TWEEDE KAMER DER STATEN-GENERAAL **2**

Vergaderjaar 2020-2021

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)**

Nr. 4 **ADVIES AFDELING ADVISERING RAAD VAN STATE EN NADER RAPPORT**[1]

Hieronder zijn opgenomen het advies van de Afdeling advisering van de Raad van State d.d. 15 april 2021 en het nader rapport d.d. 18 juni 2021, aangeboden aan de Koning door de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties. Het advies van de Afdeling advisering van de Raad van State is cursief afgedrukt.

Blijkens de mededeling van de Directeur van Uw kabinet van 19 maart 2021, no. 2021000512, machtigde Uwe Majesteit de Afdeling advisering van de Raad van State haar advies inzake het bovenvermelde voorstel van wet rechtstreeks aan mij te doen toekomen. Dit advies, gedateerd 15 april 2021, nr. W04.21.0081/I, bied ik u hierbij aan.

De Afdeling advisering van de Raad van State heeft een aantal opmerkingen bij het voorstel en adviseert daarmee rekening te houden voordat het bij de Tweede Kamer wordt ingediend.

Hieronder zijn opgenomen het voornoemde advies, in cursief weergegeven, en de reactie daarop.

Bij Kabinetsmissive van 19 maart 2021, no.2021000512, heeft Uwe Majesteit, op voordracht van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het voorstel van wet houdende algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid), met memorie van toelichting.

Het voorstel betreft een novelle, die strekt tot wijziging van het wetsvoorstel inzake de Wet digitale overheid,[2] *indien dit voorstel tot wet wordt verheven. Aanleiding voor deze wijzigingen zijn de in de parlementaire behandeling bij de Eerste Kamer geuite zorgen inzake privacybescherming, in het bijzonder in relatie tot de positie van private technologieondernemingen. Om aan deze zorgen tegemoet te komen worden 'privacy by design', het verhandelverbod inzake persoonsgegevens en 'open source' als hoofdelementen wettelijk verankerd.*

De Afdeling advisering van de Raad van State merkt in dit advies op dat de begrippen privacy by design en open source niet voldoende worden uitgewerkt. Datzelfde geldt voor het verbod voor private aanbieders om inloggegevens commercieel te benutten. 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.

---

[1] De oorspronkelijke tekst van het voorstel van wet en van de memorie van toelichting zoals voorgelegd aan de Afdeling advisering van de Raad van State is ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer

[2] Gewijzigd voorstel van wet voor algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid), Kamerstukken I 2019/20, 34972, A.

Achtergronden en voorstel

De Wet digitale overheid bevat (een eerste tranche van) regels ten behoeve van de verdere digitalisering van de overheid. Het voorstel stelt onder meer regels over het verplichten van bepaalde standaarden, het beheer van diensten binnen de digitale infrastructuur van de overheid, informatieveiligheid en digitale toegang tot publieke dienstverlening. Het wetsvoorstel is op 18 februari 2020 door de Tweede Kamer aangenomen en ligt nu ter behandeling voor in de Eerste Kamer. De vaste commissie Binnenlandse Zaken en de Hoge Colleges van Staat/Algemene Zaken en Huis van de Koning van de Eerste Kamer heeft een hoorzitting gehouden met deskundigen, die daarin zorgen hebben geuit over de privacybescherming.[3] Op basis daarvan heeft deze Kamercommissie prealabele vragen aan de regering gesteld.[4] Dit heeft geleid tot de in de voorliggende novelle voorgestelde aanpassingen van het wetsvoorstel.

De geuite zorgen zien in het bijzonder op drie aspecten. In de eerste plaats is benadrukt om op het niveau van de wet te regelen dat bij het ontwerp van de inlogmiddelen rekening moet worden gehouden met de bescherming van persoonsgegevens ('privacy by design'). In de tweede plaats is grote zorg geuit over de mogelijkheden die commerciële partijen krijgen door inloggegevens te koppelen en vervolgens gevoelige data te vergaren. In de derde plaats hebben verschillende partijen dringend geadviseerd om in de wet de verplichting vast te leggen om de identificatie- (of inlog)middelen 'open source' aan te bieden, zodat de gebruiker kan controleren of de privacy en beveiliging goed zijn geregeld.

Op voornoemde drie aspecten wordt het wetsvoorstel aangepast met de voorliggende novelle. Daarnaast constateert de Afdeling dat de deskundigen ook in algemene zin hun zorg hebben uitgesproken dat de uitwerking van de wet, wetsbegrippen en waarborgen van proportionaliteit en subsidiariteit in belangrijke mate worden gedelegeerd naar lagere regelgeving, terwijl dit op het niveau van de wet moeten worden geregeld. Dit onderwerp wordt behandeld in punt 5 van dit advies.

Privacy by design

In het voorstel wordt geregeld dat erkenning van een privaat inlogmiddel wordt geweigerd indien "het ontwerp onvoldoende voorziet in de bescherming van persoonsgegevens".[5] Volgens de toelichting zijn ontwikkelaars op grond van de Algemene verordening gegevensbescherming (AVG) al verplicht om bij het ontwerp van inlogmiddelen de beginselen van gegevensbescherming in acht te nemen. De AVG is als Europese verordening rechtstreeks toepasselijk in de lidstaten. Omzetting middels nationaal-wettelijke bepalingen is in beginsel niet toegestaan (het zogenoemde overschrijfverbod). Wel moet nog worden geregeld dat dit principe een grond is om een erkenningsaanvraag af te wijzen. Dat was eerder voorzien in een uitvoeringsregeling. De door leden van de Eerste Kamer geuite zorg is aanleiding om deze afwijzingsgrond op het niveau van de wet te verankeren.[6]

Het stelsel van inlogmiddelen berust op een andere verordening van de Europese Unie, de zogeheten eIDAS-verordening.[7] Die verordening voorziet erin dat de Europese Commissie een interoperabiliteitskader opstelt, dat onder meer de toepassing van het beginsel van privacy by design dient te bevorderen. In het vastgestelde interoperabiliteitskader is daar echter niets over geregeld.[8]

Het is juist dat krachtens de AVG ontwikkelaars reeds zijn gehouden volgens het principe van privacy by design te werken. Dit laat echter onverlet dat privacy by design een breed begrip is, dat snel kan veranderen door veranderingen in de techniek, en dat door ontwikkelaars op verschillende wijzen en deels naar eigen inzicht kan – en moet – worden ingevuld. Tegelijkertijd moeten burgers erop kunnen vertrouwen dat inlogmiddelen die door de overheid zijn erkend veilig en betrouwbaar zijn en voldoen aan dit principe. Dit betekent dat de minister alleen de inlogmiddelen mag erkennen, die, beoordeeld naar de jongste stand van de techniek, voldoen aan het principe van privacy by design. En voorts geldt dat indien een erkend middel nadien niet meer voldoet aan dit principe, de erkenning zal moeten worden ingetrokken.

De Afdeling acht het daarom van belang dat duidelijk is hoe bij de toetsing aan deze weigeringsgrond precies

---

[3] Kamerstukken I 2019/20, 34972, G.

[4] Kamerstukken I 2019/20, 34972, I.

[5] Artikel 9, zesde lid, onder b. Artikel 11, achtste lid, onder b, voorziet in een vergelijkbare bepaling voor inlogmiddelen voor bedrijven.

[6] Toelichting, onder "Privacy by design".

[7] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PB 2014, L 257).

[8] EIDAS-uitvoeringsverordening inzake het interoperabiliteitskader, (EU) 2015/1501, Pb EU 2015, L 235/1.

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. Dat ligt wel in de rede. Voor de goede orde merkt de Afdeling op dat een dergelijke precisering met het oog op de uitvoering – namelijk de erkenning van het inlogmiddel – niet in strijd hoeft te komen met het overschrijfverbod. Van belang is dat de algemene maatregel van bestuur de rechtstreekse werking van het principe van privacy by design niet belemmert en het communautaire karakter ervan niet verbergt.[9] Dit kan in de algemene maatregel van bestuur tot uitdrukking worden gebracht, opdat de herkomst van de norm duidelijk is en geen twijfel kan bestaan dat de precisering in dat licht moet worden bezien.[10]

Gelet op het voorgaande adviseert de Afdeling het voorstel aan te passen.

In reactie op hetgeen de Afdeling adviseert merk ik op dat het wetsvoorstel zal worden aangepast conform het advies van de Afdeling, waardoor bij de invulling van privacy by design de actuele stand der techniek leidend is. Hiertoe zullen 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) worden aangevuld. Dit zal bij AMvB nader worden uitgewerkt, zoals de Afdeling adviseert. Op deze wijze kunnen gebruikers van identificatiemiddelen er op vertrouwen dat door de overheid erkende middelen optimaal veilig en betrouwbaar zijn, maar wordt ook aan aanbieders van middelen duidelijkheid en rechtszekerheid geboden.

3. <u>Verhandelverbod</u>

In het voorstel wordt geregeld dat een erkenning van een inlogmiddel wordt geweigerd, indien de aanvrager "niet aannemelijk heeft gemaakt dat geen inkomsten worden verkregen uit het verhandelen of verstrekken van gebruikersgegevens".[11]

Het doel van deze wijziging is te voorkomen dat gegevens van burgers commercieel worden uitgenut.[12] 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.

In reactie op hetgeen de Afdeling adviseert merk ik op dat het wetsvoorstel tot doel heeft private partijen te reguleren die inlogmiddelen voor de toegang tot overheidsdienstverlening op de markt willen brengen. De wetsbepalingen die betrekking hebben op erkenning en weigering zijn gericht tot deze doelgroep; zij mogen geen geld verdienen aan het verhandelen of verstrekken van gegevens over gebruikers of authenticatie van gebruikers die bij het aanbieden van authenticatiedienstverlening bij publieke dienstverleners zijn verkregen.
Het in algemene zin reguleren van alle vormen van commerciële uitnutting van persoonsgegevens valt buiten de werkingssfeer van dit wetsvoorstel.
De toelichting zal op dit punt worden verduidelijkt.

---

[9] HvJ 21 december 2011, *Danske Svineproducenter*, C-316/10, ECLI:EU:C:2011:863, punt 41. Voorts zij verwezen naar de Handleiding Wetgeving en Europa van het Kenniscentrum Wetgeving en Juridische zaken van het Ministerie van Justitie en Veiligheid, paragraaf 1.2.4.c en de aldaar genoemde rechtspraak en beginselen.
[10] In dat verband zou, indien beschikbaar, aangesloten kunnen worden bij een goedgekeurd certificeringsmechanisme (vgl. artikel 25, derde lid, AVG) en ligt het in de rede om op het niveau van de Unie afstemming over de precisering te zoeken.
[11] Artikel 9, zesde lid, onder c en 11, achtste lid, onder c voor inlogmiddelen voor bedrijven.
[12] Toelichting, onderdeel "Verhandelverbod".

4. Open source

In het voorstel wordt gekozen voor het uitgangspunt van "open source, tenzij". De minister weigert een inlogmiddel te erkennen, indien bij de werking van het middel of de processen naar zijn oordeel "onvoldoende gebruik wordt gemaakt van software die onder open source licentie is gepubliceerd".[13] In de deskundigenbijeenkomst is naar voren gekomen dat open source software in beginsel de beste garanties biedt dat de software veilig en betrouwbaar is,[14] mits de gemeenschap die de software onder zijn hoede heeft voldoende groot en actief is.[15]

a. Keuze voor open source
Uit de toelichting blijkt dat het streven is om geleidelijk over te gaan op open source software. Als meer open source mogelijkheden beschikbaar komen, zullen – zo stelt de toelichting – ook aanbieders van wie closed software is toegelaten de beweging naar open source moeten maken. Tegen die tijd zullen nieuwe aanbieders open source moeten aanbieden.[16]

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.[17]

De Afdeling adviseert het voorstel aan te passen.

In reactie op hetgeen de Afdeling adviseert merk ik in de eerste plaats op, dat in de deskundigenbijeenkomst door enkele aanwezigen naar voren is gebracht dat open source software in beginsel de beste garanties biedt dat de software veilig en betrouwbaar is, mits de gemeenschap die de software onder zijn hoede heeft voldoende groot en actief is. In de Memorie van Antwoord heb ik daar enkele nuanceringen bij geplaatst, aangezien ik van mening ben dat – omwille van de veiligheid en betrouwbaarheid – telkens naar de omstandigheden van het geval moet worden gekeken. Bij de aanvraag om erkenning zal telkens worden bezien of open source redelijkerwijs mogelijk is, waarbij het geheel van door de aanvrager te nemen maatregelen wordt beoordeeld op veiligheid en proportionaliteit. In de toelichting bij de novelle wordt aangegeven hoe de weigeringsgrond terzake wordt toegepast en welke wegingsfactoren daarbij gelden, met andere woorden: hoe artikel 9, zesde lid, onder d en artikel 11, achtste lid, onder d worden ingevuld met de geleidelijkheidsnorm en daarmee de beweging naar open source wordt gemaakt. In aansluiting op hetgeen de Afdeling adviseert zullen het zevende lid van artikel 9 en het derde lid van artikel 14 worden aangevuld, ter verankering van de bevoegdheid om een verleende erkenning te wijzigen, schorsen of in te trekken naarmate open source meer gemeengoed is.

b. Nadere uitwerking
Het is niet duidelijk wat onder "open source software" moet worden verstaan. De regering lijkt hieronder slechts te verstaan dat de broncode van de software openbaar is, zodat iedereen de betrouwbaarheid kan onderzoeken.[18] Onder open source kan echter ook worden verstaan dat de software door iedereen gratis te kopiëren, te gebruiken en te wijzigen is, en dat ontwikkelaars worden aangemoedigd om de software te verbeteren.

Het voorstel omschrijft het begrip als "software die onder een open source licentie is gepubliceerd" en laat de minister een ruime beoordelingsvrijheid bij de vraag wat verder onder dat begrip moet worden verstaan. Dit leidt tot onduidelijkheid hoe deze weigeringsgrond moet worden uitgelegd.

---

[13] Voorgesteld artikel 9, zesde lid, onderdeel d.
[14] Zie onder meer hetgeen de heren Böhre en Van Boheemen en mevrouw Moerel hebben opgemerkt in de deskundigenbijeenkomst, Kamerstukken I 2019/20, 34972, G, p. 6, 11, 14 en 25.
[15] Kamerstukken I 2020/21, 34972, L, p. 26.
[16] Toelichting, onder "Open source", onder "Wegingsfactoren bij toetsing".
[17] De minister kan een erkenning intrekken als – kort gezegd – niet langer wordt voldaan aan de erkenningsgronden (artikel 9, zevende lid).
[18] Kamerstukken I 2020/21, 34972, L, p. 26.

In het licht van het voorgaande, adviseert de Afdeling de toelichting, en zo nodig het voorstel aan te passen.

In reactie op hetgeen de Afdeling adviseert, merk ik op dat de Afdeling terecht opmerkt dat open source meebrengt dat de software door iedereen gratis te gebruiken, te kopiëren en te wijzigen is, en dat ontwikkelaars worden aangemoedigd om de software te verbeteren. De betekenis van "open source software" staat evenwel los van de wijze waarop de weigeringsgrond wordt toegepast. De toelichting zal op dit punt worden aangepast.

5. <u>Mate van delegatie</u>

Bij de behandeling van het voorstel in de Eerste Kamer is uitvoerig aandacht besteed aan de vraag of het wetsvoorstel zelf voldoende regelt en er niet teveel wordt gedelegeerd naar het niveau van algemene maatregel van bestuur of ministeriële regeling. Bij de deskundigenbijeenkomst zijn er indringende vragen gesteld over het niveau van regelgeving. De regering heeft geen aanleiding gezien het voorstel uit te breiden of aan te vullen. In de memorie van antwoord gaat de regering uitgebreid in op de algemene uitgangspunten bij delegatie van regelgeving; daarna behandelt ze pagina's lang de inhoud van het voorstel.[19]
In het deskundigenoverleg en het voorlopig verslag van de Eerste Kamer wordt de vraag gesteld of het advies van de Afdeling advisering op dit punt wel is opgevolgd.[20] In dat advies stelde de Afdeling dat het voorstel abstract en techniekonafhankelijk was geformuleerd en dat de uitwerking van de abstracte begrippen werd gedelegeerd aan lagere regelgeving. Zo werden begrippen als DigiD, MijnOverheid, DigiD Machtigen en het BSN-Koppelregister geregeld in de (ministeriële) Regeling voorzieningen GDI. 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.[21]

In de memorie van antwoord stelt de regering nu dat het advies van de Afdeling is opgevolgd. Het wetsvoorstel bevat de taken, verantwoordelijkheden en functionaliteiten met betrekking tot een aantal belangrijke voorzieningen van de generieke digitale infrastructuur. Concretisering en uitwerking vindt plaats bij lagere regelgeving; de grondslagen hiervoor worden in het wetsvoorstel ingekaderd en begrensd. "Anders dan de fracties lijken te menen, zit er derhalve geen licht tussen de zienswijze van de Afdeling Advisering van de Raad van State en die van de regering," zo stelt de regering.[22]

Het wetsvoorstel was echter niet gewijzigd op de punten die de Afdeling noemde. Het voorstel zoals destijds voorgelegd aan de Afdeling en de versie die nu bij de Eerste Kamer ligt zijn op het punt van de techniekonafhankelijkheid hetzelfde. In beide versies omschrijft het voorstel de functionele eisen waaraan de "generieke digitale infrastructuur" van de overheid moet voldoen, en wordt de techniekafhankelijke uitwerking overgelaten aan lagere regelgeving. Het gaat dan vooral om het Besluit digitale overheid, waarvan een conceptversie is voorgehangen bij de Eerste en Tweede Kamer. In die regeling worden de begrippen DigiD, MijnOverheid, DigiD Machtigen en het BSN-Koppelregister wel uitdrukkelijk geregeld.[23]

Zoals in de memorie van antwoord wordt vermeld, dient een wet de hoofdelementen van de regeling te bevatten. Het gevaar van techniekonafhankelijke 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 wet dient man en paard te noemen en het niet te laten bij de algemene aanduiding dat het gaat om zoogdieren. Bij abstracte wettelijke regels is het nog wel mogelijk zich voor te stellen wat daar op dit moment concreet onder moet worden verstaan, maar niet welke betekenis zij in de toekomst kunnen krijgen.

---

[19] Kamerstukken I 2020/21, 34972, L, p. 3-13.
[20] Kamerstukken I 2019/20, 34972, G, p. 12.
[21] Advies van 3 mei 2018, W04.17.0400, Kamerstukken II 2017/18, 34972, nr. 4, punt 6.
[22] Kamerstukken I 2020/21, 34972, L, p. 6.
[23] Kamerstukken II 2019/20, 34972, nr. 45. bijlage.

Als het voorstel op die manier wordt versterkt, hoeft dat geen rem te zijn op technologische vernieuwingen. Het voorstel bevat immers al twee bepalingen die de regering de mogelijkheid geven om tijdelijk van onderdelen van de wet af te wijken om ruimte te geven aan innovatie.[24]

De Afdeling adviseert in de toelichting op het voorgaande in te gaan en het voorstel aan te vullen met techniekafhankelijke elementen uit het ontwerp-Besluit digitale overheid, of anders aan te geven waarom dat niet wenselijk is.

In reactie op hetgeen de Afdeling opmerkt over de mate van delegatie, merk ik in de eerste plaats op, dat de zorg van een aantal deskundigen – en deze zorg kwam terug in vragen van de Eerste Kamer – primair verband hield met privacybescherming en open source. Het wetsvoorstel is naar aanleiding van de deskundigenbijeenkomst en het voorlopig verslag van de Eerste Kamer juist op die punten aangevuld, waardoor privacy bij design, open source en het verhandelverbod naar het niveau van de formele wet zijn getild.

In de tweede plaats merk ik op, dat conform het verzoek van de Eerste Kamer in de Memorie van Antwoord artikelsgewijs is aangegeven hoe het wetsvoorstel zich verhoudt tot de uitgangspunten inzake delegatie van wetgeving. Hierbij is toegelicht op welke wijze de centrale onderdelen van de generieke digitale infrastructuur (gdi) in de wet zelf zijn geregeld. Sprake is 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. 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.
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 (oa technische) ontwikkelingen. Dit sluit aan bij de eveneens tijdens de deskundigenbijeenkomst naar voren gebrachte opvatting dat bij dit type wetgeving delegatie alsmede betrokkenheid van het parlement (gecontroleerde delegatie) in de rede ligt.

Tot slot merk ik op, dat anders dan de Afdeling meent de door haar genoemde bepalingen, die de mogelijkheid bieden tot (tijdelijke) afwijking van de wet, geen soelaas bieden voor de toekomstbestendigheid van de gdi-voorzieningen.
De werkingssfeer van deze bepalingen is namelijk beperkt tot de toegang tot elektronische dienstverlening (inlogmiddelen) bij de overheid.

De Afdeling advisering van de Raad van State heeft een aantal opmerkingen bij het voorstel en adviseert daarmee rekening te houden voordat het voorstel bij de Tweede Kamer der Staten-Generaal wordt ingediend.

De vice-president van de Raad van State,
Th.C. de Graaf

Ik moge U hierbij verzoeken het hierbij gevoegde gewijzigde voorstel van wet en de gewijzigde memorie van toelichting aan de Tweede Kamer der Staten-Generaal te zenden.

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

---

[24] Bij algemene maatregel van bestuur kan worden afgeweken van de wet om nieuwe methoden te onderzoeken waarmee authenticatie doeltreffender en veiliger kan plaatsvinden (artikel 26). Verder kan de minister een erkende dienst ontheffing verlenen van bij of krachtens artikel 13 gestelde regels, indien deze regels in de weg staan aan technologische ontwikkelingen aangaande een betrouwbare toegang van ondernemingen en rechtspersonen tot elektronische dienstverlening (artikel 13, zesde lid).