Aan de minister van Binnenlandse Zaken en
Koninkrijksrelaties
Postbus 20011
2500 EA DEN HAAG

Datum
31 maart 2017

Onderwerp
Reactie consultatie wetsvoorstel GDI

Uw kenmerk

Ons kenmerk
JtH/RvZ/HS/RS/
2017/048

Bijlage(n)

Geachte minister,

Op 22 december 2016 is het voorstel voor de Wet generieke digitale infrastructuur (Wet GDI) voor internetconsultatie opengesteld. Omdat het wetsvoorstel potentieel grote regeldrukeffecten heeft, hebben wij besloten te reageren op deze consultatieversie. Onze reactie leest u in deze brief.

Bij de beoordeling van de regeldruk, gaan wij altijd uit van de volgende drie vragen:
1. Nuloptie: is er een taak voor de overheid en is regelgeving het meest aangewezen instrument?
2. Is de regeldruk proportioneel ten opzichte van het beleidsdoel? Zijn er minder belastende alternatieven mogelijk?
3. Is gekozen voor een passende uitvoeringswijze met oog voor dienstverlening?

Het kabinet wil de digitale dienstverlening van de overheid intensiveren. Een veilige en betrouwbare, digitale toegang tot deze dienstverlening is dan van groot belang. Het wetsvoorstel regelt de wettelijke randvoorwaarden voor het stelsel waarmee digitale toegang tot bestuursorganen wordt ingericht. Bestuursorganen zijn verplicht aan te sluiten op het stelsel. Burgers en bedrijven krijgen binnen het stelsel de keuze uit verschillende veilige middelen voor identificatie.

Regeldrukeffecten voor burgers en bedrijven

Het oogmerk is om de regeldruk voor burgers en bedrijven te verminderen door één erkend authenticatiemiddel in te voeren waarmee alle overheidsdienstverlening bereikbaar wordt. De memorie van toelichting (MvT) zegt daarover: *"Het wetsvoorstel regelt het voor authenticatie relevante deel van de infrastructuur bij bestuursorganen, zodat burgers met één erkend middel van het juiste betrouwbaarheidsniveau toegang hebben tot de digitale dienstverlening van alle bestuursorganen en aangewezen organisaties waarop het voorstel ziet. Hierdoor verminderen voor burgers de (administratieve) lasten, doordat hij niet langer aan diverse overheidsorganen dezelfde gegevens hoeft te verschaffen."*
De consultatieversie van het wetsvoorstel geeft niet aan hoeveel de regeldruk zal afnemen, omdat de regeldrukeffecten nog niet zijn gekwantificeerd. Dat is ook lastig omdat deze vooral

Contact
Rijnstraat 50 | Postbus 16228 | T (070) 310 86 66 | www.actal.nl
2515 XP Den Haag | 2500 BE Den Haag | info@actal.nl | @actal_info

afhangen van lagere regelgeving en omdat er onzekerheden zijn die een precieze kwantificering in dit stadium belemmeren. Het is wel mogelijk om de regeldrukeffecten in beeld te brengen met behulp van scenario's voor de invulling van de Wet GDI. Deze scenario's kunnen ook helpen bij de keuze voor de minst belastende beleidsoptie.

Wij adviseren om de regeldrukgevolgen van het wetsvoorstel te kwantificeren, bijvoorbeeld aan de hand van scenario's of bandbreedtes voor de nadere invulling van de wet.

De uiteindelijke regeldrukeffecten hangen sterk af van de nadere invulling door lagere regelgeving. Daarom verzoeken wij u om in een latere fase de ontwerpversies van deze lagere regelgeving aan ons voor te leggen voor ex-ante-toetsing.

Noodzaak van wetgeving

De regering vindt het gewenst dat overheden verplicht kunnen worden om gebruik te maken van open standaarden voor het elektronisch verkeer. Het wetsvoorstel regelt de wettelijke grondslag die nodig is om deze verplichting te kunnen opleggen. Actal verwelkomt deze mogelijkheid. Het verplichten van open standaarden[1] kan een goede bijdrage leveren aan het terugdringen van regeldruk: het voorkomt onder andere een "vendor lock-in"[2], en heeft naar verwachting een positief effect op de duurzaamheid van de digitale infrastructuur.

Daarnaast stelt het wetsvoorstel de wettelijke randvoorwaarden voor het stelsel voor authenticatie. Aansluiting op dit stelsel wordt verplicht voor bestuursorganen en ook voor private organisaties die elektronische diensten verlenen waarvoor een veilige en betrouwbare authenticatie essentieel is. Bijvoorbeeld zorgverzekeraars en pensioenuitvoerders. Echter, de MvT maakt niet duidelijk welke authenticatieproblemen zouden ontstaan zónder deze wet. Het lijkt erop dat de wettelijke verplichtingen alleen zijn geformuleerd voor het gebruiken van private authenticatiemiddelen bij publieke diensten. Het waarom van deze keuze is echter niet duidelijk. Als de overheid zich zou beperken tot publieke authenticatie, is wetgeving voor het toelaten en erkennen van private middelen misschien niet nodig. De Europese verordening over elektronische identificatie en vertrouwensdiensten voor elektronische transacties (EU Nr. 910/2014) laat lidstaten vrij om de private sector te betrekken bij het aanbieden van authenticatiemiddelen. Op dit moment zijn er al private én publieke elektronische identificatiemiddelen naast elkaar in gebruik. Bijvoorbeeld: DigiD, een publiek middel dat burgers toegang biedt tot overheidsdiensten, zorgverlening en zorgverzekeringen; en Idin, een private authenticatiemiddel dat toegang biedt tot de Belastingdienst en een zorgverzekeraar.

Private en publieke oplossingen naast elkaar leveren niet per se meer gemak op voor gebruikers. Ze kunnen ook extra regeldruk veroorzaken, zoals out-of-pocket-kosten. Gebruikers moeten kiezen voor een authenticatiemiddel en kunnen dus ook fout kiezen. Bijvoorbeeld omdat ze een hoger betrouwbaarheidsniveau nodig hebben en hun leverancier daarvoor geen

[1] Niet te verwarren met open source software. Open standaarden zijn niet-leverancier-gebonden bestandsformaten. Ook closed software (wel leverancier-gebonden) werkt doorgaans met open standaarden. Op dit moment bestaat "pas toe of leg uit"-beleid voor open standaarden.

[2] Het gebruik van open standaarden zou de overheid kunnen beschermen tegen het te veel moeten vertrouwen, of te veel afhankelijk zijn van een enkele leverancier. Maar een "vendor lock-in" van een leverancier maakt zijn klanten van hem afhankelijk omdat voor hen het veranderen van leverancier dan grote omschakelingskosten en/of ongemak tot gevolg zou hebben.

upgrade-mogelijkheid biedt. Dat levert frustratie en extra kosten op. Het is niet duidelijk in welke situatie er méér regeldruk is: [1] de overheid accepteert uitsluitend inlogmiddelen die zij zelf aanbiedt; of [2] de overheid accepteert meerdere, publieke en private inlogmiddelen. Daarom is het niet mogelijk om een heldere afweging te maken tussen deze twee opties.

Wij adviseren om de noodzaak van het wetsvoorstel beter te onderbouwen en daarbij expliciet onderstaande vragen te beantwoorden:

- **Wat gebeurt er als de overheid geen nieuw beleid maakt voor authenticatiemiddelen en de aansluiting daarop?**
- **Welke noodzaak is er om naast publieke authenticatiemiddelen ook private middelen te erkennen en aan te laten sluiten?**

Aansluiting is niet het einddoel

Het gevaar bestaat dat overheidsorganisaties denken dat ze er zijn als ze de verplichte aansluiting op de erkende inlogvoorziening hebben geregeld. Dit kan tot teleurstelling leiden bij burgers en bedrijven. Bijvoorbeeld omdat ze weliswaar kunnen inloggen bij een (semi)overheidsdienst, maar de achterliggende dienst niet volledig digitaal kunnen afnemen. Bijvoorbeeld: sommige gemeenten hebben wel een aansluiting op DigiD, maar voor een parkeervergunning moet de burger toch nog naar het loket. Verschillende gemeenten communiceren dat de procedure voor ondertrouw is gedigitaliseerd, maar dat is slechts gedeeltelijk gerealiseerd. De voorbereidende procedure gaat digitaal, maar om definitief in ondertrouw te gaan, is nog steeds een gang naar de gemeente nodig. De Ombudsman onderzoekt dit voorjaar (2017) hoe het komt dat burgers soms pas bij de eerste aanmaning, die altijd per post komt, ontdekken dat de overheid een onprettig bericht voor ze heeft. Eerdere berichten zijn dan digitaal verzonden terwijl de burgers niet wisten dat ze hun post digitaal zouden ontvangen. Of ze krijgen digitaal bericht van instanties hoewel ze niet daarvoor hebben gekozen, of zich dat niet realiseren.
Inloggen is nooit het einddoel; het gaat erom burgers en bedrijven daarna digitaal verder te helpen. Het is hierbij ook belangrijk om geen verkeerde verwachtingen te wekken over de online dienstverlening. Bijvoorbeeld bij de vooraf ingevulde aangifte inkomstenbelasting (VIA). De burger verwacht dat de voorlopige aanslag voor de IB ook vooraf is ingevuld. Een wijziging aanbrengen in de voorlopige aanslag zou dan niet veel inspanning vergen. Maar als blijkt dat de voorlopige aanslag niet vooraf is ingevuld, en dat voor het wijzigen álle inkomensgegevens moeten worden opgegeven, veroorzaakt dat teleurstelling en mogelijk afhaken van de burger.

Een wettelijke verplichting tot gebruik van een erkend inlogmiddel is dus geen garantie voor een betere digitale dienstverlening. Als de digitale dienstverlening beperkt blijft tot inlogmogelijkheden, terwijl de burger een deel van zijn zaken daarna toch analoog moet regelen, lijkt de dienstverlening ondergeschikt te worden gemaakt aan de wens van de overheid om haar burgers te kunnen identificeren.

Wij adviseren om het doel van de Wet GDI nadrukkelijker voorop te stellen. Maak duidelijk dat de verplichte aansluiting op erkende authenticatiemiddelen een middel is voor de verdergaande digitalisering en optimalisatie van de dienstverlening.

Meerdere authenticatiemiddelen voor hoger betrouwbaarheidsniveau

Burgers en bedrijven kunnen vaak niet van tevoren inschatten welk betrouwbaarheidsniveau een overheidsorganisatie zal eisen bij het inloggen. Als zij dan een authenticatiemiddel hebben aangeschaft met een te laag betrouwbaarheidsniveau, dienen zij extra kosten te maken als zij een extra inlogmiddel moeten aanschaffen.

Minder belastend zou het zijn, als wordt toegestaan om verschillende authenticatiemiddelen naast elkaar te gebruiken om op die manier een hoger betrouwbaarheidsniveau te realiseren.[3] Burgers en bedrijven hoeven dan minder vaak een nieuw authenticatiemiddel aan te schaffen.[4]

Wij adviseren om het wettelijk mogelijk te maken om in te loggen met behulp van meerdere authenticatiemiddelen, als die naast elkaar het vereiste betrouwbaarheidsniveau realiseren.

Uniforme overheidsdiensten? Dan één betrouwbaarheidsniveau

Artikel 5 lid 6 van het wetsvoorstel stelt dat "bestuursorganen en aangewezen organisaties bepalen met inachtneming van bij ministeriële regeling te stellen regels voor welke elektronische dienst tenminste het betrouwbaarheidsniveau substantieel of hoog geldt".[5] De ruimte die het wetsvoorstel hiermee aan bestuursorganen laat, kan leiden tot ongelijkheid. Bijvoorbeeld: gemeente A eist voor een bepaalde dienst bijvoorbeeld betrouwbaarheidsniveau *substantieel*, terwijl bestuursorgaan B betrouwbaarheidsniveau *hoog* eist. Dat is te verdedigen als er een inhoudelijk verschil is tussen de diensten. Maar als het gaat om dezelfde diensten, zoals de aanvraag van een paspoort, dan ligt het in de lijn der verwachting dat daarvoor hetzelfde betrouwbaarheidsniveau geldt. Daarmee wordt onnodige complexiteit en regeldruk als gevolg van verschillen tussen bestuursorganen voorkomen. In de ministeriële regeling die later zal worden vastgesteld, kan deze ruimte met nadere eisen worden ingeperkt.

Wij adviseren om bij uniforme overheidsdiensten ook uniformiteit in de betrouwbaarheidseisen na te streven door de beslissingsruimte in te perken in de nog vast te stellen ministeriële regeling.

Een loper past op vele sloten

Een inlogmiddel dat meer diensten online bereikbaar maakt, is voor dieven aantrekkelijker.[6] En voor de eigenaar van de gestolen online-identiteit levert dat meer problemen op.[7] Ook als er per ongeluk iets fout gaat met de online-identiteit, zijn de gevolgen voor de eigenaar groter als het

[3] Het gaat hier om de zogenoemde multi factor authentication. Deze maakt gebruik van factoren die onafhankelijk van elkaar, bij voorkeur via verschillende kanalen, verschillende eisen stellen: (1) iets dat iemand in zijn bezit ***heeft*** (bijv. een pasje), (2) iets dat iemand ***weet*** (bijv. een pin of wachtwoord), (3) iets dat iemand ***kan*** (bijv. een handtekening zetten), en/of (4) iets dat iemand ***is*** (zoals een bio-kenmerk, bijv. een vingerafdruk). De combinatie van deze verschillende eisen zorgt voor de realisatie van een hoger betrouwbaarheidsniveau dan de inlogmiddelen op zichzelf bieden.

[4] Zie ook ons advies over de regeldruk bij de registratie van machtigingen voor de Belastingdienst van 26 januari 2017.

[5] Op pagina 48 van de MvT wordt hierover toegelicht: "*Indien een burger of een bedrijf er (in de toekomst) voor kiest om via elektronische weg met een bestuursorgaan zaken te doen, is het vervolgens de vraag op welke elektronische wijze hij dit kan doen. Het nieuwe artikel 2:15 Awb verplicht het bestuursorgaan een kanaal (specifiek webformulier, een algemeen contactformulier, een app of een e-mail) voor het type bericht aan te wijzen. Op grond van dit wetsvoorstel zal het bestuursorgaan, voor zover het gaat om dienstverlening waarvoor het betrouwbaarheidsniveau substantieel of hoog geldt, deze dienstverlening alleen kunnen aanbieden met gebruik van erkende authenticatiemiddelen. Het is op grond van dit wetsvoorstel aan het bestuursorgaan om volgens bij ministeriële regeling te stellen regels, te bepalen voor welke elektronische diensten ten minste dit betrouwbaarheidsniveau substantieel of hoog geldt.*"

[6] Ongeveer 2% / 280.000 burgers geeft aan in de afgelopen twee jaar slachtoffer van identiteitsfraude te zijn geweest. Nulmeting adres- en Identiteitsfraude (BZK, 2016) en Identiteit in cijfers (Panteia, 2014).

[7] De MvT vermeldt 15.000 geblokkeerde DigiD's per jaar.

inlogmiddel toegang geeft tot meerdere private en publieke diensten. In de fysieke wereld zijn sloten waarvoor lopers[8] bestaan veel minder veilig dan sloten waarbij dat technisch onmogelijk is.

Jaarlijks worden enkele honderdduizenden burgers slachtoffer van identiteitsdiefstal. Zij krijgen dan te maken met grote bureaucratische rompslomp.[9] Het wetsvoorstel voorziet al in repressieve en correctieve maatregelen[10] en in maatregelen voor de herkenning van misbruik.[11] Maar het is daarnaast ook belangrijk om de gevolgen voor de getroffen eigenaren te minimaliseren. Het moet voor hen eenvoudiger worden om hun online-identiteit te herstellen en deze weer te kunnen gebruiken. Een belangrijke factor daarin is een betere coördinatie tussen de instellingen waarbij de slachtoffers zijn aangesloten. Het onderbreken, blokkeren en intrekken van de digitale identiteit is noodzakelijk, maar niet voldoende.

Wij adviseren om aanvullend op de repressieve maatregelen een proactieve ondersteuning te regelen voor burgers van wie de online-identiteit is gestolen of beschadigd. Die ondersteuning zou moeten voorzien in tijdelijke oplossingen, en tevens in een zo spoedig mogelijk herstel van de online-identiteit en de toegangsmogelijkheden die daaraan waren gekoppeld.

Een brief met gelijke inhoud en strekking hebben wij gezonden aan uw collegaminister van Economische Zaken.

Wij verzoeken u de definitieve versie van het wetsvoorstel Generieke digitale infrastructuur voor ex-ante-toetsing aan ons voor te leggen, voordat besluitvorming in de ministerraad plaatsvindt. Dit stelt ons in staat een formeel advies uit te brengen en ons eindoordeel aan u kenbaar te maken.

Wij zien uit naar uw reactie.
Hoogachtend,

J. ten Hoopen
Voorzitter

R.W. van Zijp
Secretaris

[8] Een loper is een sleutel die op meerdere sloten past. Een klassieke loper past op alle sloten van een bepaald type. Moderne lopers passen op een vooraf bepaald deel van de sloten. Zij worden bijvoorbeeld in hotels gebruikt door schoonmakers.
[9] De slachtoffers zijn veel tijd en energie kwijt aan het ongedaan maken van de identiteitsfraude. Bron: "*Help! Ze hebben mijn identiteit gestolen!!*" (Rapport identiteitsfraude SAFECIN, 2008)
[10] Noodzakelijk omdat er ook burgers zijn die bewust proberen hun online-identiteit kwijt te raken.
[11] Herkenning van misbruik is noodzakelijk omdat burgers er soms belang bij kunnen hebben om problemen met hun authenticatiemiddelen te veroorzaken.