Thauris
Prinses Catharina-Amaliastraat 5
2496 XD Den Haag

Postbus 95315
2509 CH Den Haag

t: 070 820 96 60
e: info@thauris.nl
www.thauris.nl

Ons kenmerk

-

Uw kenmerk

-

Bijlage

-

Onderwerp

Internetconsultatie GDI

Datum

31 maart 2017

Geachte heer, mevrouw,

Thauris is al jaren betrokken bij initiatieven gericht op het ontwerpen, implementeren en verbeteren van de digitale overheid en heeft hier altijd de verbinding gezocht tussen publieke en private organisaties die een rol spelen in informatieketens. Om die reden reageren wij hierbij dan ook graag op de internetconsultatie met betrekking tot de Wet generieke digitale infrastructuur (GDI).

Met interesse en waardering hebben wij kennisgenomen van het concept-wetsvoorstel GDI. Wij zien dit wetsvoorstel als een belangrijke stap vooruit in de richting van de verdere digitalisering van de dienstverlening van de overheid. Door dit wetsvoorstel zal het mogelijk worden om op een eenduidige, gemakkelijke en betrouwbare manier zaken te doen met de overheid, zowel voor burgers als voor bedrijven. Wel zien wij nog ruimte voor verbetering, in het bijzonder met betrekking tot de beoogde marktwerking en de betrouwbaarheid van het stelsel. Daarop zal hierna worden ingegaan.

**Markt en Overheid**

Wanneer het voor burgers en bedrijven noodzakelijk is bij de ‘verplichte’ elektronische communicatie gebruik te maken van middelen, kan niet altijd verwacht worden dat zij gebruik maken van middelen die uitsluitend door marktpartijen geleverd worden. Voor de doelgroepen of gevallen waar de marktoplossingen niet voldoende toepasbaar zijn, dient de overheid een gepaste alternatieve oplossing te bieden. Echter, dezelfde overheid kan het zich niet veroorloven om met publieke middelen voor alle segmenten maximale toegevoegde waarde te leveren. Dit is juist de kracht van marktpartijen, die het risico kunnen nemen om een unieke propositie te ontwikkelen voor een doelgroep, bijvoorbeeld zzp’ers. Wij vragen de wetgever vooraf de kaders

expliciet te maken om het algemene belang te waarborgen, zonder afbreuk te doen aan mogelijke positieve marktinitiatieven en de innovatie die zij kunnen bewerkstelligen.

In het bijzonder verzoeken wij u aandacht te besteden aan de positie van zzp'ers. Wanneer zij in privé optreden, kunnen zij uiteraard gebruikmaken van het publieke middel dat door de overheid verstrekt wordt, maar er moet voor gewaakt worden dat zij dit publieke middel niet in een zakelijke context kunnen gebruiken. In de zakelijke context moeten zij gelijk behandeld worden met andere ondernemers die een andere rechtsvorm gekozen hebben, en gebruikmaken van de middelen die op de markt verkrijgbaar zijn.

*Publieke middelen.* Uit het wetsvoorstel en de memorie van toelichting blijkt dat de overheid zelf ook middelen wil gaan aanbieden op de niveaus substantieel en hoog. Hiermee zal zij dus concurreren met eventuele private middelenaanbieders. Tegelijkertijd wil de overheid met het wetsvoorstel bereiken dat er marktwerking tussen private middelenaanbieders ontstaat. Dit roept de vraag op op welke wijze de overheid zich te gedragen heeft, wanneer zij zich op deze markt begeeft. Deze vraag zal beantwoord worden aan de hand van de gedragsregels zoals die gesteld zijn in de Wet Markt en Overheid (Hoofdstuk 4b van de Mededingingswet (Mw), zie ook Kamerstukken II 2007-2008, 31 354, nr. 3). Vanzelfsprekend is de formele wetgever juridisch bevoegd om af te wijken van deze wet, maar wij menen dat de hierin vervatte beginselen van waarde zijn.

*Verplichting tot doorberekening van alle kosten (art. 25i Mw)*. Indien de overheid economische activiteiten verricht, moet zij de volledige kosten hiervan doorberekenen aan de burger die van deze economische activiteiten gebruikmaakt. Met deze gedragsregel wordt voorkomen dat de overheid de markt kan verstoren door producten 'te goedkoop' in de markt te zetten. Hieraan lijkt tegemoet gekomen te worden door de kosten van het e-rijbewijs en de e-NIK aan de burger door te berekenen (p. 45 MvT). De vraag dringt zich dan wel op of de burger ook nog de mogelijkheid zal krijgen om een gewoon rijbewijs of een gewone identiteitskaart af te nemen, waar de kosten van het elektronische identificatiemiddel dan ook niet in zijn meegerekend. Indien immers alle rijbewijzen en identiteitskaarten alleen nog maar in de e-variant beschikbaar worden, is de doorberekening van de kosten niet meer dan een mooi gebaar: de burger zal dan immers verplicht zijn om deze kosten te voldoen als hij wil autorijden of zonder paspoort aan zijn identificatieplicht wil voldoen. Er is dan in feite sprake van koppelverkoop.

*Verbod op functievermenging (art. 25l Mw).* Voorkomen moet worden dat functievermenging optreedt tussen de overheid als uitvoerder van haar publieke taak en de overheid als marktpartij. Onduidelijk is nog hoe hieraan vormgegeven zal worden rond het e-rijbewijs en de e-NIK, nu bij deze middelen de publieke functie (identificeren en rijvaardigheid aantonen) en de private functie (functioneren als inlogmiddel) onlosmakelijk aan elkaar verbonden zijn. De overheid kan bij de uitgifte van de het e-rijbewijs en de e-NIK daarbij volledig steunen op de infrastructuur die zij al heeft aangelegd ten behoeve van de uitoefening van haar publieke taak in het kader van de uitgifte van gewone identiteitskaarten en rijbewijzen. Wij zouden graag zien dat maatregelen getroffen worden om aan deze bevoordeling van de overheid als marktpartij tegemoet te komen.

*Maximumtarieven*. In het wetsvoorstel is ook de mogelijkheid opgenomen om maximumtarieven voor authenticatiemiddelen vast te stellen. Dit zien wij als een ernstige bedreiging voor de goede marktwerking, zeker nu ook aan de maximering geen minimum is gesteld – noch in het wetsvoorstel, noch in de toelichting. Ook als niet direct wordt overgegaan tot het instellen van een maximumtarief, ontstaat door de mogelijkheid hiervan grote rechtsonzekerheid waardoor partijen die overwegen tot deze markt toe te treden, er niet op kunnen vertrouwen dat de door hen voorgenomen prijsstelling blijvend in overeenstemming met de wet zal zijn.

**Veiligheid en betrouwbaarheid**

Het wetsvoorstel streeft na om de dienstverlening van de overheid veilig en betrouwbaar te kunnen ontsluiten. Hiermee wordt zowel gedoeld op technische betrouwbaarheid (hacks voorkomen, etc.) als 'analoge' betrouwbaarheid (is de houder van het middel wel wie hij zegt dat hij is?). Beide vormen van betrouwbaarheid zijn zeer belangrijk voor het slagen van het stelsel.

Wij zien dat dit wetsvoorstel veel doet om de veiligheid en betrouwbaarheid van het stelsel te waarborgen. Voorbeelden hiervan zijn het invoeren van middelen op niveau 'hoog', het invoeren van een koppelregister waardoor de identiteit van een natuurlijk persoon eenduidig aangeduid kan worden en een sterke positie voor de toezichthouder. Wel denken wij dat de veiligheid en betrouwbaarheid met enkele eenvoudige maatregelen nog meer verhoogd kan worden.

*Koppeling met de Kamer van Koophandel*. In het voorstel wordt geregeld dat, indien een middel voor ondernemers wordt uitgegeven, de authenticatiedienst de vertegenwoordigings-bevoegdheid van de bijbehorende natuurlijke persoon moet controleren bij het Handelsregister (MvT, p. 20). Dit is uiteraard noodzakelijk, nu het Handelsregister de authentieke bron is met betrekking tot de vertegenwoordigingsbevoegdheid van bestuurders van rechtspersonen.

Echter, het Handelsregister kan slechts aantonen dat de persoon in kwestie vertegenwoordigings-bevoegd is op het moment dat de controle plaatsvindt. Als deze controle alleen plaatsvindt bij *uitgifte* van het middel, maar niet bij *gebruik* hiervan, kunnen zich nog steeds situaties voordoen waarin een rechtspersoon onbevoegd vertegenwoordigd wordt. Zeker nu een authenticatiemiddel vaak enige jaren geldig is, is de informatie die ten tijde van de uitgifte nog actueel was, dat ten tijde van het gebruik vaak niet meer.

Dit probleem komt uiteraard ook in de papieren wereld voor. Zeker voor kleinere transacties is het niet gebruikelijk het Handelsregister te bellen om zich ervan te vergewissen met een vertegenwoordigingsbevoegd bestuurder van doen te hebben. Men neemt dit aan, en pas als er problemen komen, wordt het Handelsregister geraadpleegd. (Deze handelswijze is door de Hoge Raad goedgekeurd in zijn arrest d.d. 3 februari 1984, *NJ* 1984, 386 (Damen/Geho). Hierin maakt de Hoge Raad duidelijk dat niet bewezen hoeft te worden dat degene die vertrouwd heeft op een in het Handelsregister ingeschreven feit, voorafgaand aan het vertrouwen het Handelsregister geraadpleegd heeft.)

Door voortschrijdende technologie doet zich nu echter de mogelijkheid voor om dit probleem op een nieuwe manier op te lossen: authenticatiediensten kunnen ook bij het *gebruik* de controle bij het Handelsregister uitvoeren. Zij kunnen bijvoorbeeld een heuristiek implementeren die op basis van de leeftijd van het authenticatiemiddel en de belangwekkendheid van de uitgevoerde handeling, een inschatting maakt of een hercontrole noodzakelijk is. Zo zal een authenticatiedienst eerder geneigd zijn een hercontrole uit te voeren bij een middel dat reeds twee jaar geleden is uitgegeven en sindsdien nooit meer is gebruikt, dan bij een middel dat de week daarvoor is uitgegeven. Ook ligt een hercontrole meer voor de hand wanneer iemand probeert in te loggen op een portaal waar bedrijfsgevoelige informatie kan worden ingezien, dan op een portaal waar slechts belastingaangifte gedaan kan worden.

Het enige bezwaar tegen deze methodiek is dat hiermee hoge kosten gepaard gaan. Het elektronisch raadplegen van de bestuurdersinformatie bij het Handelsregister kost ten minste €0,95 per keer (art. 3 lid 2 sub k van de Financiële regeling handelsregister 2014). Aangezien een authenticatie slechts enkele centen zal kosten, zijn deze kosten zeer substantieel. De overheid zou hierin tegemoet kunnen komen door voor authenticatiediensten binnen de GDI een aparte tariefklasse in te richten, of deze diensten in het geheel vrij te stellen van betaling aan het Handelsregister. Hiermee zou het stelsel sterk aan betrouwbaarheid winnen, aangezien dan bij een authenticatie kan worden aangetoond dat degene die inlogt, op dat moment bevoegd is de rechtspersoon te vertegenwoordigen.

*Het BSN-koppelregister en terugkerende gebruikers*. Uitgangspunt van het stelsel is dat de verwerking van het BSN door private partijen, waaronder authenticatiediensten, tot het minimum beperkt moet worden, maar dat wel zekerheid moet kunnen worden verkregen over de identiteit van de persoon in kwestie. Omdat naam, geboortedatum en geboorteplaats op zichzelf een persoon niet uniek identificeren, is verwerking van het BSN hiervoor wel in enige mate noodzakelijk. Om deze verwerking tot het minimum te beperken, is het BSN-koppelregister geïntroduceerd, waarmee de authenticatiedienst het BSN veilig kan afleveren bij publieke dienstverleners.

Ook binnen het private domein kan er behoefte zijn om gebruikers uniek te identificeren. Denk bijvoorbeeld aan de patiënt die een medisch dossier heeft opgebouwd met een middel van authenticatiedienst X, en vervolgens overstapt naar authenticatiedienst Y. Dan moet hij nog steeds bij datzelfde medische dossier kunnen, terwijl andere mensen met dezelfde naam, geboortedatum en geboorteplaats daar niet bij kunnen. Wij kunnen uit de werking van het koppelregister, zoals beschreven op pp. 17-18 van de MvT, niet afleiden dat dit zo werkt. Zou u, indien dit wel het geval is, dit kunnen verduidelijken, en indien dit niet het geval is, kunnen overwegen het ontwerp van het koppelregister op dit punt aan te passen?

*Een beoordelingskader voor betrouwbaarheidsniveaus.* Wij zijn zeer gunstig gestemd om te lezen dat het wetsvoorstel ervan uitgaat dat ook middelen van het betrouwbaarheidsniveau hoog zullen worden ingevoerd. Wel missen wij centrale sturing op het gebied van de toepassing van betrouwbaarheidsniveaus.

De hoogte van het betrouwbaarheidsniveau zou idealiter samen moeten hangen met (onder meer) de gevoeligheid van de informatie die zich achter de betreffende authenticatie bevindt of de impact van de rechtshandelingen die verricht kunnen worden. Het risico bestaat echter dat de keuze voor een bepaald betrouwbaarheidsniveau vooral wordt ingegeven door de status quo, waardoor een vicieuze cirkel ontstaat: zo lang weinig mensen een middel van het niveau hoog hebben, is het niet aantrekkelijk om authenticatie op dat niveau te eisen, en zolang weinig diensten authenticatie op dat niveau eisen, is het niet aantrekkelijk om een middel op niveau hoog aan te schaffen. Dit is juist de plaats waar de overheid een rol kan spelen door bepaalde betrouwbaarheidsniveaus af te dwingen en zo deze vicieuze cirkel te doorbreken.

Wij zouden er daarom voorstander van zijn als er een beoordelingskader zou komen aan de hand waarvan centrale en decentrale overheden voor elke dienst konden vaststellen welk betrouwbaarheidsniveau het beste gebruikt kan worden voor een bepaalde dienst. Dit kader zou bindend kunnen zijn, of op basis van pas-toe-of-leg-uit.

Een bijkomend voordeel van een dergelijk beoordelingskader is dat het kleinere decentrale overheden handvatten geeft aan de hand waarvan zij hun dienstverlening kunnen inrichten, waardoor zij hierover zelf geen specialistische kennis hoeven in te kopen. Hierdoor kan in de eerste plaats bij de initiële aansluiting worden bespaard. Ook geeft dit houvast indien geschillen ontstaan over het toegepaste beveiligingsniveau, bijvoorbeeld in het geval dat informatie gelekt is en een burger klaagt dat het bestuursorgaan zijn informatie niet voldoende beveiligd heeft. Als het gebruikte betrouwbaarheidsniveau is vastgesteld aan de hand van een goed onderbouwd beoordelingskader, kan aansprakelijkheid van het bestuursorgaan voorkomen worden.

Wij hopen dat wij u met deze opmerkingen van dienst kunnen zijn en zien uit naar het definitieve wetsvoorstel zoals dat aan de Tweede Kamer zal worden aangeboden.

Hoogachtend,

mr. V.B. de Haan