

Aan de staatssecretaris van Binnenlandse Zaken en
Koninkrijksrelaties
De heer drs. R.W. Knops
Postbus 20011
2500 EA DEN HAAG

Datum
6 november 2017

Onderwerp
Wet GDI

Uw kenmerk

Ons kenmerk
MvH/RvZ/HS/RS/bs/
ATR0031/2017-U052

Bijlage(n)

Geachte heer Knops,

Op 16 oktober 2017 heeft ATR de Memorie van Toelichting van de na consultatie aangepaste Wet generieke digitale infrastructuur (Wet GDI) ontvangen. Deze memorie bevat de berekening van de gevolgen voor de regeldruk. Op 17 oktober 2017 is in ambtelijk overleg vastgesteld dat de gevolgen voor de regeldruk conform een eerder advies van Actal in beeld zijn gebracht en dat toetsing door ATR mogelijk is.¹ Hieronder treft u het advies van ATR aan.

Toetsingskader

ATR beoordeelt de gevolgen voor de regeldruk van voorgenomen wet- en regelgeving aan de hand van het volgende toetsingskader:

1. Nut en noodzaak: is er een taak voor de overheid en is wetgeving het meest aangewezen instrument?
2. Zijn er minder belastende alternatieven mogelijk?
3. Is gekozen voor een uitvoeringswijze die werkbaar is voor de doelgroepen die de wetgeving moeten naleven?
4. Zijn de gevolgen voor de regeldruk volledig en juist in beeld gebracht?

1. Onderbouwing nut en noodzaak

De memorie van toelichting geeft (onder andere) de volgende onderbouwing van het nut en de noodzaak voor een wettelijk kader voor de generieke digitale infrastructuur:

- 1) Elektronische dienstverlening tussen lidstaten geven ons een zorgplicht voor het inrichten van een knooppuntvoorziening. Aan die voorziening en de bijbehorende dienstverlening worden eisen gesteld ten aanzien van de authenticatie van burgers en bedrijven.
- 2) Diensten met rechtsgevolgen en gegevensuitwisseling van bijzondere persoonsgegevens vergen een hogere betrouwbaarheid en meer zekerheid dan het huidige DigiD biedt.

¹ Actal, Advies consultatie wetsvoorstel GDI, 31 maart 2017.

Contact

Rijnstraat 50
2515 XP Den Haag

Postbus 16228
2500 BE Den Haag

T (070) 310 86 66
info@atr-regeldruk.nl

www.atr-regeldruk.nl

- 3) Eisen ten aanzien van de betrouwbaarheid van de authenticatie en de vertrouwelijkheid van persoonsgegevens zijn essentieel voor nieuwe vormen van digitale dienstverlening, onder andere in de zorgsector en in de strafrechtketen.
- 4) Het ontwikkelen van en de verplichting tot aansluiten van publieke middelen naast private middelen wordt gemotiveerd door de eis dat burgers niet afhankelijk van private middelen mogen zijn voor het afnemen van publieke (digitale) dienstverlening.

Het college constateert dat de memorie van toelichting na de consultatie op onderdelen is aangepast. De memorie geeft invulling aan het advies van Actal om de noodzaak van wetgeving scherper te onderbouwen en daarbij aan te geven waarom voor de authenticatiemiddelen nieuwe wetgeving noodzakelijk is. Tevens motiveert de toelichting waarom wordt gekozen om publieke en private beveiligingshulpmiddelen naast elkaar toe te laten. Het college concludeert dat nut en noodzaak van het wetsvoorstel hiermee voldoende zijn toegelicht.

2. Minder belastende alternatieven

De huidige private voorziening met verschillende leveranciers die inlogmiddelen aanbieden in verschillende combinaties van betrouwbaarheidsniveaus, is voor ondernemers ingewikkeld en bewerkelijk. Deze complexiteit wordt in de volgende paragraaf verder toegelicht. In plaats van de nu beschikbare private middelen zou de authenticatie ten behoeve van de publieke dienstverlening ook met één publieke dienst kunnen worden gerealiseerd. Dit alternatief met één publiek inlogmiddel is misschien minder belastend voor bedrijven dan een variëteit aan private middelen. Het alternatief van één publiek inlogmiddel waarmee bedrijven toegang kunnen krijgen tot publieke dienstverlening, wordt in het voorstel echter niet uitgewerkt. Het gevolg van het niet uitwerken van dit alternatief is dat niet kan worden vastgesteld of de keuze voor verschillende private voorzieningen ook het minst belastende alternatief is.

2.1 Het college adviseert om te de gevolgen voor de regeldruk van één publiek inlogmiddel voor bedrijven te onderzoeken.

Het college onderkent dat het hanteren van één inlogmiddel risico's met zich brengt. Een belangrijk risico is dat bedrijven niet kunnen uitwijken indien het inlogmiddel uitvalt of indien hun identiteit is gecompromitteerd. Het college merkt daarbij echter op dat er andere manieren zijn om de kwetsbaarheid te beperken en continuïteit te waarborgen. Deze manieren zouden een plaats kunnen krijgen in het onderzoek naar de regeldrukgevolgen van het alternatief met één inlogmiddel.

3. Werkbare uitvoeringswijze

Het uitgangspunt dat burgers en bedrijven hun digitale diensten 24/7 kunnen 'afnemen' bij de overheid, is de grond voor enkele van de gemaakte keuzes. Als verschillende (publieke en private) middelen naast elkaar kunnen worden gebruikt, draagt dat bij aan een betere betrouwbaarheid en beschikbaarheid. Hoewel de MvT dat niet noemt, draagt deze keuze ook bij aan een grotere robuustheid tegen fraude en diefstal van identiteitsmiddelen. Bovendien vergroten hierdoor de controle- en herstelmogelijkheden bij fraude en diefstal. De keuze voor deze uitvoeringswijze kan voor burgers echter wel extra kosten met zich mee brengen in het geval ze meerdere identificatiemiddelen aanschaffen. Deze kosten zijn nu nog niet in te schatten maar

worden naar verwachting gerechtvaardigd door de grotere betrouwbaarheid, robuustheid en veerkracht.

Ondernemers worden in de huidige situatie op een vergelijkbare wijze geconfronteerd met extra kosten voor de aanschaf van e-Herkenningsmiddelen. Als blijkt dat een eerder aangeschaft identificatiemiddel bij een andere overheidsdienst (op een later moment) niet voldoet, ziet de ondernemer zich gedwongen tot het aanschaffen van een nieuw middel of het aanschaffen van een “upgrade”. Bij ondernemers bestaat hier weinig begrip voor: waarom kan een kleine ondernemer die maar zelden hoeft in te loggen, geen éénmalig eHerkenningsmiddel gebruiken? Met een ‘ticket voor toegang’ zouden ondernemers in veel gevallen geholpen zijn. De behoefte aan eenmalige toegang blijkt ook uit het bestaan van spoedprocedures voor eHerkennenning.

eHerkennenning biedt vijf betrouwbaarheidsniveaus (niveau 1, 2, 2+, 3 en 4). De Wet GDI zal de eIDAS verordening volgen en slechts drie betrouwbaarheidsniveaus kennen. De verwachting is echter dat eHerkennenning zal worden erkend als bedrijfs- en organisatiemiddel. Dan zouden de betrouwbaarheidsniveaus niet meer passen. In de huidige situatie staan overheidsorganisaties doorgaans namelijk niet alle vijf niveaus van eHerkennenning toe. Dit leidt tot onnodige complexiteit, bestaande uit verschillende betrouwbaarheidseisen en benodigde middelen bij verschillende overheden, voor soms zelfs gelijke producten. Een voorbeeld van die complexiteit vormen de keuzes van Nederlandse provincies. Zij hebben zes verschillende combinaties van betrouwbaarheidsniveaus.² De variëteit bij gemeentes is nog groter. Omdat een middel met een te laag of niet-ondersteund betrouwbaarheidsniveau niet kan worden ingezet, moeten bedrijven onnodige kosten maken voor het aanschaffen van een authenticatiemiddel dat wel wordt ondersteund en voldoende betrouwbaar is. Bovendien leveren niet alle aanbieders alle vijf beveiligingsniveaus, wat die aanschaf onnodig ingewikkeld maakt. De complexiteit, samen met onvoldoende terughoudendheid aan overheidszijde voor het kiezen van hoge betrouwbaarheidsniveaus, leidt tot onnodige kosten en onnodige veiligheidshandelingen bij bedrijven voor het gebruik van eHerkennenning.

Samengevat bestaat de complexiteit uit:

- 1) Complexe betrouwbaarheidsniveaus (5 niveaus) die niet met de eIDAS verordening (3 niveaus) overeenkomen.
- 2) Verschillen in duur, prijs en diensten van eHerkenningsmiddelen die worden aangeboden door verschillende private aanbieders. Commerciële overwegingen van aanbieders maken dat elke wijziging of aanvulling met kosten gepaard gaat.
- 3) Vergelijkbare overheidsdiensten vragen verschillende betrouwbaarheidsniveaus.
- 4) Complexiteit van de machtigingen en het ontbreken van middelen die eenmalig toegang verschaffen of eenmalig machtigen (tickets).

² Bijvoorbeeld: Overijssel gebruikt de niveaus EH1 en EH2, Zuidholland EH1 en EH2*. Voor eenzelfde type subsidieaanvraag eist de ene provincie EH2, terwijl EH2 niet wordt geaccepteerd door een andere provincie.

Deze complexiteit bemoeilijkt het gebruik van eHerkenning en verhoogt de kosten voor bedrijven. Bovendien onttrekt zij onnodig hoge betrouwbaarheidseisen aan het zicht.³ Daardoor is niet uit te sluiten dat er onnodige beveiligingshandelingen moeten worden verricht, met onnodige regeldruk als gevolg.

Iemand machtigen om een verplichting van de overheid na te komen kan door het gebruik van digitale middelen bewerkelijker worden, en soms wordt het zelfs onmogelijk. Zo kon voor het doen van een belastingaangifte vroeger een andere burger of adviseur worden gemachtigd door de aangiftebrief (en pincode) af te geven. Nu moeten voor het machtigen verschillende stappen worden ondernomen: aanvragen, afgegeven, toestemming geven of accepteren en bewaken van het gebruik. Dat is ingewikkelder dan voorheen. Bovendien moet bij het afgeven van machtigingen worden nagedacht over de vraag of deze machtiging voor één keer of voor altijd moet gelden.

Het college stelt vast dat de complexiteit van het gebruiken van eHerkenning niet voldoet aan de eisen voor een werkbare uitvoering van de Wet GDI. Het college acht een vereenvoudiging en uniformering of standaardisering noodzakelijk op alle vier de punten.

3.1 Het college adviseert om de betrouwbaarheidsniveaus van eHerkenning terug te brengen tot de drie niveaus van de eIDAS.⁴

3.2 Het college adviseert in overleg met aanbieders van eHerkenningmiddelen te komen tot een standaardisering van abonnementen en aanvullende diensten.

3.3 Het college adviseert de betrouwbaarheidseisen van overheidsorganisaties te uniformeren en waar mogelijk te verlagen⁵.

3.4 Het college adviseert het gebruik van machtigingsvoorzieningen te vereenvoudigen.

4. Gevolgen voor de regeldruk

Voor burgers maken enkele nu nog onbekende factoren en de verwachte lange duur van de implementatie (de "uitrol") het niet mogelijk om een realistische inschatting te maken van de regeldrukgevolgen. De regeldruk voor bedrijven is wel in beeld gebracht. Daarvoor is een scenario gevolgd. Gezien de onzekerheden over de mate van acceptatie en het tempo van de groei van het gebruik van digitale authenticatiemiddelen, ziet het college dat als de best mogelijke benadering.

³ Een hoger betrouwbaarheidsniveau valt niet goed te verdedigen als een andere overheidsorganisatie een lager betrouwbaarheidsniveau wel voldoende acht. Deze verschillen zijn niet makkelijk waarneembaar omdat er geen overzicht is van de vereiste betrouwbaarheidsniveaus voor dezelfde diensten bij verschillende overheidsorganisaties.

⁴ Uit ambtelijk overleg met BZK is ons duidelijk geworden dat reeds is besloten om de betrouwbaarheidsniveaus van eHerkenning in overeenstemming met eIDAS (met 3 niveaus) te brengen.

⁵ In ambtelijk overleg heeft BZK aangegeven dat het uniformeren van betrouwbaarheidseisen tussen grote uitvoeringsorganisaties is gerealiseerd.

Aan de hand van het scenario is zo goed mogelijk in beeld gebracht welke kosten bedrijven moeten maken voor het kennisnemen, afsluiten en in beheer hebben van een abonnement op een authenticatiedienst. Tegenover deze kosten worden baten verwacht die zullen bestaan uit een vermindering van het tijdsbeslag voor fysiek bezoek aan overheidsinstellingen, voor het invullen van papieren formulieren, en voor het ondertekenen en verzenden van stukken. Ook wordt verwacht dat bedrijven die een erkend inlogmiddel voor de hele overheid gaan gebruiken, minder tijd kwijt zullen zijn aan het beheren van toekennen van machtigingen. Van de omvang van deze besparingen is vooralsnog geen goede inschatting te maken.

Het college stelt vast dat de regeldruk, gegeven de onzekerheden en nog bij lagere regelgeving in te vullen factoren, adequaat in beeld is gebracht.

Dictum

Gelet op het voorgaande luidt het advies van het college over het Wetsvoorstel Wet generieke digitale infrastructuur (wet GDI):

Het wetsvoorstel indienen nadat met het bovenstaande rekening is gehouden.

Het college vertrouwt erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,

w.g.

M.A. van Hees
Voorzitter

R.W. van Zijp
Secretaris