Adviescollege toetsing regeldruk

> **Retouradres** Postbus 16228 2500 BE Den Haag

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

ATR, Adviescollege toetsing regeldruk
Rijnstraat 50
2515 XP Den Haag

Postbus 16228
2500 BE Den Haag

T 070 310 86 66
E info@atr-regeldruk.nl
www.atr-regeldruk.nl

Onze referentie MvH/RvZ/RS/bs/ATR1257/2020-U113
Uw referentie

Datum 6 augustus 2020
Betreft Regeling betrouwbaarheidsniveaus Wet Digitale Overheid

Geachte heer Knops,

Op 8 juli 2020 is de voorgenomen Regeling betrouwbaarheidsniveaus Wet Digitale Overheid (WDO) voor toetsing en advies aangeboden aan het Adviescollege toetsing regeldruk (ATR). De regeling vormt een uitwerking van de WDO voor wat betreft het classificeren van elektronische overheidsdiensten en het niveau van authenticatie daarbij, met het oog op een veilige inlog bij overheidsdienstverlening door burgers en bedrijven.

Toetsingskader

ATR beoordeelt de gevolgen voor de regeldruk aan de hand van het volgende toetsingskader:

1. Nuloptie (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. Nut en noodzaak

Burgers en bedrijven hebben belang bij veilige digitale overheidsdienstverlening. Van belang daarbij is zowel de inrichting van de dienstverlening zelf, als de digitale toegangscontrole tot deze dienstverlening. Belangrijk is daarom vast te stellen dat de overheid de dienst verleent aan de juiste persoon. Om deze reden is in de wet gekozen om de vaststelling van de mate van toegangscontrole en de keuze voor het toegangsmiddel een verplichtend karakter te geven. Doel van dit voorstel is om de toegang tot overheidsdienstverlening veiliger te maken en inlogniveaus voor vergelijkbare dienstverlening bij verschillende overheden eenduidiger.
Bestuursorganen en aangewezen organisaties moeten op grond van de wet bepalen welk betrouwbaarheidsniveau op een door hen aangeboden dienst van toepassing is. De wet bepaalt dat bij ministeriële regeling regels worden gesteld over de wijze waarop bestuursorganen en aangewezen organisaties dat doen en op welke wijze zij ervoor zorgen dat het betrouwbaarheidsniveau kenbaar is. Het voorstel bevat deze regels. Ter uitwerking van de WDO bevat de regeling een normatief kader dat mede is gebaseerd op de Europese

eIDAS-verordening.[1] Daarmee wordt bepaald welk betrouwbaarheidsniveau voor authenticatie ('laag', 'substantieel' of 'hoog') bij overheidsdienstverlening van toepassing is.

Het college constateert dat nut en noodzaak van het voorstel zijn onderbouwd. Het college ziet geen aanleiding voor adviespunten bij het onderdeel nut en noodzaak.

2. Minder belastende alternatieven

2.1 Tijdelijk lager niveau van authenticatie

De regeling maakt gebruik van de ruimte die de wet biedt om tot maximaal 2 jaar na inwerkingtreding van de regeling authenticatie toe te staan met een middel op een lager betrouwbaarheidsniveau dan het niveau dat wordt voorgeschreven. Dit betekent dat bij diensten, waarvoor gebruik moet worden gemaakt van een middel met betrouwbaarheidsniveau substantieel respectievelijk hoog, het gebruik van een inlogmiddel met het niveau 'laag' resp. 'substantieel' is toegestaan, mits sprake is van twee factor authenticatie.
De periode van 2 jaar biedt de mogelijkheid om op basis van de praktijk vast te stellen of er diensten zijn waarvoor het lagere niveau van authenticatie blijkt te volstaan. Door de ervaringen in de eerste twee jaar actief te monitoren en het normenkader op basis daarvan te actualiseren, bestaat de kans om onnodige lasten in de toekomst, als gevolg van een te hoog voorgeschreven authenticatieniveau, te voorkomen.

2.1 Het college adviseert a) te monitoren of authenticatie met een middel met een lager niveau werkbaar en uitvoerbaar is in de praktijk, en b) op basis van deze praktijkervaring te besluiten over de mogelijkheid om bij diensten structureel een lager niveau van authenticatie voor te schrijven.

Het college gaat er aanvullend op adviespunt 2.1 vanuit dat het authenticatieniveau bij een dienst alleen wordt verhoogd als de inhoudelijke noodzaak daartoe is aangetoond.

2.2 Diensten zonder (eisen aan) authenticatie

De onderhavige regeling richt zich op overheidsdiensten waarvoor eisen worden gesteld aan de authenticatie. De toelichting benoemt dat "een groot deel van de elektronische diensten in het geheel geen authenticatie behoeft door de gebruiker". Dat is bijvoorbeeld het geval bij algemene informatievoorziening waarbij de vaststelling van de identiteit van een burger of bedrijf niet van belang is, zoals bij het (anoniem) bezoeken van een overheidswebsite of het inzien van een WOZ-waardering. De regeling zelf maakt echter geen gewag van de categorie overheidsdiensten waarvoor geen authenticatie nodig is. Daardoor valt niet uit te sluiten dat dienstverleners onnodige lasten opleggen door ('voor de zekerheid') onnodige authenticatie te eisen. Dit kan worden tegengegaan door bijvoorbeeld in bijlage 2 expliciet duidelijk te maken dat er een categorie diensten is waarvoor geen authenticatie vereist is. Deze categorie ontbreekt nu in het normenkader.

2.2 Het college adviseert in de regeling te verduidelijken in welke situaties c.q. bij welke diensten geen authenticatie door de gebruiker noodzakelijk is.

[1] eIDAS staat voor 'Electronic Identities and Trust Services' en verwijst naar elektronische identificatiemiddelen en vertrouwensdiensten. De eIDAS-verordening is op 29 september 2018 ingegaan. Vanaf dat moment moeten publieke organisaties en private organisaties met een publieke taak Europees erkende inlogmiddelen accepteren binnen de digitale dienstverlening. Deze verplichting geldt onder andere voor organisaties die gebruik maken van DigiD en eHerkenning. Hiermee wordt het makkelijker en veiliger om binnen Europa online zaken te regelen.

3. Werkbaarheid

3.1 Uniforme bepaling niveau authenticatie per dienst

Bestuursorganen en aangewezen organisaties moeten op grond van het normenkader bepalen welk betrouwbaarheidsniveau op een door hen aangeboden dienst van toepassing is met het oog op authenticatie. De voorliggende regeling bepaalt welk betrouwbaarheidsniveau van toegang tot dienstverlening aan de orde is, afhankelijk van het type dienstverlening en de gegevens die van belang zijn voor de toegang tot deze dienst (bijvoorbeeld over hoe privacygevoelig gegevens zijn). De regeling legt geen specifieke betrouwbaarheidsniveaus vast voor de toegang tot specifieke overheidsdiensten. De regeling bepaalt bijvoorbeeld niet welk niveau van authenticatie van belang is voor inzage in medische gegevens, bij een melding van geboorte of van overlijden. Het is uiteindelijk aan de dienstverleners is om het betrouwbaarheidsniveau te bepalen. Hierdoor bestaat een kans op verschillen tussen dienstverleners bij verder uniforme diensten. Dit kan de werkbaarheid belemmeren voor burgers en/of bedrijven die actief zijn in meerdere gemeenten. Het is bovendien niet in lijn met het beleidsdoel van de regeling om de voorspelbaarheid van de dienstverlening te vergroten. De werkbaarheid van de regeling en de dienstverlening is gediend bij (meer) uniformiteit.

Eerder is door het Forum Standaardisatie een Handreiking opgesteld over de betrouwbaarheidsniveaus voor digitale dienstverlening voor overheidsorganisaties. Die handreiking bevat voorbeelden van (concrete) overheidsdiensten en betrouwbaarheidsniveaus die op basis van o.a. de bepalingen uit eIDAS-verordening bij elkaar horen. De Handreiking heeft echter geen bindend karakter. Het is mogelijk om de handreiking te gebruiken voor het verbeteren van de werkbaarheid van de regeling door voor dezelfde overheidsdiensten eenzelfde betrouwbaarheidsniveau vast te stellen. Daartoe kan een tabel uit de Handreiking (bindend) worden verwerkt in de regeling.

3.1 Het college adviseert voor uniforme overheidsdiensten het verplichte niveau van authenticatie (uniform) voor te schrijven, en indien hiervoor niet wordt gekozen dit inhoudelijk te motiveren in de toelichting.

Opvolging van adviespunt 3.1 kan bovendien voorkomen dat het vereiste niveau van authenticatie in de loop der tijd aan veel verandering onderhevig is en dat er grote verschillen tussen dienstverleners (bijvoorbeeld gemeenten) ontstaan. Dit vergroot de voorspelbaarheid en daarmee ook de werkbaarheid van de voorliggende regeling.

4. Gevolgen regeldruk

De regeling bevat een beknopte, kwalitatieve beschrijving van de lasteneffecten voor burgers en bedrijven. De regeling stelt dat de bepalingen het betrouwbaarheidsniveau en de betrouwbaarheid van overheidsdienstverlening verhoogt, evenals de veiligheid van de communicatie met de overheid. Daar staat tegenover dat "de hogere eisen leiden tot extra lasten voor burgers en bedrijven vanwege aan te schaffen middel(en) en extra lasten bij het inloggen, en tot meer handelingen voor de dienstaanbieder om met zekerheid iemands identiteit te kunnen vaststellen". De toelichting concludeert dat "alles afwegend, de extra lasten als verantwoord en proportioneel worden beschouwd". Deze conclusie wordt echter niet nader onderbouwd. Daarbij speelt dat een kwantitatieve onderbouwing van de baten en van de (regeldruk)kosten ontbreekt. Hierdoor kan op dit moment geen onderbouwde uitspraak worden gedaan over de proportionaliteit van de

(regeldruk)kosten. Het college acht het echter mogelijk om met behulp van bandbreedtes een kwantitatief beeld te schetsen van regeldrukeffecten van de regeling. Op basis van de huidige situatie en wijze van authenticatie, en de frequentie waarmee bepaalde diensten worden afgenomen, kan dit beeld worden bepaald. Inzicht in de omvang van de effecten draagt bij aan onderbouwde besluitvorming over de regeling.

4.1 Het college adviseert de regeldrukeffecten van de regeling uit te werken in de toelichting conform de Rijksbrede methodiek.

Dictum

Gelet op bevindingen en adviespunten is het eindoordeel van ATR bij de voorgenomen Regeling betrouwbaarheidsniveaus Wet Digitale Overheid:

De regeling niet vaststellen, tenzij met de adviespunten rekening is gehouden.

Het college benadrukt dat dit dictum geen inhoudelijke oordeel is over het voorstel maar alleen de onderbouwing ervan betreft. Het college vertrouwt erop u hiermee voldoende te hebben geïnformeerd en gaat er vanuit dat in het definitieve voorstel wordt toegelicht op welke wijze u met onze adviespunten rekening hebt gehouden.

Hoogachtend,

w.g.

M.A. van Hees
Voorzitter

R.W. van Zijp
Secretaris