezag uit de BRP werk ik samen met het Ministerie van J&V. De hiervoor gerealiseerde oplossing is recentelijk beproefd door de jeugdbeschermingsketen en wordt nu verder getest in de zorgsector. Ikzelf draag zorg voor het maken van ICT-voorzieningen die de benodigde registers kunnen bevragen en verklaringen over bevoegdheden kunnen verstrekken aan de dienstverleners. Publieke dienstverleners, zoals de Belastingdienst, zorginstanties, gemeenten en het UWV, hebben ook een rol. Zij moeten ervoor zorgen dat hun systemen aangesloten zijn op de ICT-voorzieningen en dat wettelijk vertegenwoordigers bij hen terecht kunnen om diensten namens een ander af te nemen. Het betreft dus een hele keten die goed en vooral zorgvuldig ingericht moet worden. Niet alleen technisch, maar ook juridisch. De waarborgen moeten immers goed geregeld zijn en blijven.

Deze leden hebben tenslotte kennisgenomen van het besluit van het kabinet om de compensatieregeling voor ondernemers voor het gebruik van het inlogmiddel eHerkenning met ingang van 1 oktober 2022 met twee jaar te verlengen. Deze leden vragen of de Staatssecretaris voornemens is om deze compensatieregeling te handhaven na twee jaar, als er na deze twee jaar nog steeds geen gratis publiek alternatief is.

Ja, ik zal de compensatieregeling verlengen totdat er een gratis publiek alternatief beschikbaar is.

Vragen en opmerkingen van de leden van de D66-fractie

De leden van de D66-fractie hebben met interesse kennisgenomen van de stukken over de uitvoering van Wet digitale overheid (Wdo) en hebben vragen over de uitvoering van de extra eisen die opgenomen zijn in de novelle.

Regeling nadere eisen identificatiemiddelen, authenticatiediensten en machtigingsdiensten Wdo

Artikel 1.1 Begripsbepalingen en artikel
Artikel 2.5 Gebruik van software met openbare broncode

De leden van de D66-fractie merken op dat de begrippen openbare broncode en open source hier door elkaar worden gebruikt. Sterker nog, het lijkt alsof het hier om hetzelfde gaat. Deze leden zijn het hier niet mee eens. Open source is iets anders dan openbare broncode. De leden van de D66-fractie vragen ook waarom het begrip open source niet hier gedefinieerd is.

Allereerst is het goed te benadrukken dat «open source» een veelzijdig begrip is, dat verschillend wordt gebruikt en begrepen. De regeling vertrekt vanuit de doelen die het kabinet nastreeft met het toepassen van open source. Het voornaamste doel dat het kabinet in dit geval voor ogen staat is om transparantie te realiseren over de werking van inlogmiddelen. Zo is voor eenieder kenbaar hoe inlogmiddelen werken, en is daarmee controleerbaar hoe de verwerking van persoonsgegevens plaatsvindt. Dit doel wordt bereikt door de broncode te publiceren. Van belang is daarbij dat dit op een zodanige manier gebeurt dat deze broncode daadwerkelijk raadpleegbaar en controleerbaar is. Hiermee regel ik de aspecten die

belangrijk zijn vanuit het doel, namelijk transparantie van software die wordt gebruikt. Daardoor is het niet nodig om open source te definiëren.

Hoe heeft de Staatssecretaris in deze regeling invulling gegeven aan de motie-Dekker-Abdulaziz over een «open source, tenzij»-principe opnemen in de Wet digitale overheid (Kamerstuk 35 868, nr. 11)?

Het open source, tenzij- principe is als gevolg van de motie-Dekker-Abdulaziz vastgelegd in de eisen voor identificatiemiddelen. In de algemene maatregelen van bestuur (AMvB's) is vastgelegd dat voor aangewezen componenten van een inlogmiddel software moet worden gebruikt waarvan de broncode openbaar is. Componenten moeten op basis van die regels worden aangewezen tenzij dit onwenselijk is vanwege de veiligheid, de continuïteit of de beschikbaarheid van het aanbod van inlogmiddelen. In de aanbiedingsbrief bij de ministeriële regeling (Kamerstukken II, 35 868, nr. 17) heeft u de aangepaste artikelen ontvangen.

Artikel 3.1

De leden van de D66-fractie hechten veel waarde aan de «privacy bij design»-eis die in de novelle van de wet is toegevoegd. Bij de toelichting van artikel 3.1 derde lid op pagina 66 staat dat een Data protection impact assessment (DPIA) wordt geëist in de ministeriële regeling. Deze leden vinden dit een goed plan, maar vragen de Staatssecretaris waarom dit niet gewoon in deze bewoording ook in de ministeriële regeling staat.

Inhoudelijk ben ik het met de leden eens. Het komt op hetzelfde neer. De Algemene Verordening Gegevensbescherming hanteert in de tekst de term «gegevensbeschermingseffectbeoordeling». Dit komt overeen met wat in de praktijk bekend staat als een Data protection impact assessment (DPIA). Uit oogpunt van regelgeving is in de tekst van de ministeriële regeling de term «gegevensbeschermingseffectbeoordeling» aangehouden, en in de toelichting het meer gangbare «DPIA» gebruikt.

Verhandelverbod (novelle)

Zowel in brief en verschillende toelichtingen komen de leden van de D66-fractie het verhandelverbod tegen. Dit sluit goed aan bij het debat en bij de wet. Echter zien deze leden ook hier geen woord over de ministeriële regeling. Er wordt geschreven dat het verder uitgewerkt wordt, maar die uitwerking ontbreekt. Kan de Staatssecretaris toelichten waar en hoe het verhandelverbod uitgewerkt wordt? Hoe gaat deze eis bijvoorbeeld uitzien bij een aanbesteding?

In de Wet digitale overheid is precies vastgelegd waarvoor aanbieders van inlogmiddelen gegevens van burgers en bedrijven mogen gebruiken. Namelijk: inlogmiddelen uitgeven, burgers en bedrijven laten inloggen bij de overheid en hen ondersteunen bij eventuele problemen. Als aanbieders van inlogmiddelen zich hier niet aan houden, dan overtreden zij de AVG (doelbinding). Materieel wordt het verbod nader geregeld in de uitvoeringsregelgeving, in de AMvB's voor burgermiddelen en bedrijfsmiddelen. Op basis van de ministeriële regeling dienen toegelaten aanbieders zich aan het verhandelverbod te houden. Bij de toelating, maar ook daarna, wordt daarop gecontroleerd en zal ik bij overtreding hiervan handhaven.

Vragen en opmerkingen van de leden van de CDA-fractie

De leden van de CDA-fractie hebben kennisgenomen van de verschillende kabinetsbrieven die zien op de toegang tot, toezicht op en eisen aan inlogmiddelen onder de Wet digitale overheid (Wdo). Deze leden hebben hierover nog enkele vragen.
De leden van de CDA-fractie hechten eraan om te blijven benadrukken dat onder de Wet digitale overheid de burger niet verplicht zijn om digitaal zaken te doen met de overheid, maar dat burgers en bedrijven het recht hebben om digitaal zaken te doen met de overheid en dat het belangrijk is dat dit veilig, betrouwbaar en gebruiksvriendelijk gebeurt. Deze leden lezen in de brief over de Voortgangsrapportage Domein Toegang dat de aansluiting van alle overheidsorganisaties op het nieuwe stelsel naar verwachting in de tweede helft van 2026 volledig afgerond zal zijn. Deze leden vragen of deze zinsnede ziet op het volledige nieuwe stelsel, of dat dit alleen ziet op het deel van het stelsel dat ziet op de toegang via een machtiging. Deze leden vragen of de Staatssecretaris nader kan toelichten waarom het tot 2026 duurt voordat de volledige aansluiting is afgerond.

Vooropgesteld: het recht, dus niet de plicht, op digitaal diensten afnemen van de overheid wordt geregeld in het voorstel Wet modernisering elektronisch bestuurlijk verkeer. Het voorstel Wet digitale overheid regelt enkel dat het afnemen van diensten bij publieke dienstverleners, veilig kan.
De zinsnede ziet op het volledig nieuwe stelsel van Toegang inclusief machtigen. De volledige aansluiting duurt nog geruime tijd omdat de inwerkingtreding van de Wet digitale overheid niet met een «big bang» gepaard gaat. De organisatorische en technische inrichting van het stelsel kan het komende jaar worden afgerond nu er duidelijkheid komt over het juridische kader dat de wet geeft inclusief de lagere regelgeving. Daarnaast wordt bij de introductie van het nieuwe stelsel rekening gehouden met de uitvoeringspraktijk en vervangingsinvesteringen die de overheidsdienstverleners moeten doen.

De leden van de CDA-fractie lezen in de brief de passage: «Concreet betekent de invoering van het stelsel Toegang dat een burger of bedrijf naast respectievelijk DigiD of eHerkenning zelf kan kiezen wat voor middel (publiek of privaat) gebruikt wordt om bij verschillende overheidsdienstverleners in te loggen.» Deze leden vragen de Staatssecretaris in hoeverre er op dit moment keuzevrijheid is voor bedrijven, met name tussen een privaat of een publiek middel. Deze leden vragen of de Staatssecretaris kan aangeven of er een publiek inlogmiddel voor bedrijven komt, en hoe zij bovengenoemde keuzevrijheid voor bedrijven waarborgt.

Op dit moment is er een beperkte keuzevrijheid voor bedrijven. Om in te loggen bij de overheidsdienstverlening dient er gebruik te worden gemaakt van eHerkenning, dat in een publiek private samenwerking wordt uitgegeven. De Wdo maakt het mogelijk dat er ook nieuwe private aanbieders in het bedrijvendomein hun diensten kunnen aanbieden. Daarnaast wordt gewerkt aan de introductie van een publiek middel voor bedrijven om toegang te krijgen tot de digitale dienstverlening van de Belastingdienst. De bredere inzetbaarheid van het publieke bedrijfsmiddel bij andere overheidsdienstverleners vergt nog nadere uitwerking en zal geregeld worden in de tweede tranche van de Wdo.

De leden van de CDA-fractie vragen of de Staatssecretaris nadenkt over een minimum en/of een maximum aan het aantal publieke en private inlogmiddelen, vanuit het oogpunt van eenvoud voor burgers en bedrijven en effectief en efficiënt toezicht vanuit het Agentschap Telecom.

Ik heb geen minimum- of maximumaantal aanbieders voorzien. Iedereen mag meedoen. Alleen is in ieder geval een publiek middel randvoorwaardelijk.

De leden van de CDA-fractie vragen hoe vaak sms-authenticatie nog wordt gebruikt als tweefactorauthenticatie bij het inloggen met DigiD. Deze leden vragen of de Staatssecretaris kan toelichten voor welke overheidsdiensten inloggen via sms-authenticatie naar verwachting straks niet meer mogelijk is. Deze leden vragen ook of het niet omslachtig is om deze groep op termijn gebruik te laten maken van een machtiging, en of het niet veel effectiever is om ervoor te zorgen dat nog veel meer mensen de ID-check toevoegen en welke stappen de Staatssecretaris hiertoe zet.

Op dit moment maken 11 miljoen van de actieve 16,5 miljoen DigiD-accounts gebruik van de DigiD-app. De overige accounts maken alleen gebruik van gebruikersnaam en wachtwoord, al dan niet in combinatie met sms-authenticatie. De 215.000 mensen die nog geen gebruik maken van tweefactor-authenticatie worden geïnformeerd dat veiliger gebruik van de dienstverlening noodzakelijk is, wat zij kunnen doen om een middel met een hoger betrouwbaarheidsniveau te krijgen en hoe zij hiermee geholpen kunnen worden. In de beschikbare communicatie over DigiD wordt de app expliciet onder de aandacht gebracht.[4]
SMS-authenticatie blijft sowieso mogelijk zolang er diensten op betrouwbaarheidsniveau laag worden aangeboden. Gelet op de hiervoor genoemde aantallen is het gebruik en de bekendheid met de DigiD-app groot. Het vaststellen van het betrouwbaarheidsniveau van elektronische diensten is aan de dienstverlener. Het benodigde betrouwbaarheidsniveau hangt onder andere af van de gevoeligheid van de gegevens die ontsloten worden. Zo kan ik me voorstellen, gezien de gevoeligheid van medische gegevens, dat die in de toekomst door zorgverleners worden aangeboden op de niveaus substantieel en hoog.
Het is niet zo dat de machtigingsfunctie als het dwingende alternatief voor de sms-authenticatie wordt gepresenteerd. De machtigingsfunctie is er eerder voor de doelgroep die een bepaalde overheidsdienstverlening aan een ander wil overdragen, zoals bijvoorbeeld het doen van belastingaangifte.

De leden van de CDA-fractie hebben nog enkele vragen over de brief Ministeriële regeling met eisen aan inlogmiddelen voor burgers en bedrijven. Deze leden vragen in het kader van het verhandelverbod of de Staatssecretaris een voorbeeld kan geven van een situatie waarin een partij via andere (commerciële) dienstverlening kan beschikken over persoonsgegevens van een gebruiker. Deze leden vragen bovendien hoe de mogelijkheid voor een gebruiker om verstrekking aan derden te beëindigen er precies uit komt te zien en wat een gebruiker daar zelf voor moet doen.

In bepaalde gevallen zal een aanbieder van inlogmiddelen naast inlogdienstverlening ook andere diensten verlenen. Hierbij kan bijvoorbeeld gedacht worden aan een bank. Voor de reguliere dienstverlening van de bank beschikt de bank al over persoonsgegevens van haar klanten, zoals identificerende, betaal- en inkomensgegevens. Juist in dergelijke situaties acht ik het van het grootste belang dat gebruiks- en gebruikersgegevens van inlogdienstverlening niet gekoppeld kunnen worden aan andere gegevens. Om die reden heb ik een stevig verhandelverbod en strikte doelbinding verankerd in de wet.

---

[4] Kamerbrief Informeren burgers over verhoging authenticatieniveau, Kamerstuk 26 643, nr. 942, 22 november 2022.

De mogelijkheid voor de gebruiker om verstrekkingen aan derden te beëindigen is bedoeld als derde slot op de deur naast de twee voornoemde wettelijke waarborgen. Het betreft in feite een vangnetbepaling. De gebruiker kan een beroep doen op de verplichte bepaling in de gebruikersovereenkomst door de aanbieder van inlogmiddelen schriftelijk te verzoeken om te stoppen met de verstrekking. Dit past in het streven om burgers meer regie op hun gegevens te bieden. Indien de aanbieder hier geen gehoor aan geeft, dan voldoet hij niet aan de voorwaarden van de erkenning. De gebruiker kan dit aan mij melden en dit stelt mij in staat om passende maatregelen te treffen, zoals het opleggen van een boete of het intrekken van de erkenning.

De leden van de CDA-fractie constateren dat nog niet duidelijk wordt hoe de Staatssecretaris wil omgaan met het vormen van communities die meekijken op de software. Deze leden vragen of de Staatssecretaris, zoals ook gevraagd in het debat van 1 juni 2022, wil verduidelijken of en hoe zij dergelijke communities gaat stimuleren, en welke concrete stappen zij hiertoe in de komende periode zet.

Ik verwijs de leden naar mijn eerder gegeven antwoord op de soortgelijke vraag van de VVD.

Vragen en opmerkingen van de leden van de SP-fractie

De leden van de SP-fractie hebben de voornemens over het digitale toegangstelsel gelezen en hebben hierover nog enkele opmerkingen en vragen. Deze leden lezen dat de sms-authenticatie blijft bestaan, maar lezen tevens dat voor meerdere toepassingen dit straks onbruikbaar zal zijn. Mensen kunnen dan gebruik maken van de app, waarbij ook een controle van een identificatiebewijs gevraagd kan worden. Indien zij dit niet willen of kunnen, kunnen zij een ander digitaal machtigen. Deze leden vinden dit een grote achteruitgang in de zelfredzaamheid van mensen; mensen die de app niet veilig genoeg achten of niet werkbaar genoeg verliezen zo immers de mogelijkheid om zelf digitaal zaken te kunnen doen met de overheid. Deze leden lezen tevens dat nog niet helemaal helder is waar een fysiek alternatief niet meer mogelijk is. Zou dat niet eerst helemaal duidelijk moeten zijn, alvorens mensen die de app niet willen of kunnen gebruiken uit te sluiten van deze toepassingen? Hoe verhoudt zich het voornemen om mensen zelf regie te laten voeren op hun digitale gegevens tot het advies iemand te machtigen?

Het klopt dat sms-authenticatie blijft bestaan, maar in de toekomst voor meerdere toepassingen niet meer bruikbaar zal zijn. In het geval er over wordt gegaan van de huidige naar nieuwe niveaus zal ik dit tijdig met uw Kamer delen. Het uitgangspunt is dat digitaal moet kunnen maar niet verplicht is. Iedereen moet mee kunnen doen. Zo is het ook opgenomen in het voorstel Wet modernisering elektronisch bestuurlijk verkeer (Wmebv), dat nu in de Eerste Kamer ligt. Dit wetsvoorstel biedt mensen het recht om digitaal zaken te doen met de overheid, maar verplicht dit niet. Er moet altijd een ander kanaal openstaan voor mensen die niet digitaal willen of kunnen. Middels een zorgplicht moeten bestuursorganen ondersteuning bieden aan mensen die niet aan het digitale verkeer mee kunnen doen. De Wmebv zorgt ervoor dat burgers en bedrijven een betere rechtspositie hebben in het digitale contact dat zij met de overheid hebben. Om digitaal diensten af te kunnen nemen, is het belangrijk dat inloggen met DigiD bij de overheid en andere organisaties veilig, betrouwbaar en toegankelijk is en blijft. Ik realiseer mij dat digitale ontwikkelingen voor veel mensen lastig zijn. Om die reden wordt er altijd een afweging gemaakt tussen inclusiviteit van de voorziening, veiligheid en een betrouwbare identiteitsvaststelling. Als burgers hulp nodig hebben

bij het gebruik van de middelen dan kunnen zij onder andere terecht bij de Informatiepunten Digitale Overheid in bibliotheken. Als zij zelf niet langs digitale weg diensten af willen nemen, kunnen burgers ook iemand machtigen.

De leden van de SP-fractie lezen dat er wordt ingezet op een eventuele verbreding van een publiek inlogmiddel voor bedrijven. Waarvoor wordt hiervoor gekozen, nu het stelsel nog niet volledig functioneert en de wet nog niet in werking is getreden?

De keuze voor een breder beschikbaar publiek middel voor bedrijven is al eerder gemaakt in reactie op de Motie van der Molen (Kamerstukken 34 972, nrs. 32 en 53). Deze keuze heb ik bij verschillende gelegenheden herbevestigd omdat het Kabinet er aan hecht dat er altijd ook een publiek inlogmiddel is, zowel voor burgers als voor bedrijven. Op dit moment wordt gewerkt aan een publiek middel voor het inloggen bij MijnBelastingdienst Zakelijk door enkelvoudig zelfstandig bevoegde bestuurders. Het voornemen was om het publieke middel voor het inloggen bij MijnBelastingdienst Zakelijk in het eerste kwartaal van 2023 in gebruik te nemen. Gezien de afhankelijkheid hiervan van de inwerkingtreding van de Wdo, schuift de ingebruikname hiervan op. De bredere inzetbaarheid van het publieke bedrijfsmiddel bij andere overheidsdienstverleners vergt nog nadere uitwerking en zal geregeld worden in de tweede tranche van de Wdo.

De leden van de SP-fractie lezen voorts dat er per ministeriële regeling wordt geregeld dat er verplichte digitale inzage en correctie is bij aanbieders van inlogmiddelen. Als een ministeriële regeling bedoeld is om snel iets te kunnen wijzigen, wat wordt hier dan voorzien dat snel gewijzigd dient te worden? Deze leden zien dit als een fundamentele waarborg voor het functioneren van een dergelijk inlogmiddel en de juiste bescherming van mensen. Waarom is ervoor gekozen om dit niet in de wet op te nemen maar per ministeriële regeling op te nemen? Dezelfde vragen stellen zij over het herstelvermogen, de bescherming bij het inloggen en de beperking van het verwerken van het burgerservicenummer.

Ik ben het met de leden eens dat dergelijke rechten niet in een ministeriële regeling moeten worden geregeld. En dat is ook niet gebeurd. De reden waarom dit in de ministeriële regeling wordt genoemd, is omdat hierin de eisen zijn opgenomen waaraan aanbieders van inlogmiddelen worden getoetst. Door toelating worden de aanbieders hieraan gebonden en wordt gezorgd dat de rechten kunnen worden geeffectueerd (en niet gecreëerd).
De rechten die gelden voor burgers worden op een hoger niveau geregeld. Zo bevat de Algemene verordening gegevensbescherming (Avg) een inzage- en correctierecht. Dat recht geldt rechtstreeks op grond van de Avg. Ook de grondslagen voor het herstelvermogen worden niet in de ministeriële regeling geregeld (maar in de wet zelf en in het besluit digitale overheid). Datzelfde geldt voor de door de SP-fractie aangehaalde beperkingen aan het verwerken van het burgerservicenummer. Deze beperking en kadering van deze verwerkingen is opgenomen op wetsniveau, namelijk in artikel 16 van het wetsvoorstel.