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)

W[1]

MEMORIE VAN ANTWOORD

Ontvangen 10 oktober 2022

1. Inleiding

Met belangstelling heb ik kennisgenomen van de reacties en vragen van de leden van de fracties van de VVD, CDA, PvdA en GroenLinks, D66 en PVV naar aanleiding van het wetsvoorstel en de novelle.

De leden van de **VVD**-fractie hebben met belangstelling kennisgenomen van het voorstel van wet 34.972 Wet digitale overheid (Wdo) en de daaraan toegevoegde novelle 35.868 Novelle Wet digitale overheid (Novelle). Graag stellen de leden de volgende vragen die betrekking hebben op het open source aspect van het wetsvoorstel en de novelle.

De leden van de **CDA**-fractie hebben met waardering kennisgenomen van de novelle. Aangegeven is dat het hier een kaderwet betreft, waarbij de meer concrete bepalingen worden vastgelegd in AMvB's en MR's. In het kader van uitvoerbaarheid en handhaafbaarheid hebben de leden van de CDA-fractie toch enkele vragen. De leden van de fractie van **50PLUS** sluiten zich aan bij de vragen gesteld door de leden van de CDA-fractie.

De leden van de fracties van de **PvdA** en **GroenLinks** hebben de novelle met interesse gelezen en zijn tevreden met de wijzigingen van de regering, die middels de novelle worden doorgevoerd in de Wet digitale overheid inzake open source, privacy by design en het verhandelverbod inzake persoonsgegevens. Ook zijn de leden tevreden dat de regering het gros van de adviezen van de Raad van State heeft overgenomen. Toch resteren enkele vragen.

Met belangstelling hebben de fractieleden van **D66** de ontwikkelingen omtrent dit wetsvoorstel gevolgd, waarbij het indienen van de novelle door de leden als een groot pluspunt wordt gezien. Voor de leden van de D66-fractie is privacy een groot goed en zij achten het van belang om met

[1] De letter W heeft alleen betrekking op 34 972.

kst-34972-W
ISSN 0921 - 7371
's-Gravenhage 2022

de huidige digitalisering privacy te waarborgen. De leden steunen dat deze novelle beoogt het toezicht op gegevensbescherming wettelijk te verankeren, maar hebben nog wel enkele vragen over de uitvoerbaarheid van het toezicht?

De leden van de **PVV**-fractie hebben kennisgenomen van de Novelle Wet digitale overheid en het voorstel Wet digitale overheid en hebben hierover enkele vragen.

Ik dank de leden van de fracties van de VVD, CDA, PvdA en GroenLinks, D66 en PVV voor hun inbreng en graag ga ik hieronder in op deze vragen in de hoop en verwachting hiermee bij te dragen aan een spoedige behandeling van het wetsvoorstel.

Mijn antwoorden zijn in het onderstaande steeds gecursiveerd weergegeven.

2. Advies Raad van State

De leden van de **D66**-fractie zouden de regering het volgende willen voorleggen. Nadat de novelle is ingediend heeft de Raad van State nog een keer een schriftelijk advies uitgebracht. De regering stelt dat het advies en de novelle goeddeels met elkaar in overeenstemming zijn. Kan de regering in een leesbaar overzicht aangeven op welke punten het advies van de Raad van State in lijn is met de novelle en op welke punten niet?

Anders dan de leden van de D66-fractie lijken te stellen, heeft de Raad van State in het kader van de Wet digitale overheid slechts advies uitgebracht over het wetsvoorstel zelf en over de novelle. Ook heeft de Raad - wellicht doelt de fractie daarop- een rapport gepresenteerd over digitalisering in wetgeving en rechtspraak in juni 2021 waarin de Raad onder andere de Wet digitale overheid noemt. In het onderstaande overzicht van de bij de novelle gemaakte opmerkingen door de Raad, is ook aangegeven waar de opmerking in het rapport op ziet.

De Raad verleent aan de novelle een licht dictum, namelijk een dictum 2. Dat wil zeggen dat de Raad een aantal opmerkingen had bij het voorstel en adviseert daarmee rekening te houden voordat het bij de Tweede Kamer wordt ingediend. De Raad maakte de volgende opmerkingen:

Onderwerp in advies	Hoe verwerkt in novelle
Het begrip privacy by design kan beter uitgewerkt. *De Afdeling acht het van belang dat duidelijk is hoe bij de toetsing aan deze weigeringsgrond precies wordt beoordeeld of een middel aan het principe van privacy by design voldoet. In de toelichting wordt hier niet op ingegaan en evenmin is voorzien in een nadere precisering van deze eis bij algemene maatregel van bestuur.*	*De novelle is aangepast conform het advies van de Afdeling.* *Hoe is dat gebeurd?: Aanvulling van het zesde lid, onder b (weigeringsgrond), en het zevende lid (wijzigen, schorsen of intrekken van erkenning) van artikel 9, het achtste lid, onderdeel b (weigeringsgrond) van artikel 11 en het derde lid van artikel 14 (wijzigen, schorsen of intrekken van erkenning).*

Onderwerp in advies	Hoe verwerkt in novelle
Het begrip open source kan beter uitgewerkt worden *De Afdeling merkt op dat dit streven om geleidelijk over te gaan op open source software niet naar voren komt in de voorgestelde weigeringsgrond dat «onvoldoende gebruik wordt gemaakt van software die onder open source licentie is gepubliceerd».* *Bovendien biedt het wetsvoorstel niet met zoveel woorden de mogelijkheid om een erkenning in te trekken naarmate er meer aanbieders bij komen die open source software aanbieden.* *Het verbod voor private aanbieders om inloggegevens commercieel te benutten kan sluitender geregeld.* *...In de voorgestelde weigeringsgrond wordt echter gekeken naar de inkomsten die worden verkregen uit het «verhandelen of verstrekken» van gebruikersgegevens. Met deze omschrijving staat niet vast dat elke vorm van commerciële uitnutting van persoonsgegevens wordt uitgesloten. Zo zijn er bijvoorbeeld websites die geld verdienen met het plaatsen van gerichte advertenties. Bij die methode komen er geen persoonsgegevens in handen van de adverteerders, tenzij de bezoeker van de website zelf op de advertentie klikt. De Afdeling adviseert het verhandelverbod op een meer sluitende manier te omschrijven.*	*Novelle en toelichting bij novelle zijn aangevuld* *Hoe is dat gebeurd?: Het zevende lid van artikel 9 en het derde lid van artikel 14 zijn aangevuld, ter verankering van de bevoegdheid om een verleende erkenning te wijzigen, schorsen of in te trekken naarmate open source meer gemeengoed is.* *In de toelichting bij de novelle is aangegeven hoe de weigeringsgrond ter zake wordt toegepast en welke wegingsfactoren daarbij gelden.* *De toelichting bij de novelle is aangevuld. Er zijn hierbij geen andere eisen gesteld die gaan over commerciële uitnutting van persoonsgegeven. Dit valt buiten de scope van het reguleren van inlogmiddelen, daar is de Wdo de plek derhalve niet voor en het valt ook buiten de bevoegdheid van de Minister van BZK.*

Onderwerp in advies	Hoe verwerkt in novelle
Het voorstel is niet techniekafhankelijk opgezet *Verder constateert de Afdeling dat het voorstel techniekonafhankelijk is opgezet en daardoor onvoldoende uitwerking geeft aan het primaat van de wetgever. In verband met die opmerkingen is aanpassing van het voorstel en de toelichting wenselijk.* *Bepaalde begrippen zouden in de wet moeten worden opgenomen* *De Afdeling achtte het echter aannemelijk dat MijnOverheid en het BSN-Koppelregister, die een centrale plaats innemen in de communicatie tussen overheid en burger, de komende jaren zullen blijven bestaan. Daarom adviseerde zij deze centrale onderdelen van de generieke digitale infrastructuur in de wet zelf te regelen.*	*Niet overgenomen: Er is bewust gekozen voor een techniekonafhankelijke formuleringen* *Er is sprake van een functionele formulering, waarbij met betrekking tot de GDI-voorzieningen wordt omschreven wat doel en werking(ssfeer) ervan zijn; de wet bepaalt in artikel 5, eerste en tweede lid, waartoe de voorzieningen dienen en wat deze (moeten) kunnen. Deze wettelijke kaders vormen de hoofdelementen van de materie, zijn normatief en concreet voor wat betreft werkingssfeer en begrenzing.* *Kortom: we regelen de waarborgen rondom de functionaliteiten die worden gebruikt, niet de techniek die die functies invult. Dat is verstandig, want als de techniek wijzigt, blijven de waarborgen gelden.* *Niet overgenomen: De namen noemen is onwenselijk want niet toekomstbestendig, en biedt anderzijds geen zekerheid over de eisen aan deze voorzieningen. De artikelen bevatten deze inkadering wel en zijn voldoende concreet en afgebakend.* *Duidelijk is wat er onder moet worden volstaan en welke functionaliteit de Minister moet verzorgen; het is niet nodig en niet wenselijk om in de wet de voorzieningen met een door de techniek ingegeven benaming aan te duiden. Dit zou belemmerend zijn, zowel voor ontwikkeling als technische waarborgen. Als er een techniek beschikbaar komt die de burger beter beschermt, wil ik deze snel kunnen inzetten zonder daarvoor eerst de wet te hoeven aanpassen. De nadere uitwerking geschiedt op het niveau van – aan het parlement voorgelegde – AMvB, waarbij de voorzieningen wel bij naam worden aangeduid. Op deze wijze is de wet niet abstract – dat zou afbreuk doen aan de duidelijkheid en rechtszekerheid – maar techniekonafhankelijk en daardoor tot op zekere hoogte toekomstbestendig en kan, op democratisch gelegitimeerde wijze, worden ingespeeld op (onder andere technische) ontwikkelingen.*

In het rapport over digitalisering in wetgeving en rechtspraak gaat de Raad eveneens in op de keuze tussen techniekafhankelijk en techniekonafhankelijk formuleren van wetgeving. De Raad zegt daar op p. 123 over: «Voor deze dilemma's bestaat geen standaardoplossing. Telkens zal de wetgever een afweging moeten maken tussen de mate van techniekafhankelijkheid en van techniekonafhankelijkheid en tussen de mate van regeling in de wet en van delegatie naar lagere regelgeving. Op deze twee «assen» ware telkens de juiste balans te vinden, gegeven de te regelen vraagstukken. In de toelichting op wet- en regelgeving kan worden onderbouwd hoe in het voorstel deze balans is gevonden. Dit biedt aan het parlement een aanknopingspunt om zich hier expliciet over uit te laten. De rechtszekerheid zal in ieder geval voorop moeten staan: burgers mogen naar eigen inzicht handelen tenzij dit in strijd is met duidelijke, concrete wettelijke regels. Dit uitgangspunt kan in het gedrang komen wanneer de wetgever een uitweg zoekt in onbepaalde begrippen en de invulling overlaat aan de al dan niet digitale uitvoering. De Afdeling adviseert daarom om techniekonafhankelijk regelgeven slechts daar toe te passen waar dit aantoonbaar het beoogde doel bereikt. Zo niet, dan is tenminste uiterste terughoudendheid geboden.»

In de wetsbehandeling van de Wdo en de novelle is dit vraagstuk meerdere malen ter sprake gekomen. Mijn voorganger en ik hebben hierbij steeds betoogd dat de voorliggende regels voldoende duidelijk en concreet zijn. Daarnaast is aan het door de Raad bij dit vraagstuk genoemde bezwaar van ontbreken van parlementaire betrokkenheid bij delegatie ondervangen door de gecontroleerde delegatie die het wetsvoorstel kent. De Tweede Kamer heeft ingestemd met de door de regering gemaakte keuze. Het is nu aan uw Kamer. Bij de beantwoording van de vraag van GroenLinks over de vormgeving van de regels over open source, ga ik nader in op dit vraagstuk.

3. Open source

De regering stelt dat software open source is wanneer de broncode publiek gemaakt is en als er sprake is van een gemeenschap die zich bezighoudt met het controleren en verbeteren van de open source software. De leden van de **VVD**-fractie vragen de regering om een verduidelijking wanneer aan deze twee criteria wordt voldaan.

Allereerst is het goed te benadrukken dat «open source» een veelzijdig begrip is, dat verschillend wordt gebruikt en begrepen. Ik zal in deze beantwoording vertrekken 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 daadwerkelijk raadpleegbaar en controleerbaar is.

Het begrip open source vindt zijn oorsprong in de juridische verschijningsvorm van softwarecode en de rechten die worden toegekend. De programmeur (of de organisatie waar deze voor werkt) heeft het auteursrecht op de broncode die hij maakt. Net als een schrijver dat heeft op een boek.

Op basis van zijn auteursrecht kan hij ervoor kiezen rechten toe te kennen aan anderen, of daar voorwaarden aan te stellen. De auteursrechthebbende bepaalt zelf welke rechten hij toekent en welke voorwaarden hij stelt.

Leveranciers van inlogmiddelen kunnen transparantie bieden door op een voor eenieder toegankelijke plaats op het internet de broncode te publiceren.

Een ander open source doel dat in dit wetstraject is geformuleerd is het scheppen van de mogelijkheid dat derden verbetervoorstellen kunnen doen. Hiertoe moet ook de mogelijkheid geboden worden aan derden om – in eigen beheer – verbeteringen te kunnen testen. Leveranciers kunnen beperkingen in de licentie opnemen ten aanzien van (commercieel) hergebruik.

Wat betreft de aanwezigheid van een gemeenschap die zich bezighoudt met het controleren en verbeteren van de open source software, neem ik dit antwoord te baat om daarover een aantal zaken te verduidelijken. Waar het in de kern om gaat is dat de software veilig is, onderhouden wordt, en beschikbaar is en blijft.

Open source software (de broncode) is geen dienst. Om software in te kunnen zetten voor dienstverlening is (veel) meer nodig. Ter vergelijking: een CV-ketel is niet te gebruiken zonder dat deze wordt geïnstalleerd en regulier onderhoud krijgt. Zo zal er hosting moeten zijn om de broncode te kunnen installeren. Maar ook beheerders die zorgen dat de software blijft draaien. Er zullen audits moeten worden gedaan die aantonen dat de software veilig is. Daarvoor kan een bedrijf worden ingeschakeld dat dit organiseert, of het kan onder eigen verantwoordelijkheid (bijvoorbeeld door de overheid zelf) worden gedaan. Een voorbeeld van dit laatste is de Coronamelder App. Een essentiële randvoorwaarde is dat de software wordt onderzocht, onderhouden en verbeterd door een voldoende grote groep van actieve ontwikkelaars. Dit kan – en zal vaak – een bedrijf zijn dat de software heeft ontwikkeld of dat het onderhoudt of ondersteuning van bepaalde open source software als dienst aanbiedt. De sterkte, activiteit en omvang van de ondersteuning zijn randvoorwaardelijk voor de kracht en meerwaarde van een open source project. Is die ondersteuning er niet, dan vervalt het voordeel en kan er zelfs een risico ontstaan omdat veiligheidsproblemen niet opgemerkt worden en door kwaadwillenden benut kunnen worden.

In het geval van toegelaten inlogmiddelen zal het de leverancier van het inlogmiddel in kwestie zijn die ervoor moet zorgen dat de onderdelen van diens software op de bovenstaande manier worden beheerd. Dit vormt vanzelfsprekend (bij zowel gesloten als open software) onderdeel van de verantwoordelijkheid van leveranciers om te zorgen voor een deugdelijk product. Het gebruiken van veilige en betrouwbare softwarecomponenten maakt onderdeel uit van de verantwoordelijkheid van de aanbieder om veilige en betrouwbare dienstverlening aan te bieden binnen de eisen zoals gesteld in de ministeriële regeling.

Bovenstaande laat zien dat een open gemeenschap vraagt om andersoortig beheer dan een «gesloten gemeenschap» (lees: de interne organisatie van de leveranciers en diens eventuele onderaannemers). Aangezien het altijd de verantwoordelijkheid is van een aanbieder om de veiligheid en betrouwbaarheid te borgen, worden voor de aanbieder geen nadere eisen gesteld aan, of de aanwezigheid van een community en derhalve ook niet aan de omvang en samenstelling van de open gemeenschap. Het doel is niet om bedrijven mensen van buiten hun organisatie de software te laten (mee)onderhouden. Dat moet de aanbieder, zoals gezegd, zelf doen. De aanbieder is daarop aanspreekbaar.

Dit staat echter los van het belang dat ik hecht aan de aanwezigheid van een community. Het moge duidelijk zijn dat willen we de verschillende mogelijkheden (en aldus de voordelen) van open source benutten, enkel de code openbaar maken niet volstaat.

De regering ziet zoals gezegd derden die de gepubliceerde broncode kunnen onderzoeken, waardoor de leverancier de code beter kan onderhouden en verbeteren, als een belangrijke aanvullende waarborg voor de veiligheid. Immers, hoe groter en sterker de gemeenschap hoe groter de kans dat onverhoopte veiligheidsproblemen aan het licht komen voordat kwaadwillenden er gebruik van (kunnen) maken. Het voordeel van het meer-ogenprincipe, het bereiken van meer veiligheid doordat iedereen kan meekijken, wordt immers groter als de gemeenschap groter is. Andere voordelen die zich d.m.v. open source manifesteren zijn een groter publiek vertrouwen in het middel, het verlagen van de drempels tot samenwerking en het bevorderen van interoperabiliteit.

Om deze voordelen te behalen is het regelen van transparantie als verplichting voor de aanbieders alleen niet voldoende. Het is, zoals ik tijdens de plenaire behandeling van novelle op de wet digitale overheid in de Tweede Kamer heb aangegeven, belangrijk dat er ook echt een community is of komt die daadwerkelijk actief meekijkt op de software. Dat voorkomt dat de geschetste voordelen van de geboden transparantie niet behaald worden. Om deze reden ga ik zelf stimuleren dat er een community komt die meekijkt op alle bij inlogmiddelen gebruikte softwarecomponenten. Hoe en in welke mate of vorm stimulering nodig is zal ik bezien in het licht van de ontwikkeling. Ik heb ter ondersteuning van de positie van de community en om te zorgen dat aanbieders meewerken, uitdrukkelijk in de ministeriële regeling opgenomen dat aanbieders aan derden een mogelijkheid moeten bieden om kwetsbaarheden van de software te melden en voorstellen te doen voor aanpassing van die software. Ook wordt geregeld dat de aanbieder adequaat moet reageren op die voorstellen en aan de melder moet terugkoppelen tot welke handelingen de melding heeft geleid.

Wat betekent de «richting inzetten naar gebruik van open source» voor de vereisten die worden vastgesteld in de ministeriële regeling inzake open source? Is de regering voornemens deze regeling periodiek te herzien?

Open source werken wordt meer en meer de standaard in overheidsland. De ministeriële regeling waarin de eisen aan inlogmiddelen worden opgenomen, maakt het mogelijk om dat beheerst te kunnen doen en faciliteert een groeimodel, zodat de veiligheid en continuïteit van toegang tot digitale diensten van (semi-)publieke dienstverleners niet in het geding komen. Voor de (inhoudelijke) eisen die aan open source worden gesteld heeft dit geen gevolgen, maar wel voor het tijdstip waarop deze eisen gaan gelden. Dat kan verschillen, waarbij geldt: zo snel als het kan, maar zo beheerst als het moet.

Dit groeimodel wordt in de conceptregeling Eisen identificatiemiddelen Wdo vormgegeven door een proces waarin stapsgewijs componenten die gebruikt worden voor de verwerking van persoonsgegevens ten behoeve van inlogdienstverlening aan te wijzen waarvan de broncode open source moet zijn vanaf dat moment. Van deze componenten kunt u op dit moment kennis nemen vanwege de voorlegging van de ministeriële regeling hierover aan beide Kamers. Deze componenten dienen door de aanbieder – dan wel een derde auteursrechthebbende – gepubliceerd te zijn. Het is goed denkbaar dat een aanzienlijk deel van de componenten al bij de toetreding tot het stelsel open source is. Daarom dient de aanbieder ten behoeve van die toetreding tevens een overzicht van zijn functionele componenten en de software die daarvoor wordt gebruikt aan de toezichthouder, het Agentschap Telecom, ter toetsing te verstrekken.

De aanwijzingen en ingangsdatums van de open source componenten zullen worden vastgelegd in de bijlage bij de ministeriële regeling. Om te zorgen dat met deze aanwijzing zal worden voldaan aan de vereisten van veiligheid, continuïteit en een breed beschikbaar aanbod van inlogmiddelen, is het nodig om hierover tevoren kennis in te winnen bij experts. Gedurende de internetconsultatie van de regeling zullen deze hierop actief door mij worden bevraagd.

De aanwijzing van componenten en systemen in de regeling vindt vervolgens plaats nadat ik mij heb laten adviseren door experts met kennis van zowel open source software als de (werking van) inlogmiddelen. Door deze experts wordt ook na de eerste vaststelling van de regeling waarin de eerste componenten en datums al worden aangewezen regelmatig bekeken of en zo ja, per wanneer publicatie van de

broncode van componenten mogelijk is en dus nieuwe aanwijzing in de bijlage kan plaatshebben. Hierbij wordt rekening gehouden met de veiligheid en continuïteit. Daarbij houd ik bij de aanwijzing en het tijdstip daarvan rekening met de reacties die ik ontvang uit de internetconsultatie. Het is voor mij van belang dat ik zo kort mogelijke maar wel realistische termijnen aanhoud.

Zo ja, op basis van welke criteria of advies en wordt daarbij ook rekening gehouden met een redelijke overgangstermijn voor dienstverleners die de nieuwe software moeten implementeren in hun middelen?

Gelet op de samenhang van deze vraag met de vragen van het CDA over de wijze waarop de toegroei plaatsvindt, en voor welke componenten dat dan geldt, heb ik voor de overzichtelijkheid voor gekozen om deze vraag op die plek te beantwoorden.

De regering wil het gebruik van open source software zoveel mogelijk verplichten en leunt voor de veiligheid van deze software op een niet nader gedefinieerde gemeenschap. Kan de regering aangeven aan welke vereisten deze gemeenschap moet voldoen? Welk niveau van sterkte, activiteit en omvang moet deze gemeenschap hebben, en op wat voor manier en door wie wordt dat gecontroleerd? Wordt er in het toezicht ook rekening gehouden met de mogelijkheid dat deze gemeenschappen op een gegeven moment ook niet meer aan de eisen voldoen? En hoe wordt hierop toegezien? Wat heeft het voor gevolgen voor toegelaten middelen die gebruikmaken van open source software als de daarbijbehorende gemeenschap niet meer voldoet aan de vereisten? Wie is er uiteindelijk eindverantwoordelijk dat de door de overheid verplichte open source software ook daadwerkelijk doet wat die moet doen?

Graag verwijs ik voor de eenduidigheid van de beantwoording de leden naar het antwoord op de vraag van de leden van de VVD-fractie ten aanzien van open source gemeenschap en daaraan te stellen criteria.

De regering heeft aangegeven dat onder open source een openbare broncode én een actieve community die een en ander toetst op veiligheid en betrouwbaarheid wordt verstaan. Zowel medewerkers van het (aanbiedende) bedrijf als vrijwilligers mogen lid zijn van deze community. De leden van de **CDA**-fractie vragen de regering in hoeverre er eisen aan omvang en samenstelling van deze community worden gesteld? Is er zicht op het profiel van de deelnemers?

Zoals gezegd in mijn antwoord bij de vragen van de VVD-fractie schept open source in dit verband de mogelijkheid om input van derden te verkrijgen op de broncode. Hoewel dit onderdeel uitmaakt van de verantwoordelijkheid om te zorgen voor een deugdelijk product, heb ik in de regels expliciet gemaakt dat aanbieders adequaat op meldingen moeten reageren en dat aan melders moeten terugkoppelen. Daar hoort bij dat de aanbieder van het middel beschikt over ter zake kundige medewerkers/ontwikkelaars.

Hoe wordt getoetst of de adviezen van deze community betrouwbaar zijn én of ze daadwerkelijk worden opgevolgd door de aanbieder van de desbetreffende broncode?

De gemeenschap is een aanvullende waarborg die aanbieders van inlogmiddelen helpt om hun professionele verantwoordelijkheid naar beste mogelijkheden te kunnen invullen. De regelgeving eist dat aanbieders een kanaal openstellen voor meldingen van kwetsbaarheden in de software en verbetervoorstellen adequaat opvolgen. Vanuit de

verantwoordelijkheid voor het leveren van een deugdelijk product is het aan de aanbieder om de adviezen van de gemeenschap te bestuderen, te beoordelen en er adequate opvolging aan te geven. Op het moment dat het niet opvolgen van een advies vanuit de gemeenschap leidt tot een kwetsbaar middel dat niet meer veilig is, zal dat de facto ertoe leiden dat niet meer wordt voldaan aan de vereisten die de ministeriële regeling stelt. Indien de aanbieder een onvoldoende veilig of onbetrouwbaar inlogmiddel aanbiedt, dan trekt de Minister van BZK de erkenning in.

Bij de introductie van een nieuw inlogmiddel zal de community vermoedelijk meer alert zijn dan gedurende de daaropvolgende jaren van gebruik. Hoe houdt de regering zicht op de veiligheid en betrouwbaarheid van de inlogmiddelen door de jaren heen?

Zoals ik in de beantwoording hiervoor heb aangegeven gelden voor veiligheid van de inlogmiddelen de eisen zoals die in de ministeriële regeling zijn opgenomen. De aanbieders van inlogmiddelen moeten daaraan voldoen bij de toelating en ook daarna. Daarop wordt door het Agentschap Telecom toezicht gehouden gedurende de periode dat inlogmiddelen zijn toegelaten. De veiligheid van de gebruikte softwarecomponenten maakt daarvan onderdeel uit. De primaire veiligheid van de middelen borg ik aldus door de aanbieders aan de toelatingseisen te houden en hen daarop aan te spreken als dat nodig is.

Zoals ik hiervoor heb betoogd, hecht ik grote waarde aan het bestaan van gemeenschappen die meekijken. Dit stelt iedereen die dat wil (de gemeenschap) in staat om de broncode te onderzoeken, kwetsbaarheden te melden en eventueel verbetervoorstellen te doen. Dit veel-ogen principe is een aanvullende waarborg voor de veiligheid en betrouwbaarheid van inlogmiddelen. Ik neem zelf een stimulerende rol in het laten ontstaan van en actieve invulling van de rol door communities.

Overigens, kunnen ook andere aanbieders dan de ontwerper van de broncode deze code ook gaan gebruiken?

De primaire doelstelling van de regeling van open source in de ministeriële regeling is het bereiken van transparantie over de werking van de gebruikte software. In het verlengde daarvan is het zoals ik hiervoor heb geantwoord, voor die doelstelling voldoende dat aanbieders de broncode publiceren op een zodanige wijze dat de code daadwerkelijk onderzocht kan worden. Aanbieders mogen in de toegepaste licentie de overige rechten, waaronder verdere gebruiksrechten, op de software voorbehouden. Dat zal betekenen dat andere aanbieders dan de ontwerper de code niet mogen gebruiken. Daar kunnen overigens goed voorstelbare redenen voor zijn, bijvoorbeeld om de gedane investering te kunnen uitnutten. De regeling staat er niet aan in de weg dat aanbieders (open source) software licenties voor zelf ontworpen software hanteren (of ervan gebruik maken).

In de novelle wordt aangegeven dat er gewerkt wordt naar open source; dat de opzet is toe te groeien naar open source. Welke termijn verwacht de regering dat nodig is om volledige open source voor te schrijven?

De termijn om alle componenten van inlogmiddelen volledig open source aan te bieden is zo kort mogelijk. Het is evenwel niet mogelijk nu reeds een exacte indicatie te geven van de benodigde termijn. Deze termijn is mede afhankelijk van ontwikkelingen op het gebied van open source. Bij de beantwoording van de vragen van de VVD-fractie gaf ik aan dat ik hiervoor in gesprek zal gaan met experts.

Welke termijn nodig is, hangt af van de specifieke oplossingen die aanbieders van inlogmiddelen gaan hanteren. Aanbieders zullen tijd nodig hebben om de (onderdelen van) broncode zoals zij die hanteren gereed te maken voor publicatie.

Het zal tijd kosten om alle relevante broncode «publiceer-klaar» te maken. Voorstelbaar is dat dit voor omvangrijke code veel tijd en inspanning kan vergen. Hier geldt: deze tijd zal zo kort mogelijk moeten zijn, maar wel zo lang als nodig om de omschakeling veilig en beheersbaar te kunnen maken.

Daarnaast kan het zijn dat aanbieders voor functionaliteiten gebruik maken van software die door derde partijen is ontwikkeld, en dat deze partijen niet willen dat de broncode van deze software wordt gepubliceerd. Aanbieders zullen in dat geval een redelijke termijn moeten worden gegund om voor functionaliteiten die het betreft ofwel alternatieve open source mogelijkheden te vinden, ofwel de benodigde functionaliteit zelf te ontwikkelen.

De verplichting broncode te publiceren zal dus nog niet vanaf de start van de toelating van middelen gaan gelden. Er is uitstel nodig om veiligheid en continuïteit te kunnen bieden en om een breed aanbod aan nieuwe middelen op korte termijn te kunnen laten toetreden. Dat laatste is belangrijk omdat daarmee het aanbod spoedig kan worden vergroot en er «vitaliteit» in het stelsel van middelen komt. Aanbieders zullen dan binnen de door het kabinet gestelde grenzen met elkaar concurreren, wat innovatie op veiligheidsmethoden en gebruiksvriendelijkheid bevordert.

Kan aangegeven worden welke functionaliteiten open source moeten zijn. Zijn dat alleen de aanvraag- en inlogfunctie?

Het doel is – zoals eerder beschreven – om toe te groeien naar het zo veel als mogelijk open source aanbieden van inlogmiddelen en machtigingsdiensten. Het open source vereiste zal naast de aanvraag- en inlogcomponent ook van toepassing zijn op onder meer logging, beheer van machtigingen, inzage en schorsing. Om de transparantie en controleerbaarheid van de verwerking van persoonsgegevens te borgen zal het vereiste van toepassing worden op alle componenten waarin persoonsgegevens worden verwerkt in het kader van de erkenning.

In de bijlage 1 bij de conceptregeling eisen identificatiemiddelen Wdo, die met uw Kamer wordt gedeeld, is vermeld op welke componenten het open sourcevereiste van toepassing zal worden. Aan alle genoemde componenten wordt in de vast te stellen versie een datum verbonden, waarop de verplichting ingaat. De periode van de internetconsultatie en de inbreng uit de consultatie wordt gebruikt om deze data te bepalen.

Volgens de novelle (artikel 9 zesde lid, onder d) zal een aanbieder van digitale diensten worden geweigerd indien naar het oordeel van de Minister onvoldoende gebruik is gemaakt van software die onder open source licentie is gepubliceerd. Waarom, zo vragen de leden van de **PvdA**-fractie, is de open source niet als harde eis gesteld? En a fortiori: waarom is deze harde eis niet gesteld aan nieuwe aanbieders, die immers niet te maken hebben met transitieproblemen?

Eén van de redenen om voor een systeem van open toelating te kiezen is het creëren van vitaliteit in het stelsel doordat er verschillende inlogmiddelen beschikbaar komen voor toegang tot digitale overheidsdienstverlening. Dit gaf ik ook aan in de beantwoording hiervoor van de vragen van de CDA-fractie. Dat de inlogmiddelen van potentiële nieuwe toetreders nu

nog niet gebruikt kunnen worden voor de toegang tot de overheid betekent niet dat de inlogmiddelen nog niet zijn ontwikkeld. Derhalve hebben ook toetredende leveranciers tijd nodig voor de transitie naar open source. Het open source vereiste zal voor alle inlogmiddelen op dezelfde wijze en binnen dezelfde termijnen vorm worden gegeven.

Kan de regering aangeven wat de nadere kaders zijn voor de «voorkomende gevallen» als bedoeld onder lid c, in hoeverre betekent dit dat de broncode niet openbaar hoeft te worden gemaakt?

Artikel 18 leden b en c van het Besluit identificatiemiddelen voor natuurlijke personen Wdo stellen ten aanzien van de broncodes:

b. *een beschrijving van de wijze waarop de werking van het identificatiemiddel en het authenticatieproces gebaseerd is op software:*
   i. *waarvan de broncode openbaar is gemaakt; of*
   ii. *waarvan de broncode valt onder een open-source licentie, waarbij deze licentie wordt beschreven;*

c. *in voorkomend geval, de overwegingen om voor delen van de werking van het authenticatiemiddel en het authenticatieproces geen gebruik te maken van broncode bedoeld in onderdeel b, subonderdeel i. en ii, gerelateerd aan de overwegingen genoemd in artikel 6, tweede lid.*

Het kan hier bijvoorbeeld gaan om publicatie van code van componenten waarbij openbaarheid afbreuk kan doen aan veiligheid, bijvoorbeeld het tegengaan van fraude en misbruik. Op het moment dat dergelijke controles transparant worden gemaakt wordt hun doel ondergraven. Overigens wordt ernaar gestreefd om ook hier zoveel mogelijk van de code transparant te maken, zodat slechts de controlecriteria niet openbaar worden, maar werking van de componenten wel.

In paragraaf 3.2 van de Nota van toelichting bij het Besluit wordt ten aanzien van de opensource-licentie gesteld: «Met dit besluit wordt dit groeimodel mogelijk gemaakt. Op grond van dit besluit stelt een Minister een norm vast waaraan een aanvrager moet voldoen met betrekking tot het gebruik van open source software in de processen van het identificatiemiddel. De norm wordt vastgesteld met inachtneming van de beschikbare software met een open source-licentie, de veiligheid van die software en de gevolgen van het implementeren voor het aanbod van identificatiemiddelen voor gebruik bij overheidsdienstverlening. Om groei naar meer open source af te dwingen wordt de norm zodra dat mogelijk is gelet op de relevant belangen, naar boven bijgesteld.

Kan de regering specifieker duiden wat hier onder een groeimodel wordt verstaan en wat hiervoor de kaders en criteria zijn? Er wordt gesproken over «een Minister die «een norm» vaststelt. Kan de regering aangeven op welke vakminister/departement dit betrekking heeft (mag er van worden uitgegaan dat dit de in het besluit als «Onze Minister» de Minister van Binnenlandse Zaken en Koninkrijksrelaties betreft) en preciezer duiden wat de aard en strekking is van deze «norm»?
In reactie op de kritiek van de Raad van State op dit punt verwijst de regering naar de «geleidelijkheidsnorm». Kan de regering aangeven in hoeverre deze norm überhaupt wel normerend werkt? Hoe verhoudt deze bepaling zich met het gegeven dat broncodes binnen de overheid in beginsel al openbaar behoren te zijn?

Ik verwijs voor het antwoord naar de vragen van de VVD-fractie, waar ik deze onderwerpen heb geadresseerd.

De Raad van State merkt in zijn advies over de Wet digitale overheid op dat dit streven om geleidelijk over te gaan op open source software niet naar voren komt in de voorgestelde weigeringsgrond dat «onvoldoende gebruik wordt gemaakt van software die onder open source licentie is gepubliceerd.».[2] Bovendien biedt het wetsvoorstel niet met zoveel woorden de mogelijkheid om een erkenning in te trekken naarmate er meer aanbieders bij komen die open source software aanbieden. De regering gaat nauwelijks in op het bovengenoemde punt van de Raad van State. De leden van de fracties van de **PvdA** en **GroenLinks** vragen of de regering dit alsnog kan doen en aangeven hoe zij dit proces inricht in het licht van de woorden van de Raad van State?

De Raad van State merkt op dat uit de memorie van toelichting een streven blijkt om geleidelijk over te gaan op open source software, maar dat dit streven niet naar voren komt in de in het wetsvoorstel vervatte weigeringsgrond, zoals opgenomen in artikel 9, zesde lid, onderdeel d (burgerdomein) en artikel 11, achtste lid, onderdeel d Wdo (bedrijvendomein).

Van belang is om onderscheid te maken tussen het moment van aanvragen van een erkenning en het moment dat de erkenning is verleend. Een aanvraag kan door de Minister worden geweigerd. Een reeds verleende erkenning kan door de Minister worden gewijzigd, geschorst of ingetrokken op grond van artikel 9, zevende lid (burgerdomein) of krachtens artikel 14, derde lid Wdo (bedrijvendomein).

Het wetsvoorstel schept wel degelijk een bevoegdheid om een (reeds verleende) erkenning in te trekken, indien er op een later moment naar het oordeel van de Minister onvoldoende gebruik wordt gemaakt van software die onder een open source licentie is gepubliceerd. Wat onvoldoende gebruik inhoudt, wordt verduidelijkt in bijlage 1 van de conceptregeling eisen identificatiemiddelen Wdo. Deze bijlage zal periodiek aangepast worden naar aanleiding van ontwikkelingen op het gebied van de beschikbaarheid van open source alternatieven. De Minister wijst aan van welke componenten de broncode gepubliceerd moet worden en per wanneer. Die aanwijzing wordt vastgelegd in de bijlage en daarmee wordt via de bijlage invulling gegeven aan de geleidelijkheid. De Minister kan de erkenning van leveranciers intrekken op grond van voornoemde bepalingen, indien inlogmiddelen niet uitgevoerd zijn met gepubliceerde broncodes conform de aanwijzing in die bijlage.

De Raad van State schrijft, refererend aan de memorie van antwoord, dat de wet hoofdelementen van de regeling dient te bevatten.[3] Het gevaar van techniekonafhankelijk omschreven wetgeving is dat de wet zo abstract wordt dat de hoofdelementen niet meer herkenbaar worden beschreven, zodat het parlement als medewetgever er zich geen voorstelling van kan maken waarmee het instemt.

De leden van de **GroenLinks**-fractie delen deze mening en willen graag van de regering weten of zij dit ook ziet. Kan zij hierin de vergelijking van de Raad van State meenemen dat de aanduiding zoogdieren ook niet voldoende concreet is.

De regering deelt de mening van de Raad van State dat wetgeving voldoende concreet moet zijn. Daardoor weten degenen die door die wetgeving worden geraakt wat van hen wordt verwacht of wat zij mogen

---

[2] *Kamerstukken II* 2020/21, 35 868, nr.4.
[3] *Kamerstukken I* 2020/21, 34 972, P.

verwachten en weet het parlement waarmee instemming wordt gevraagd. Naar mijn mening is het punt dat de Raad van State maakt over de techniekonafhankelijke formuleringen in het wetsvoorstel in dit licht niet terecht.

Het advies is gericht op de aanduiding van bepaalde voorzieningen waarvoor de Minister van BZK verantwoordelijk is. Het wetsvoorstel bepaalt, op wetsniveau, welke voorzieningen door de Minister van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK) beschikbaar moeten worden gesteld en gehouden. Daarbij is van belang dat duidelijk is wat die voorzieningen inhouden, dus welke functionaliteiten deze voorzieningen moeten hebben. In het voorbeeld van het BSN-koppelregister regelt het wetsvoorstel dat er een voorziening moet zijn die het mogelijk maakt dat personen, ondernemingen of rechtspersonen bij het afnemen van elektronische publieke diensten aan de hand van een uniek identificerend nummer kunnen worden geïdentificeerd. De wet verplicht de Minister van BZK om te borgen dat een voorziening met die functies beschikbaar is en blijft. De wijze waarop deze verplichting is geformuleerd is effectief en concreet. Het vereiste resultaat is duidelijk. Het vastleggen van de techniek waarop die voorziening draait of de naam van die voorziening in de wet vastleggen, draagt niet bij aan het doel van de wet, namelijk zorgen voor een infrastructuur waarmee in bepaalde functies is voorzien. Een aanduiding van een voorziening aan de hand van de gebruikte techniek of het vastleggen van de naam van de voorziening, in plaats van de functie, is naar mijn mening zelfs minder duidelijk. Het gaat immers om dat het te verwachten resultaat duidelijk is en niet om de techniek of de naam.

De vergelijking met de aanduiding van zoogdieren in plaats van paarden gaat naar mijn mening dan ook mank. Een betere vergelijking vind ik een wetsvoorstel waarin wordt voorgeschreven dat de Minister moet voorzien in voldoende trekkracht voor het verplaatsen van een boomstam met een specifiek gewicht. Daarmee is duidelijk welk resultaat van de Minister wordt verwacht. Het toevoegen van de specifieke techniek (tractor, katrol, lier of dierlijke trekkracht) voegt daaraan niets toe en het noemen van de naam van het apparaat of dier dat in de trekkracht zal voorzien ook niet. Het vastleggen van het gewenste resultaat is van belang, niet de gebruikte techniek of de naam van de oplossing.

Gelet op het voorgaande deel ik de opvatting van de Raad van State niet en ben ik van mening dat de bepalingen van het wetsvoorstel duidelijk zijn geformuleerd en dat het aanduiden van voorzieningen in de vorm van techniekaanduiding of naamgeving afbreuk doet aan de door ons allen gewenste duidelijkheid.

De leden van de fractie van **D66** hebben geconstateerd dat de regering tijdens de behandeling van de novelle in de Tweede Kamer heeft toegezegd dat het streven van dit wetsvoorstel «open source, tenzij» zal zijn. Kan de regering toelichten wanneer de uitzondering op de open source geldig is?

In dit kader is het goed op te merken dat het «Open, tenzij»-principe een uitgangpunt is dat geldt voor de publieke sector. In de Kamerbrief over vrijgeven broncode overheidssoftware van april 2020 is dit principe geïntroduceerd. Dit is toentertijd onder meer ingegeven door de notie dat voor digitale oplossingen die door (of in opdracht van) de overheid worden gemaakt zou moeten gelden dat publiek geld ook tot publieke code moet leiden. Zo regelt ook de ARBIT dat de auteursrechten in principe aan de opdrachtgevende overheidspartij toevallen, een belangrijke voorwaarde om open source te kunnen publiceren. Voor code die

niet in opdracht van de overheid (en niet met publieke middelen) is gemaakt liggen de zaken anders.
Door toepassing van «open source, tenzij»-principe in het kader van dit wetsvoorstel onderstreept de regering dat de broncode van de voor de inlogmiddelen gebruikte componenten in principe openbaar moet zijn. De Minister wijst componenten aan waarvan de broncode op een daarbij gegeven datum moet worden gepubliceerd.
Wanneer dit voor reeds bestaande inlogmiddelen (DigiD voor burgers en eHerkenning voor bedrijven) een risico oplevert voor de veiligheid en de beschikbaarheid van deze inlogmiddelen gaat deze verplichting voor deze middelen pas later gelden.

Het is aan de Minister – en dus uitdrukkelijk niet aan de aanbieders van inlogmiddelen – om te bepalen of voor bepaalde componenten (voorlopig nog) gebruik mag worden gemaakt van closed source software. Ik merk daarbij ten overvloede op dat de regeling ook voor deze inlogmiddelen zo wordt ingericht dat de «tenzij» steeds kleiner wordt.

Op welke manier gaat er toezicht gehouden worden dat dit doel wordt bewerkstelligd?

Het toezicht op de toepassing van open source vindt plaats bij zowel de aanvraag als na de verlening van de erkenning. Tijdens de aanvraagprocedure wordt getoetst of het inlogmiddel gebruik maakt van software waarvan de broncode is gepubliceerd voor alle componenten die door de Minister zijn aangewezen. De aanvrager van een erkenning neemt hiervoor in de erkenningsaanvraag een beschrijving op van alle gebruikte componenten op waarin persoonsgegevens worden verwerkt in het kader van inlogdienstverlening. De beschrijving omvat ook informatie over publicatie van de broncode. Het Agentschap Telecom controleert of het inlogmiddel van de partij die de aanvraag indient voldoet aan de open source eisen. Dat wil concreet zeggen: of er sprake is van de inzet van een closed source component terwijl de datum zoals opgenomen in de regeling daarvoor verstreken is. Indien dit het geval is, dan wordt een middel niet toegelaten.

Na de verlening van de erkenning gelden de eisen voor toelating van het stelsel onverminderd voor toegelaten partijen. Toegelaten partijen moeten dan ook zorgen dat zij, voor zover nodig, hun software aanpassen wanneer op grond van de ministeriële regeling een nieuwe aanwijzing van kracht wordt van de functionele componenten waarvoor de broncode dient te worden gepubliceerd. Ook leveranciers die reeds een erkenning hebben, zullen hieraan moeten voldoen en het Agentschap Telecom controleert hierop zoals hierboven vermeld.

Wordt er in de evaluatie en de tussentijdse monitoring van de werking van de wet bezien of dit streven in de praktijk daadwerkelijk wordt gehaald?

De evaluatie van de wet omvat een verslag over de doeltreffendheid en de effecten van de wet in de praktijk, waarin in het bijzonder aandacht wordt geschonken aan de toegankelijkheid van elektronische dienstverlening en de getroffen maatregelen op het gebied van beveiliging en privacybescherming. De toepassing van open source is een van dergelijke maatregelen en zal derhalve meegenomen worden in de wetsevaluatie.

Tijdens de mondelinge behandeling van de novelle in de Tweede Kamer heeft de regering meermalen benadrukt dat open source niet alleen maar bestaat uit openbaarheid, maar ook dat er een community van mensen is die rondom de openbare software werkt om te kijken of die op een goede manier functioneert en of er mogelijkheden zijn die te verbeteren. De

leden van de D66-fractie constateren dat de regering zowel een beroep doet op vrijwilligers als op betaalde krachten uit de open source community. Kan de regering de leden fractie van D66 laten weten of er casus in andere landen zijn waar al een beroep wordt gedaan door regeringen op dit soort communities? Hoe werkt het daar in de praktijk? Is het niet risicovol als er alleen op vrijwilligers wordt geleund?

Ten aanzien van het punt over de communities en het beroep dat ik daarop doe refereer ik graag aan de voorgaande beantwoording bij de vragen van de VVD-fractie. Zoals gezegd hecht ik grote waarde aan het bestaan van gemeenschappen gezien de bijkomende voordelen die zij hebben, en ik ga de totstandkoming van communities ook stimuleren, echter ik stel daar de primaire veiligheid van inlogmiddelen niet van afhankelijk.

Er zijn verscheidene landen waar door overheden gebruik wordt gemaakt van communities. Deze landen treffen maatregelen om de deelname van professionals binnen dergelijke communities te bevorderen. Voor Franse publieke software initiatieven is bijvoorbeeld de BlueHats community in het leven geroepen. Deze community bestaat onder meer uit software ontwikkelaars, IT-wetenschappers en overheidsmedewerkers. Ook wordt in Frankrijk het «Lutece» platform gebruikt voor onder meer het faciliteren van democratische participatie en het rapporteren van stedelijke issues. In het kader van Lutece worden experts betaald om bij te dragen aan de community. De Italiaanse overheid onderneemt ook acties om burgers en hackers mee te nemen in de digitale transformatie door onder meer te voorzien in hackerspaces en kent ontwikkelaars die met publiek geld worden betaald om actief bij te dragen aan open source communities.

Hoewel de leden van de D66-fractie het streven van «open source, tenzij» onderschrijven, zijn er vragen over de uitvoerbaarheid. Kan de regering zekerheid bieden dat er genoeg capaciteit is om de transitie open source, tenzij»» door te voeren bij bestaande overheidsprogramma's?

Voor de duidelijkheid merk ik op dat de overheidsbrede transitie naar open source (tenzij) buiten de reikwijdte van deze wetsbehandeling valt, maar in de bredere open tenzij beleidslijn. Deze vraag gaat in feite over de capaciteit/inspanning die overheden zelf moeten leveren om te zorgen dat zij (intern) meer gaan werken met open source.

Zijn er op dit moment «closed source» inlogmiddelen die onbruikbaar zouden kunnen worden omdat zij niet voldoen aan de nieuwe wettelijke eisen? In de memorie van toelichting wordt gesproken over een redelijke termijn waarbinnen erkende aanbieders aanpassingen moeten doorvoeren. Hoe lang is deze redelijke termijn?

Gelet op de huidige middelen (DigiD, eHerkenning) die door burgers en bedrijven worden gebruikt, betekent het per direct onverkort open source vereisen dat deze middelen niet aan de open source eis zouden voldoen. Dit is een belangrijke reden om ook voor deze inlogmiddelen te kiezen voor een groeipad. Ten aanzien van de termijn wijs ik de leden op de eerdere beantwoording terzake.

De fractieleden van de **PVV** vragen de regering nader te duiden hoe met name ten aanzien van het punt van open source aan deze kritiek tegemoet is gekomen, nu dit weliswaar in de formele wet wordt genoemd, maar van een eenduidige invulling en normering van dit begrip geen sprake is en dit inhoudelijk nog altijd afhankelijk is van de nadere invulling per ministeriële regeling?

Tijdens de deskundigenbijeenkomst, waarbij deskundigen in gesprek met uw Kamer hun aandachtspunten hebben meegegeven, is naar voren gebracht dat het oorspronkelijke wetsvoorstel niet voorzag in toetsing op drie criteria die van belang zijn voor toelating van private partijen. Deze elementen waren wel in lagere regelgeving vastgelegd, maar het wetsvoorstel voorzag niet in een verplichting om op de desbetreffende criteria te toetsen. Met de novelle is op wetsniveau vastgelegd dat op deze drie criteria moet worden getoetst. Het specificeren van de toepassing van die criteria vindt in lagere regelgeving plaats. Dat gebeurt bij algemene maatregel van bestuur die Uw Kamer in het kader van de voorhangprocedure is voorgelegd. In het geval van toetsing op software met openbare broncode, vindt het aanwijzen van de componenten waarvoor de broncode openbaar moet zijn in de genoemde ministeriële regeling plaats. Het regelingsniveau van de ministeriële regeling is gekozen vanwege het gedetailleerde karakter van die aanwijzing en de aansluiting van dit onderwerp op de regeling van de overige eisen in die ministeriële regeling.

Bij de behandeling in de Tweede Kamer kon de regering op het punt van de invulling en normering van open source geen duidelijke inkadering aangeven van de beoogde inzet van de «community». De regering gaf hierbij aan dit nog te moeten «uitwerken» en de scherpte nog te moeten definiëren. Kan de regering op dit punt een nadere duiding en afbakening van criteria en doelen omtrent de «open source community» aangeven?

In de periode sinds de behandeling van de wet in de Tweede Kamer heb ik de verdere uitwerking ter hand genomen. In die uitwerking is de rol van de open source community uitgekristalliseerd. Voorop staat dat ik de aanwezigheid van open source communities van belang vind en daar een actieve rol in neem. Als iedereen kan meekijken met de werking van software kan dat een belangrijke extra waarborg bieden voor de veiligheid. Daarnaast biedt transparantie en openheid van de componenten waarmee de overheid werkt of waarmee met de overheid gecommuniceerd wordt een belangrijke en steeds belangrijker wordende waarborg voor het vertrouwen dat in de inlogmiddelen gesteld kan worden. Op termijn kan het bredere gebruik van open source software er ook voor zorgen dat afhankelijkheid van specifieke partijen minder wordt (omdat software ontwikkeling en onderhoud niet meer bedrijfs- of organisatie gebonden zijn).

Ik kies er zoals hiervoor betoogd, echter niet voor om de veiligheid en betrouwbaarheid van inlogmiddelen volledig afhankelijk te stellen van de beschikbaarheid van open source communities, maar door daar als onderdeel van de eisen aan inlogmiddelen verplichtingen voor de aanbieders over op te leggen. Dat neemt echter niet weg dat het mijn verwachting is dat open source communities in de praktijk een steeds grotere bijdrage zullen leveren aan de veiligheid van de gebruikte software.

4. Privacy by design / erkenning

De Minister mag alleen de inlogmiddelen erkennen, die, beoordeeld naar de jongste stand van de techniek, voldoen aan het principe van privacy by design. Voorts geldt dat indien een erkend middel nadien niet meer voldoet aan dit principe, de erkenning zal moeten worden ingetrokken. De regering gaat niet in op het punt van de Raad van State dat de erkenning ook na acceptatie ingetrokken zou moeten kunnen worden. Erkent de regering dit, zo vragen de leden van de fracties van de **PvdA** en **GroenLinks**. Hoe gaat de regering dit controleren nadat eerder een aanbieder

voldeed aan de regels, maar daarna niet meer? Op welke wijze gaat de regering de monitoring vormgeven?

Het principe van privacy by design is primair verankerd in de Algemene verordening gegevensbescherming (hierna: AVG). Elke organisatie die persoonsgegevens verwerkt is gehouden zich aan dit beginsel te houden.

De AVG kan echter niet dienen als afwijzing van een erkenningsaanvraag of intrekking van een verleende erkenning, zonder nadere wettelijke basis. Daarom is met het voorgestelde artikel 9, zesde lid, onderdeel b, en artikel 11, achtste lid, onderdeel b, voorzien in een specifieke afwijzingsgrond voor aanvragen. Met artikel 9, zevende lid, en artikel 14, derde lid, wordt geregeld dat reeds verleende erkenning kunnen worden ingetrokken wanneer niet langer is voldaan aan het principe van privacy by design.

In toezicht is reeds voorzien, de AVG kent immers al de verplichting om te voldoen aan privacy by design. Wanneer een overtreding wordt geconstateerd kan dat, naast de handhavingsinstrumenten van de Uitvoeringswet AVG, in het uiterste geval leiden tot intrekking van de erkenning. Dat kan bijvoorbeeld het geval zijn wanneer er een nieuwe privacybeschermende techniek is ontwikkeld waarvan redelijkerwijs mag worden verwacht dat erkende partijen deze toepassen. Overigens merk ik op dat de bepaling of er sprake is van privacy by design, van meer factoren afhankelijk is dan alleen de techniek die wordt gebruikt. Bepalend is dat er een afweging wordt gemaakt tussen de verschillende AVG-beginselen (doelbinding, transparantie, bewaartermijnen, dataminimalisatie en veiligheid). Daarbij wordt aangehaakt bij de richtsnoeren die daarvoor door de gezamenlijke Europese privacy toezichthouders zijn opgesteld[4].

5. Dataminimalisatie

De regering heeft in de Tweede Kamer onderstreept dat dataminimalisatie belangrijk is. Dit zou inhouden dat partijen zo min mogelijk persoonsgegevens mogen bewaren; eigenlijk louter die gegevens die essentieel zijn. Hoe definieert de regering precies essentiële gegevens, vragen de leden van de **D66**-fractie. Kan de regering toelichten op welke manier er toezicht zal worden gehouden op partijen die aan dataminimalisatie doen? Wat zou een eventuele sanctie zijn als partijen niet voldoen aan de eisen omtrent dataminimalisatie? Waar worden die eisen opgenomen?

Op grond van de Algemene verordening gegevensbescherming (AVG) mogen persoonsgegevens alleen worden verwerkt wanneer daarvoor een grondslag bestaat. Het concept-besluit digitale overheid voorziet in grondslagen voor het verwerken van gegevens door toegelaten private partijen op grond van de Wet digitale overheid. Private partijen mogen dus voor authenticatie slechts de persoonsgegevens verwerken die in dat besluit zijn genoemd. De genoemde gegevens zijn de minimale gegevens die noodzakelijk zijn voor een authenticatie zoals die functioneel is voorzien. De gedetailleerde opsomming van deze gegevens vindt u in artikel 9b en 9c van het ontwerpbesluit digitale overheid dat aan Uw Kamer is voorgelegd in het kader van de voorhangprocedure. Op het moment dat deze regels worden overtreden wordt in strijd met de erkenning gehandeld en kan de erkenning worden ingetrokken.

---

[4] Richtsnoeren 4/2019 inzake artikel 25 Gegevensbescherming door ontwerp en door standaardinstellingen
Versie 2.0
https://edpb.europa.eu/system/files/2021
04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_nl.pdf

Buiten de verplichtingen uit het concept-besluit digitale overheid gelden de verplichtingen van de AVG voor deze private partijen. Dat geldt ook voor dataminimalisatie.

Zowel het verwerken van andere gegevens dan is toegestaan, als het niet naleven van het beginsel van dataminimalisatie, zijn overtredingen van de AVG. Dit valt onder het reguliere toezichtsterrein van de Autoriteit Persoonsgegevens. Op grond van artikel 14 van de Uitvoeringswet AVG in combinatie met artikel 83, vijfde lid, onderdeel a, van de AVG, kan de Autoriteit Persoonsgegevens voor deze overtredingen een boete opleggen tot een bedrag van 20.000.000 euro of 4% van de jaaromzet van de onderneming.

6. Menselijk contact

De regering heeft aangegeven dat mensen die in moeilijkheden komen dan wel vragen hebben over het inloggen altijd terecht moeten kunnen bij een menselijk contact. De fractieleden van het **CDA** vragen de regering aan wie deze taak wordt gegeven? Zijn dat de huidige Informatiepunten Digitale Overheid? Geldt dat voor elke publieke en private aanbieder?

Het is inderdaad belangrijk dat iedereen die moeilijkheden of vragen heeft bij of over inloggen terecht kan bij een mens. Dit geldt zowel voor de overheid als voor aanbieders van inlogmiddelen. Voor aanbieders van inlogmiddelen geldt dat zij telefonisch bereikbaar moeten zijn om burgers te woord te staan. In het realiseren van contact met een mens bij overheidsdienstverlening heb ik een coördinerende rol en werk ik samen met andere ministeries in het kader van Werk aan Uitvoering en, in het kader van het programma 1-Loketfunctie, samen met uitvoeringsorganisaties en gemeenten.
Eén van de acties die ik hiervoor onderneem is het inrichten van informatiepunten digitale overheid. Hiervan zijn er nu al 486 en er wordt toegewerkt naar een totaal van 500 informatiepunten in 2023. Daarnaast werk ik aan overheidsdienstverlening die transparant is, laagdrempelig en ook toegankelijk voor (tijdelijk) minder zelfredzame burgers.

Het streven is om binnen enkele jaren de overheidsdienstverlening zo in te richten dat de burger kan volstaan met één enkel initieel contact met een overheidsinstantie.

7. Uitnutting van persoonsgegevens

Het wetsvoorstel heeft tot doel private partijen te reguleren die inlogmiddelen voor de toegang tot overheidsdienstverlening op de markt willen brengen, zodat persoonsgegevens niet commercieel worden uitgenut. In de voorgestelde weigeringsgrond wordt gekeken naar de inkomsten die worden verkregen uit het «verhandelen of verstrekken» van gebruikersgegevens. Met deze omschrijving staat niet vast dat elke vorm van commerciële uitnutting van persoonsgegevens wordt uitgesloten. De regering heeft aangegeven dat het in algemene zin reguleren van alle vormen van commerciële uitnutting van persoonsgegevens valt buiten de werkingssfeer van dit wetsvoorstel. Dat begrijpen de leden van de fracties van de **PvdA** en **GroenLinks**, maar dat is in hun optiek een nogal summier reactie op de zorg van de Raad van State. Kan de regering aangeven hoe zij in algemene zin aankijkt tegen het reguleren van diverse vormen van commerciële uitnutting van persoonsgegevens, de wenselijkheid of de onwenselijkheid hiervan aangeven en vervolgens gericht op het voorstel van de Wet digitale overheid welke vormen van indirecte mogelijkheden van commerciële uitnutting nog mogelijk zijn? En kan zij ook aangeven, in

het verlengde van de vorige vraag inzake open source, hoe de regering dit gaat monitoren als de wereld van de techniek weer is veranderd?

De Wdo regelt dat private partijen die willen toetreden tot het stelsel van de Wdo, dat wil zeggen een inlogmiddel willen aanbieden waarmee bij de overheid ingelogd kan worden, slechts de beschikking hebben over persoonsgegevens indien en voorzover nodig om het middel in gebruik te hebben. Enig ander gebruik van deze gegevens is niet toegestaan. Hiermee is binnen de reikwijdte van de Wdo geregeld dat deze partijen de gegevens waarover ze uit hoofde van die verhouding met de burger en de overheid beschikken niet op een andere manier mogen gebruiken.

Het is mogelijk dat deze partijen nog op een andere manier over persoonsgegevens van burgers kunnen beschikken. Bijvoorbeeld als zij die gegevens aan de personen om wie het gaat hebben gevraagd, als onderdeel van (andere) commerciële dienstverlening bijvoorbeeld. Over het gebruik van op die manier verkregen gegevens gaat dit voorstel niet. Het reguleren van dergelijke verstrekkingen gaat ook het bestek van deze wet te buiten. Wel zorgt de regeling in de Wdo ervoor dat de gegevens die de aanbieder in het kader van de inlogdienstverlening heeft verkregen, niet mogen worden gekoppeld aan deze gegevens en krijgen gebruikers een mogelijkheid, als vangnet, om verstrekkingen aan derden te beëindigen zonder dat daar financiële of functionele gevolgen aan verbonden zijn.

Het wetsvoorstel creëert een verhandelverbod voor private partijen die inlogmiddelen voor de toegang tot overheidsdienstverlening op de markt willen brengen. De leden van de **D66**-fractie vragen om toe te lichten hoe het toezicht daarop zal plaatsvinden.

In de novelle is een verhandelingsverbod opgenomen. Kan de regering aangeven in hoeverre hierbij wordt gekeken naar de organisatiestructuur van het bedrijf: wordt bijvoorbeeld een bedrijf waarvan een separate afdeling, concerntak of (groot)aandeelhouder wel inkomsten verwerft uit handel in persoonsgegevens ook geweigerd? In hoeverre wordt hierbij ook rekening gehouden met de aard van de inkomsten van een UBO, zo vragen de leden van de **PVV**-fractie.

Ik beantwoord deze vragen tezamen. Bij het beoordelen van een aanvraag wordt getoetst of een aanvrager burgers de mogelijkheid geeft om het delen van gegevens aan derde partijen op elk mogelijk moment te beëindigen. Het delen van gegevens is op grond van de AVG al verboden en zal dit op grond van de Wdo eveneens zijn. Door daarnaast als extra slot op de deur burgers de mogelijkheid te bieden gegevensdeling te beëindigen wordt het, in combinatie met transparantie over gegevensdeling en de werking van de gebruikte software, voor aanvragers onmogelijk gemaakt om een verdienmodel te baseren op het verstrekken van gegevens. Wanneer een aanvrager aan deze eisen voldoet heeft de aanvrager immers voldoende aannemelijk gemaakt dat met de erkenning geen inkomsten worden verkregen uit het verhandelen of verstrekken van gegevens over gebruikers of authenticatie van gebruikers. Ik ben van oordeel dat de voorgenomen regeling de meest effectieve wijze is om het doel te bereiken, zonder dat daarbij de organisatiestructuur van het bedrijf hoeft te worden beoordeeld. Verwerkingen anders dan voor het doel van de wet, worden expliciet verboden. Koppeling met andere activiteiten is niet toegestaan. Doordat de verwerkingen van persoonsgegevens transparant dienen te zijn, zal ook direct zichtbaar zijn als aanbieders toch op andere – ongeoorloofde wijze gegevens verwerken. Door ten slotte, naast het feit dat ik zelf bij overtreding zal (laten) ingrijpen, en ik gebruikers (burger en bedrijven) zelf een extra middel in handen geef

door zich te wenden tot de aanbieder, meen ik een efficiënte en doelmatige invulling van het verbod te hebben geformuleerd.

8. Ontwikkelingen

Digitalisering kent een razendsnelle ontwikkeling en dat betekent dat de inlogmiddelen steeds getoetst moeten worden op veiligheid, betrouwbaarheid maar ook op up-to-date technieken. Kan aangegeven worden hoe dit in de praktijk zal plaatsvinden, zo vragen de **CDA**-fractieleden.

Zoals ik in de eerdere beantwoording van de vragen van de CDA-fractie heb toegelicht, gelden de eisen die gesteld worden aan inlogmiddelen niet alleen bij toelating maar ook daarna. Daarbij geldt dat de toetsing plaatsvindt aan de hand van de beoogde waarborgen, zoals veiligheid en betrouwbaarheid, en niet op de maatregelen, zoals de inzet van specifieke technieken. Juist om snel te kunnen veranderen is de systematiek van de wet gekozen zoals deze is. Zo kan er reden zijn voor een andere techniek, niet alleen als het een nieuwe techniek is (want de «oude» techniek kan wellicht nog voor een periode volstaan), maar ook als een gebruikte techniek om andere reden niet veilig meer is (bijvoorbeeld door veiligheidsproblemen). Op dat moment zal het belangrijk zijn om een alternatieve (en niet per se nieuwe) techniek te kunnen inzetten.

9. Toezicht

Eerder heeft de regering aangegeven dat het Agentschap Telecom bij dit proces van opstellen van de regeling betrokken zal zijn. Hoe reflecteert de regering op de capaciteit van het Agentschap Telecom om zorgvuldig toezicht te kunnen houden? Moet het Agentschap uitbreiden? Is er voldoende gekwalificeerd personeel?
Kan de regering duidelijkheid bieden aan de D66-fractie over de mogelijkheid van opschaling van de toezichthouders, met inachtneming van de exponentiële digitale transitie en de steeds grotere vraag naar digitale inlogmiddelen?

Bij het opstellen van deze regeling heeft nauw contact plaatsgevonden met het Agentschap Telecom. Ook de verdere uitwerking vindt plaats in nauw contact en overleg met het Agentschap Telecom. In dit contact staat het vormgeven van het toezicht op een manier die uitvoerbaar is door het Agentschap centraal. In dit contact hebben mij geen signalen bereikt over onvoldoende middelen of onvoldoende gekwalificeerd personeel.

10. Zorg

In het Tweede Kamerdebat over de Novelle op 1 juni 2022 gaf de regering aan dat zorgmedewerkers nu niet op een veilige manier met elkaar informatie over patiënten kunnen uitwisselen. Kan de regering de leden van de **PVV**-fractie aangeven op welke feiten en omstandigheden deze opmerking concreet gebaseerd is en wat de samenhang is met de Wdo?

Inlogmiddelen voor zorgprofessionals om toegang te verkrijgen tot patiëntgegevens zijn nog niet breed beschikbaar op het hoogste betrouwbaarheidsniveau (eIDAS Hoog). De huidige UZI-middelen (UZI-pas en servercertificaat) worden uitgegeven op het hoogste betrouwbaarheidsniveau onder verantwoordelijkheid van het Ministerie van VWS. Echter, de UZI-middelen zijn niet verplicht en worden niet breed gebruikt binnen de zorgsector omdat het zorgveld de middelen als gebruiksonvriendelijk en duur ervaart. VWS is samen met het zorgveld bezig het UZI-stelsel geschikt te maken voor grootschalig gebruik binnen de zorgsector. Uitgangspunt is dat voor de uitgifte en gebruik van inlogmiddelen in ieder

geval wordt aangesloten bij de digitale inlogmiddelen die vanuit de Wet digitale overheid ter beschikking komen. Op 20 december 2021 is de UZI oplossingsrichting aan de Kamer gepresenteerd in een brief over generieke functies voor elektronische gegevensuitwisseling in de zorg.

11. Delegatie

Anders dan de regering lijkt te menen, zit er volgens de Raad van State wel degelijk licht tussen de opvatting en interpretatie van de regering inzake de mate van delegatie binnen de wet dan wel AMvB's. Op het gebied van de techniekonafhankelijkheid is de wet nog hetzelfde. Erkent de regering dit nu wel? De techniekonafhankelijke uitwerking wordt overgelaten aan lagere regelgeving, ondanks het nadrukkelijk advies van de Raad van State en de wens vanuit de Kamer. Kan de regering uiteenzetten waarom hiervoor is gekozen? De regering geeft aan dat duidelijk is wat er onder wordt verstaan en welke functionaliteit de Minister moet verzorgen en dat het niet nodig en zelfs onwenselijk is om in de wet de voorzieningen met een door techniek ingegeven benaming aan te duiden. Dit zou volgens de regering belemmerd werken. Kan de regering dit puntsgewijs uiteenzetten voor de volgende, mede door de Kamer en Raad van State, genoemde begrippen als DigiD, MijnOverheid, DigiD Machtigen en het BSN-Koppelregister? In de optiek van de leden van de **GroenLinks**-fractie gaat de argumentatie inzake deze begrippen niet op om dit in lagere regelgeving te verwerken. Hoe ziet de regering dit?

Deze vraag sluit aan bij de vragen van de leden van de D66-fractie over dit onderwerp. In het antwoord op die vragen heb ik uiteengezet dat het wetsvoorstel moet voorzien in duidelijkheid over de verplichtingen van de Minister van BZK om te zorgen voor de beschikbaarheid van bepaalde functionaliteiten voor burgers en bedrijven. Daarvoor is het niet relevant op welke wijze die functionaliteiten beschikbaar worden gemaakt. Ik verwijs naar die antwoorden voor een algemene uiteenzetting van de positie van de regering.

Voor DigiD bepaalt het wetsvoorstel dat de Minister van BZK zorg moet dragen «voor de uitgifte aan natuurlijke personen die beschikken over een burgerservicenummer en het gebruik door die personen van publieke identificatiemiddelen op verschillende betrouwbaarheidsniveaus». De Minister van BZK moet dus, zo volgt uit het wetsvoorstel, zorgen voor een publiek middel op verschillende betrouwbaarheidsniveaus. Een bepaling met de strekking dat de Minister van BZK zorg moet dragen voor het beschikbaar zijn en blijven van DigiD op verschillende betrouwbaarheidsniveaus zou onvoldoende duidelijk zijn, zonder een nadere beschrijving van de functionaliteiten van DigiD. Het enige dat met een dergelijke bepaling wordt bereikt is dat de naam van het publieke middel op wetsniveau wordt vastgelegd. Naar mijn idee heeft dat geen meerwaarde. Ook het in het wetsvoorstel vastleggen van de techniek waarmee DigiD werkt heeft geen meerwaarde. Het doel van deze bepaling is dat wordt vastgelegd dát de Minister van BZK er zorg voor draagt dat natuurlijke personen altijd op verschillende betrouwbaarheidsniveaus kunnen inloggen met een publiek middel. Daarvoor is het niet relevant met welke techniek dat middel werkt.

Op wetsniveau wordt verder vastgelegd dat de Minister van BZK verantwoordelijk is voor het beschikbaar komen en blijven van een voorziening «voor elektronisch berichtenverkeer met en informatieverschaffing aan natuurlijke personen, ondernemingen en rechtspersonen». Voor burgers noemen we die voorziening de berichtenbox van MijnOverheid, maar het vastleggen van die naam zonder beschrijving van de functies is onvoldoende duidelijk. Wanneer de naam wordt toegevoegd

aan de bestaande bepaling wordt daarmee enkel de naam van de voorziening op wetsniveau vastgelegd, hetgeen naar mijn idee geen meerwaarde heeft. Hetzelfde geldt voor de achterliggende techniek, die niet relevant is voor een bepaling waarmee wordt vastgelegd dat de functionaliteit door de Minister van BZK moet worden verzorgd.

Voor de andere voorbeelden geldt telkens dezelfde redenering. Het beschrijven van de functionaliteit is noodzakelijk. Het toevoegen van de techniek of de naam heeft geen meerwaarde. Bij wijziging van de naam of de techniek zou dan een wetswijziging moeten plaatsvinden.

Tijdens de behandeling van de novelle in de Tweede Kamer zijn er zorgen geuit dat veel zaken niet in de wettekst zelf worden geregeld maar in algemene maatregelen van bestuur en/of in ministeriële regelingen. Kan de regering de leden van de **D66**-fractie op hoofdlijnen een handzaam overzicht geven wat waar en wanneer geregeld wordt?

In reactie op de vraag van de leden van de D66-fractie bied ik hierbij op twee manieren in de bijlage een overzicht van de uitvoeringsregelgeving – algemene maatregelen van bestuur en ministeriële regelingen –, de onderwerpen die hierin worden geregeld alsmede de wettelijke grondslag terzake. Een dergelijk overzicht heb ik op 14 mei 2020 eveneens aan de Tweede Kamer toegezonden in het kader van een vraag van de leden van de GroenLinks-fractie in het verslag van een schriftelijk overleg over het ontwerp besluit digitale overheid. (Tweede Kamer, vergaderjaar 2019–2020, 34 972, nr. 46). Het nu bijgevoegde overzicht is op een aantal punten gewijzigd vanwege samenvoegingen van onderwerpen in regelingen. Het Besluit en de Regeling machtigen zijn komen te vervallen en de benodigde regels in relatie tot machtigen zijn opgenomen in het Besluit digitale overheid en de Regeling voorzieningen Wdo. De voorziene ministeriële regeling bekostiging op grond van artikel 20, die het doorbelasten van kosten samenhangend met de productie en verstrekking van het publieke inlogmiddel voor burgers zou regelen (leges) is komen te vervallen en geregeld in artikel 6 van het Besluit paspoortgelden.

Nieuw in het overzicht is de ministeriële regeling dienstverleners informatieveiligheidsassessments Wdo. Deze ministeriële regeling bevat een codificering van de huidige praktijk inzake de zogenoemde ICT-beveiligingsassessments DigiD.

12. Europa

Intussen lijkt de Nederlandse wetgeving op dit terrein ingehaald te worden door Europese ontwikkelingen richting een wallet-ID. Kan de regering uitleggen waarom Nederland nog een eigen Wet digitale overheid nodig heeft in plaats van een uitvoeringsregeling voor de wallet-ID?

De vraagstelling lijkt een directe koppeling en volledige samenval van de scope van de eIDAS-verordening en de Wdo te veronderstellen. Ik hecht eraan te benadrukken dat daar geen sprake van is. De Wdo regelt waarborgen op diverse terreinen, die niet enkel betrekking hebben tot hetgeen geregeld is of wordt in de eIDAS-verordening. Zo regelt de Wdo het verplichten van standaarden en veiligheidseisen aan overheden én grondslagen voor gegevensverwerking en verantwoordelijkheden rondom de generieke digitale infrastructuur (gdi) van de overheid. Dit laatste betreft de gdi voorzieningen waarmee burgers en bedrijven nu reeds hun zaken regelen met de overheid. Dit geheel aan regelingen in de Wdo biedt burgers betere bescherming. De novelle die in de wet verwerkt wordt bevat daarbij diverse extra waarborgen ten aanzien van de privacy: eisen

die worden gesteld aan publieke en private inlogmiddelen die zowel aanvullend zijn ten opzichte van de eIDAS-verordening als een aanvulling op de AVG betreffen. Het gaat om de verplichte versleuteling van het burgerservicenummer, een striktere invulling van het verhandelverbod, de mogelijkheid om privacy by design expliciet in de toelating van inlogmiddelen mee te nemen en de toegroei naar open source.

Kan de regering een appreciatie geven van de huidige actualiteit van de wet?

Hoewel de behandeling al enige jaren vergt, staat voor de regering het nut en de noodzaak van deze wet buiten kijf. Sterker nog, de urgentie neemt juist toe. Zoals aangegeven stelt de eerste tranche van de Wet digitale overheid regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur. Het gaat daarbij enerzijds om het adequaat regelen en bieden van waarborgen aan burgers voor voorzieningen die zij nu reeds gebruiken, en anderzijds om te zorgen dat nieuwe voorzieningen op korte termijn een adequate basis kunnen krijgen. Bijvoorbeeld wettelijke vertegenwoordiging mogelijk te maken voor mensen die hun zaken niet zelf kunnen of mogen regelen. Met de eerste tranche van de Wet digitale overheid wordt dit geregeld en wordt onder andere, een systematiek voor (open) toelating en toezicht gecreëerd, welke naar gelang de maatschappelijke/politieke behoeftes en Europese ontwikkelingen, hergebruikt kan worden in volgende tranches van de Wet digitale overheid. De eerste tranche van de Wet digitale overheid creëert hiermee bovendien een stevig fundament voor toekomstige ontwikkelingen, in lijn met (toekomstige) Europese wetgeving.

De regering merkt immers meermaals op, onder andere inzake de belegging bij lagere regelgeving, dat de stand van de techniek zo snel verandert dat er snel moet worden kunnen geschakeld en dat dit via wetswijzigingen lastiger is. Hoe verhoudt zich dit tot dit voorstel?

Daar waar nodig zal de stand van de techniek belegd worden bij lagere regelgeving. Op deze wijze kan er naar behoefte, flexibeler om gegaan worden met de stand van de techniek zonder dat hiervoor de gehele wet gewijzigd dient te worden.

Zo spreken we over «privacy by design», maar spreken we nog maar beperkt over «attribute based identity» Waar zou je «attribute based identity» allemaal kunnen toepassen volgens de regering binnen de Wdo? De leden van de **PvdA-** en **GroenLinks**-fracties verzoekende regering dit mee te nemen in de bredere appreciatie.

«Attribute based identity», komt er kortgezegd op neer dat een persoon op het moment dat deze een dienst wil afnemen, de daarvoor noodzakelijke kenmerken (attributen) aan de dienstverlener levert. De mogelijkheden op deze manier «attribuut gebaseerd» diensten af te nemen is in potentie zeer groot, zowel binnen als buiten de overheid, en niet alleen voor online diensten, maar ook offline, bijvoorbeeld bij 18+ controle in winkels. Onder de huidige Wdo vindt in feite ook attribuutgebaseerde identiteitsverstrekking plaats, namelijk verstrekking van het burgerservicenummer. Dit gebeurt versleuteld, zodat het attribuut tussentijds niet aan derden geleverd kan worden, maar alleen aan de specifieke dienstverlener. Op dit moment is het zo dat de werking van de Wdo zich beperkt tot het overheidsdomein. Dit komt doordat de scope van de Wdo op dit moment gericht is op het overheidsdomein. In de tweede tranche van de Wdo zal ik inzetten op het verbreden van de scope naar het private domein.

De leden van de **PVV**-fractie lezen in de memorie van antwoord bij het voorstel Wet digitale overheid het volgende over de plannen voor een Europese digitale identiteit: «Met het voorliggende wetsvoorstel, de eerste tranche WDO, wordt reeds voor een belangrijk deel aan genoemde – toekomstige – EU-verordening voldaan. Beoogd wordt om in de tweede tranche WDO het onderwerp regie op gegevens/digitale identiteit te regelen, zoals ook aan Uw kamer gemeld in de memorie van antwoord. Hierover vindt de gedachtenvorming momenteel plaats; deze komt in belangrijke mate overeen met het onderwerp van de (wijzigings)verordening. De voorbereiding van de (wijzigings)verordening en de voorbereiding van de tweede tranche WDO zullen deels parallel plaatsvinden. Dit zorgt voor een nuttige wisselwerking, waarbij er rekening mee moet worden gehouden dat inhoud, reikwijdte en accenten van de (wijzigings-)verordening niet volledig zullen stroken met nationale beleidswensen.»[5]
Kan de regering, nu we bijna een jaar verder zijn, aangeven wat de actuele stand van zaken is van deze «gedachtenvorming»? Kan de regering ook aangeven op welke onderdelen er geen sprake zal zijn van «stroken met nationale beleidswensen»?

De eerste tranche van de Wdo legt – naast andere verplichtingen die buiten de werkingssfeer van eIDAS vallen – de basis voor de nadere invulling, en geeft waar nodig nationale invulling aan de (huidige) eIDAS-verordening. Met de gekozen systematiek in de Wdo (open toelating met eisen en toezicht daarop) heeft de Wdo een systematiek die de basis vormt waarop de (regulering van de) eIDAS-revisie kan voortbouwen. Andere functionaliteiten, zoals wallets, en eisen daaraan, kunnen met enkele aanvullingen in de wet door middel van een wetswijziging in deze systematiek worden opgenomen. Dat zal naar verwachting zijn beslag krijgen in de tweede tranche van de Wdo.

Voorts stelde de regering hierover «De verdere voorbereiding van de (wijzigings)verordening zal de komende maanden plaatshebben; na vaststelling volgt een implementatietermijn – de lengte daarvan is onderwerp van onderhandeling – waarbinnen de lidstaten hun regelgeving moeten aanpassen.».[6]
Kan de regering aangeven wat hiervan de actuele stand van zaken is en wat hiervan (vooralsnog) de impact is op de Wdo?

Naar verwachting zal het nog enige jaren duren voordat de herziening van de eIDAS verordening in werking treedt. De herziening van de eIDAS-verordening heeft geen impact op de eerste tranche van de Wdo. Dat wil zeggen de eerste tranche van de Wdo regelt wat nodig is in het hier en nu, zoals hierboven toegelicht. De eerste tranche houdt- zoveel als mogelijk al rekening met de ontwikkelingen die komen gaan, zoals de inregeling van een toelatingssystematiek voor inlogmiddelen. Voor de tweede tranche wordt vanzelfsprekend wel rekening gehouden met de herziening van de eIDAS verordening.

Over de laatste stand van zaken van de herziening van de eIDAS verordening bent u recentelijk door mij geïnformeerd in de voortgangsrapportage EDI en door mijn collega van EZK in het verslag van de Telecomraad van 3 juni jl.

In de technische briefing voor de Tweede Kamer op 10 mei 2022 werd door de ambtelijk deskundigen gesproken over implementatie van nieuwe Europese verordeningen in de volgende tranches van de Wdo, waaronder de Europese digitale identiteit. Kan de regering aangeven of met de

[5] *Kamerstukken I* 2020/21, 34 972, R, p.8.
[6] *Kamerstukken I* 2020/21, 34 972, R, p.8.

voorliggende eerste tranche van de Wdo geen onomkeerbare stappen worden gezet richting een Europese digitale identiteit? Kan de regering tevens aangeven op welke nieuwe Europese verordeningen nog meer wordt gedoeld en hoeveel extra tranches van de Wdo op dit moment zijn voorzien?

In de eerste tranche van de Wdo worden geen onomkeerbare stappen genomen. Er wordt, zoals eerder aangegeven geregeld wat er korte termijn nodig is, waarbij zoveel als mogelijk rekening wordt gehouden met toekomstige ontwikkelingen in het wettelijk kader. Een voorbeeld hiervan is het toelatingssysteem voor inlogmiddelen, dat zodanig is ingericht dat hierop kan worden voortgebouwd in het kader van de eIDAS revisie. Daarnaast is het nodig dat verschillende verordeningen in onderlinge samenhang worden geïmplementeerd. Voorbeelden daarvan zijn – naast de eIDAS-revisie – de digital markets act, de digital services act en de Single Digital Gateway verordening.

De digitale overheid is nooit af. Immers innovatie gaat altijd door. Datzelfde geldt voor wetgeving, de Wdo, die deze ontwikkeling moet sturen en kaderen. De kunst is daarom steeds zo dicht mogelijk op de ontwikkelingen te zitten. Dit is een doorlopend proces, en daarom is niet op voorhand te zeggen hoeveel tranches van de Wdo er nodig zullen zijn. Overigens is het streven steeds om nieuwe tranches zo toekomstvast mogelijk te laten zijn, zodat de houdbaarheid zo lang mogelijk is en het aantal tranche dus zo beperkt mogelijk wordt gehouden.

13. Besluit identificatiemiddelen voor natuurlijke personen Wdo

In het voorgehangen Besluit identificatiemiddelen voor natuurlijke personen Wdo[7] lezen de leden van de **PVV**-fractie in paragraaf 3.5 «Kosten voor gebruikers» van de Nota van toelichting: «De Minister van Binnenlandse Zaken en Koninkrijksrelaties biedt deze middelen als «nutsvoorziening» gratis of tegen beperkte kosten aan.»
Kan de regering nader aangeven wat hier wordt verstaan onder «beperkte kosten», hoe hoog mogen deze kosten maximaal zijn en hoe en door wie worden deze bepaald? Kunnen burgers zo worden gedwongen om onkosten te maken om digitaal te kunnen communiceren met de overheid? Indien van een inlogmiddel de erkenning wordt ingetrokken of technisch uitvalt, dient de gebruiker dan opnieuw te betalen voor de aanvraag van een alternatief inlogmiddel?

Uitgangspunt is dat de burger niet hoeft te betalen voor zijn contact met de overheid, dat wil zeggen elke keer dat hij inlogt. Wel is het zo dat voor bereiken van het gewenste betrouwbaarheidsniveau van het gebruikte middel een inlogfunctionaliteit op de identiteitskaart of rijbewijs wordt geplaatst. Met de uitgifte van deze documenten zijn leges gemoeid. Deze leges mogelijkheid is voor identiteitskaarten geregeld in de Paspoortwet en wordt voor rijbewijzen geregeld in de Wdo. Daarmee komt het publieke middel op betrouwbaarheidsniveau hoog beschikbaar.

Bij de technische briefing in de Tweede Kamer werd ten aanzien van het authenticatieproces gesproken over de inzet van tweefactor authenticatie. Kan de regering nader duiden hoe hierbij wordt omgegaan met de telefoon(nummer)gegevens/data van de gebruiker? Kan de regering uitsluiten dat telefoon(nummer)gegevens van een gebruiker hierbij aan andere datasets worden gekoppeld en/of voor andere doelen voor de overheid inzichtelijk (kunnen) worden?

---

[7] *Kamerstukken I* 2021/22, 34 972, S.

Op grond van de AVG en het concept Besluit digitale overheid en het nu nog geldende Besluit GDI, mag het telefoonnummer gebruikt worden voor de aanvraag, activering en het gebruik van de DigiD. Voor het gebruik van DigiD met tweefactor authenticatie kan een telefoonnummer vereist zijn.
Ook mag het telefoonnummer gebruikt worden bij gebruikersondersteuning of indien er signalen zijn van misbruik of oneigenlijk gebruik van de DigiD, of als er een wettelijke bepaling is waarop verstrekt moet worden. Denk hierbij aan de verwerking van gegevens in het kader van het meewerken aan een strafrechtelijk onderzoek.
Voor andere doeleinden dan bovenstaande wordt het telefoonnummer niet gebruikt.

14. Uitvoerbaarheid

In een artikel in *VNG Magazine* van 1 juli jl. lezen de leden van de **PVV**-fractie het volgende over de Wdo: «We hebben nu drie manieren om in te loggen: via DigiD, via eHerkenning of handmatig, waarbij de inwoner zelf gegevens moet invullen. Dat kunnen er straks meer worden, bijvoorbeeld met tools als Irma of Itsme. Dat betekent dat we nogal wat moeten ombouwen op de site en ook die andere inlogmiddelen moeten toevoegen.» Pijnpunt daarbij zit in de zogeheten «routeringsvoorziening». Idealiter zijn de inlogmiddelen als DigiD, Irma en Itsme sleutels die passen op hetzelfde slot. Maar het is maar de vraag of dat kan, (...). «Als dat niet kan, moet ik heel veel losse één-op-éénkoppelingen leggen. Dat leidt tot extra beheerskosten.»
Kan de regering aangeven in hoeverre deze «routeringsvoorziening» voor de verschillende inlogmiddelen praktisch haalbaar en uitvoerbaar is voor (lagere) overheden? Kan de regering nader ingaan op het genoemde punt van de extra beheerkosten, in hoeverre is in dit risico voorzien?

De Wdo maakt het mogelijk dat voor het verlenen van toegang tot de digitale dienstverlening van de publieke sector private partijen kunnen toetreden. In het ontwerp voor de nieuwe technische voorzieningen voor het stelsel Toegang, dat daarvoor nodig is, is een aantal maatregelen voorzien die het aansluiten van dienstverleners op het Stelsel (DigiD, eIDAS, eHerkenning en nieuwe private inlogmiddelen) eenvoudig en kosten efficiënt moet maken. Zo zal er gebruik worden gemaakt van industriestandaarden voor de technische verbindingen, waarmee één op één koppelingen worden voorkomen. Ook worden de huidige leveranciers, die op dit moment dienstverleners ondersteunen bij het aansluiten op DigiD, eIDAS en eHerkenning, nauw betrokken om de overgang naar het aansluiten op het nieuwe Stelsel zo eenvoudig mogelijk te maken.

Voorts stelt het artikel: «Ook is veel lagere regelgeving nog niet af, onlangs nog ging een regeling over gebruikersvoorwaarden in consultatie. Het noopte de VNG om begin juni een brief naar de Tweede Kamer te sturen, waarin aandacht wordt gevraagd voor de uitvoering. De wet kan nog niet in samenhang worden getest, schreef de VNG, omdat nog niet alle lagere regelgeving beschikbaar is. Volgens de VNG hebben gemeenten behoefte aan meer duidelijkheid, onder meer over de kosten en de planning van de wetswijziging.» Kan de regering gelet op de uitvoerbaarheid aangeven hoe de stand van zaken is van deze lagere regelgeving, de kostenverdeling en de planning? Kan de regering daarbij tevens aangeven welke afspraken zij in dit kader heeft gemaakt met gemeenten en andere lagere overheden?

Alle uitvoeringsregelgeving wordt voor consultatie voorgelegd aan het zogenoemde toetspanel Wdo. Dit toetspanel bestaat uit vertegenwoordigers van de organisaties die onder de reikwijdte van de Wdo vallen. Ook

de VNG neemt hieraan deel. Alle regels die voor de uitvoering voor dienstaanbieders van belang zijn, zijn op dit moment beschikbaar. De ministeriële regeling aansluitschema is hierop een uitzondering. Deze zal in overleg met de dienstaanbieders worden opgesteld en ingevuld.
Wat betreft de uitvoerbaarheid geldt dat de invoering van de Wdo, voor de duidelijkheid, niet gepaard gaat met een «big bang» waardoor in een klap een geheel nieuw stelsel voor Toegang volledig in werking zal treden. Ook is de wet techniekonafhankelijk. De juridische, organisatorische en technische basis van het stelsel zal naar verwachting circa een half jaar na de inwerkingtreding van de wet gereed zijn (juli 2023). Vanaf dat moment zullen overheden stapsgewijs gaan aansluiten. De aansluiting van alle overheidsorganisaties op het nieuwe stelsel zal naar verwachting in de eerste helft van 2026 volledig afgerond zijn.

Op dat moment zijn voor burgers en bedrijven alle (semi-)publieke organisaties digitaal bereikbaar met alle tot het stelsel toegelaten publieke en private inlogmiddelen. Bij het proces van inrichting, toetreding en aansluiting op het nieuwe stelsel worden alle dienstverleners nauw betrokken. Het komende half jaar wordt gewerkt aan migratieadviezen om inzichtelijk te maken wat voor de overheidsdienstverleners mogelijk en nodig is om de komende jaren op het stelsel aan te sluiten.

Daarnaast stelt het artikel: «De webformulieren die de gemeente nu heeft gebouwd, moeten straks «Wdo-proof» gemaakt worden (...). «Dat betekent dat we alle processen moeten upgraden naar een hoger betrouwbaarheidsniveau. Dat zorgt voor veel extra werk, omdat we alle formulieren weer langs moeten.» Kan de regering gelet op de uitvoerbaarheid aangeven in hoeverre rekening wordt gehouden met het Wdo-proof maken van webformulieren en het extra werk wat dit met zich meebrengt voor gemeenten? Kan de regering verder nader duiden hoe deze operatie zich verhoudt tot het gelijktijdig lopende traject van de implementatie van het Digitaal Stelsel Omgevingsrecht (DSO)?

Na inwerkingtreding van de Wdo zullen publieke dienstverleners, zoals gemeenten, al hun digitale, publieke diensten moeten classificeren naar betrouwbaarheidsniveaus. Het betrouwbaarheidsniveau is van belang voor de toegang tot de digitale dienst. Na de toegangsverlening start het dienstverleningsproces, waarbij door publieke dienstverleners veelal gebruik wordt gemaakt van een webformulier. De Wdo stelt geen eisen aan die webformulieren, maar aan de toegang daartoe.
Voor het bepalen van de betrouwbaarheidsniveaus stelt de ministeriële regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening regels. Om de benodigde tijd en capaciteit voor het kiezen van het juiste betrouwbaarheidsniveau te minimaliseren stelt het Ministerie van BZK daarnaast een online regelhulp beschikbaar. Deze tool faciliteert publieke dienstverleners bij dit proces.

15. Covid

In de nadere memorie van antwoord d.d. 14 september 2021 inzake de Wdo[8] gaf de (toenmalige) regering op de vraag van de leden van de **PVV**-fractie aan: «De leden van de PVV-fractie vragen de regering in hoeverre er plannen of intenties zijn om het in dit wetsvoorstel (en in de novelle) bedoelde identificatiemiddel ook te (kunnen) benutten voor coronamaatregelen, zoals het vaccinatiepaspoort en testen voor toegang?

[8] *Kamerstukken I* 2020/21, 34 972, R.

In antwoord op de vraag van de PVV-fractie merk ik op dat toegelaten/erkende middelen gebruikt kunnen worden bij alle diensten die door de overheid worden aangeboden. Dus ook voor de genoemde voorbeelden.».[9]

Inmiddels zijn we een jaar verder en is met het vervallen van de Tijdelijke wet maatregelen covid-19 (Twm) de wettelijke grondslag voor het coronatoegangsbewijs verdwenen. Kan de regering aangeven of in de huidige situatie de regering niet de intentie heeft om het identificatiemiddel in te zetten voor vrijheidsbeperkende collectieve coronamaatregelen, zoals een coronatoegangsbewijs?

Onder de Wdo kunnen toegelaten identificatiemiddelen gebruikt worden bij alle elektronische dienstverlening die door de overheid wordt aangeboden. Het gebruik van deze erkende identificatiemiddelen staat los van specifieke regelgeving zoals de reeds vervallen Tijdelijke wet maatregelen covid-19 (Twm).

In de bovengenoemde memorie van antwoord werd aangegeven dat «De Europese verordening met betrekking tot het digitaal EU-COVID-certificaat tot en met 30 juni 2022 van kracht zal zijn. Bij inwerkingtreding van de Wet digitale overheid zal worden bezien in hoeverre in dat kader nog maatregelen van kracht zullen zijn, waarop deze wet van toepassing wordt.».[10] Kan de regering aangeven in hoeverre de Wet digitale overheid zich in de huidige situatie zal verhouden tot het digitaal EU-COVID-certificaat, nu deze verordening met één jaar verlengd is tot 1 juli 2023?

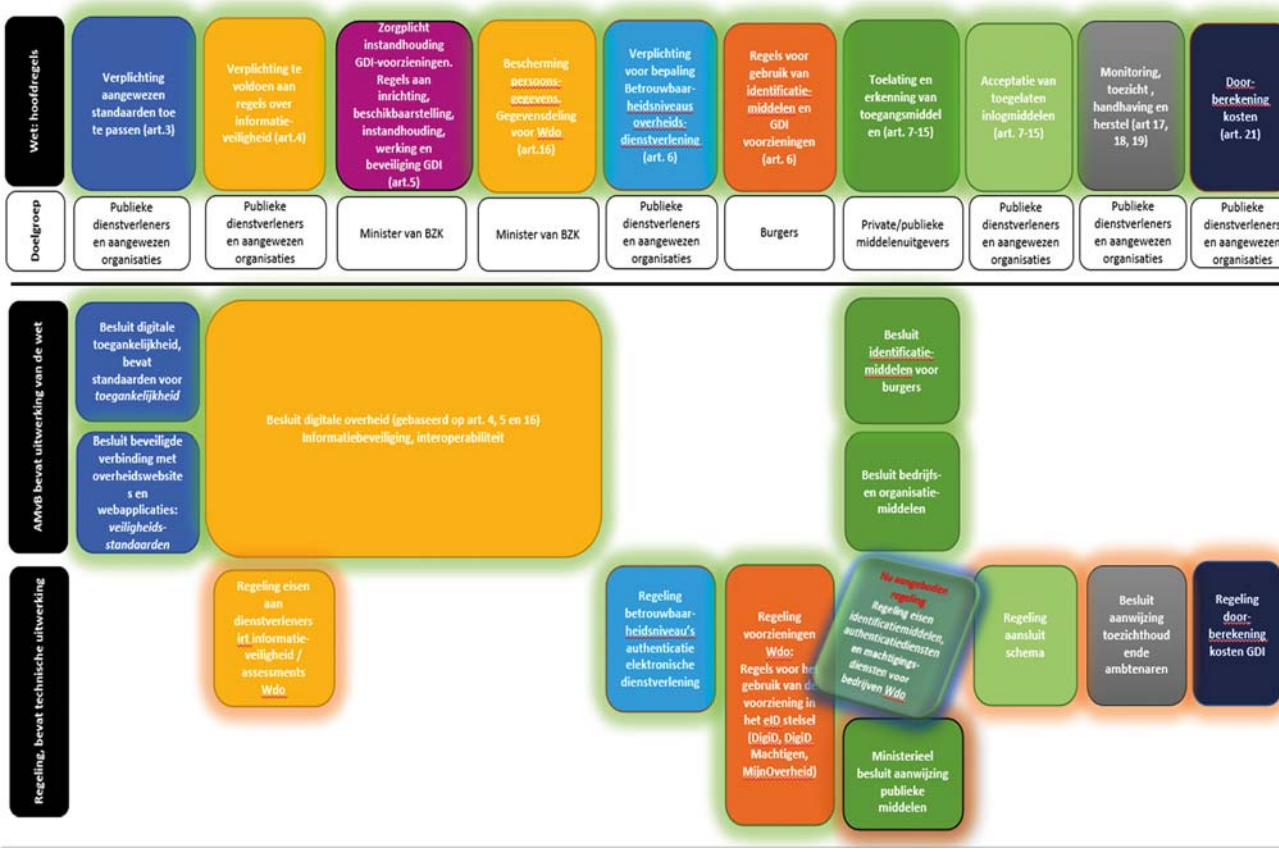
Bij inwerkingtreding van de Wet digitale overheid dienen de toegelaten inlogmiddelen te kunnen worden gebruikt bij elektronische dienstverlening vanuit bestuursorganen of aangewezen organisaties (waaronder ook zorgaanbieders). Op basis van het aansluitschema zullen middelen bij steeds meer overheidsdienstverleners gebruikt moeten kunnen worden. Dit betekent dat deze inlogmiddelen straks uiteindelijk gebruikt dienen te worden bij alle elektronische diensten die door de Nederlandse overheid wordt aangeboden, dus ook overheidsdiensten in het kader van Covid-19 en daarmee het EU-Covid certificaat. Ik merk op dat de Wet digitale overheid aan burgers geen verplichting oplegt voor het gebruik van elektronische overheidsdienstverlening.

Tevens merk ik op dat de CoronaCheck App is ontworpen conform de beginselen van privacy en security by design. De persoonsgegevens van de gebruikers van de app worden goed beschermd.

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

[9] *Kamerstukken I* 2020/21, 34 972, R, p. 7.
[10] Idem.

Figuur 1: Schematisch overzicht



Overzicht en stand van zaken: de groen omrande regelingen zijn reeds beschikbaar. Parallel aan de Memorie van Antwoord wordt de regeling met eisen aan inlogmiddelen toegezonden. De rood omrande regelingen volgen.

Figuur 2: Uitgebreid overzicht

Uitvoeringsregelgeving en uitvoeringsbesluiten onder de Wet digitale overheid

Regeling	Type regeling/ grondslag	Onderwerp + korte uitleg	Doelgroep / richt zich tot
Tijdelijk besluit digitale toegankelijk-heid	Zelfstandige amvb (art 3)	Aangewezen standaarden.	Publieke dienstverle-ners en private dienstverleners met een publieke taak.
Besluit beveiligde verbinding met overheidswebsites en -webapplicaties	AMvB (art 3)	Aangewezen veiligheidsstandaar-den.	Publieke dienstverle-ners en private dienstverleners met een publieke taak.

Uitvoeringsregelgeving en uitvoeringsbesluiten onder de Wet digitale overheid

Regeling	Type regeling/ grondslag	Onderwerp + korte uitleg	Doelgroep / richt zich tot
Besluit digitale overheid	AMvB (artt 4 en 5)	Informatiebeveiliging. Regels over de wijze waarop aangetoond kan worden hoe voldaan werking, betrouwbaarheid en beveiliging van de toegang tot elektronische dienstverlening op verschillende betrouwbaarheidsniveaus	Publieke dienstverleners en private dienstverleners met een publieke taak.
		Regels over verwerking, verstrekken en bewaren van persoonsgegevens door de voorzieningen en private middelen in het eID stelsel.	MinBZK, toegelaten private partijen, private makelaars
Regeling voorzieningen Wdo	Ministeriele regeling (art 10)	Regels voor het gebruik van de voorziening in het eID stelsel (DigiD, DigiD Machtigen, MijnOverheid)	Gebruiker (consument)
Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening	Ministeriele regeling (art 6)	Regels voor het bepalen van het betrouwbaarheidsniveau van authenticatie en machtiging voor een elektronische dienst.	Publieke dienstverleners en private dienstverleners met een publieke taak.
Besluit bedrijfs- en organisatiemiddel Wdo	Amvb (artt 11,13 en 22)	Authenticatie en identificatie van ondernemingen en rechtspersonen. Regels voor de erkenning van middelenuitgever, authenticatiedienst en machtigingsdienst voor bedrijven.	Private middelenuitgever, authenticatiedienst, machtigingsdienst voor bedrijven.
Besluit identificatiemiddelen voor burgers Wdo	AMvB (artt 9 en 22)	Regels voor toelating private middelen.	Private/publieke middelenuitgever
Regeling nadere eisen identificatiemiddelen, authenticatiediensten en machtigingsdiensten voor bedrijven Wdo	Ministeriele regeling (artt 9 en 22)	Regels voor toelating identificatiemiddelen en erkenning van authenticatiedienst en machtigingsdiensten voor bedrijven.	Private/publieke middelenuitgever, authenticatiedienst, machtigingsdienst voor bedrijven
Regeling kosten GDI	Ministeriele regeling (art 21)	Doorbelasten kosten samenhangende met de uitvoering van de GDI (artt 5 t/m 9).	Publieke dienstverleners en private dienstverleners met een publieke taak.

Uitvoeringsregelgeving en uitvoeringsbesluiten onder de Wet digitale overheid			
Regeling	Type regeling/ grondslag	Onderwerp + korte uitleg	Doelgroep / richt zich tot
Regeling aansluit-(schema)	Ministeriele regeling (art 29, lid 3)	Aansluitschema geeft gebruikers (burger/bedrijven) inzicht in het moment waarop een bepaalde dienstverlener zich conformeert aan de acceptatieplicht onder de Wdo. Vanaf dit moment kunnen burgers en bedrijven de dienstverlener daaraan houden.	Publieke dienstverleners en private dienstverleners met een publieke taak.
Regeling dienstverleners informatieveiligheids-assessments Wdo	Ministeriele regeling (art 4)	Ministeriele regeling waarin de huidige praktijk van de DigiD assessments wordt gecodificeerd.	Publieke dienstverleners en private dienstverleners met een publieke taak.
Besluit aanwijzing toezichthoudende ambtenaren (incl. binnen BZK-domein)	Ministerieel besluit (art 17, leden 1,2,4,5)	Aanwijzing toezichthoudende ambtenaren. Taak: toezicht op naleving van acceptatie, classificering en gebruik van publieke middelen in publieke domein.	MinBZK, Publieke dienstverleners en private dienstverleners met een publieke taak.
Besluit aanwijzing publieke middelen	Ministerieel besluit (art 9, lid 1)	Aanwijzingsbesluit waarmee DigiD als toegelaten middel wordt aangewezen.	Publieke middelenuitgever.