SZW (53)

Format

Uitvoerbaarheids- en handhaafbaarheidstoets Wet GDI

De wet GDI is in consultatie. Aan de (publieke) dienstverleners in de zin van de wet wordt gevraagd om de invoerings- en nalevingseffecten in beeld te brengen en een uitvoerbaarheids- en handhaafbaarheidstoets (U&H-toets) te doen. Het doel is het meer inzichtelijk krijgen van de effecten van de wet.

De vragen
Om de gevolgen van de wet duidelijk te krijgen, is het verzoek aan de organisaties die de Wet GDI moeten naleven en de departementen die een rol hebben bij de uitvoering van de wet, de vragen in dit format in te vullen. Het is de bedoeling dat zo veel mogelijk kwantitatieve gegevens boven tafel komen over de effecten en neveneffecten van de ontwerpwet.

U kunt het ingevulde format – tot en met 31 maart 2017 - sturen aan supportofficeeid@minbzk.nl. De door u verschafte informatie wordt betrokken bij de verdere voorbereiding van de wet en de bijbehorende memorie van toelichting. Vragen over dit format kunt u stellen via supportofficeeid@minbzk.nl.

Let op! De vragen vult u per departement of organisatie in. De vragen zijn bedoeld voor zowel de departementen als de (overige) bestuursorganen, behalve vraag 1a en 2a. Deze zijn alleen bedoeld voor de departementen.

Contactgegevens
Naam organisatie: SZW/DGSZI/SV
Naam contactpersoon: [redacted]
E-mail en telefoonnummer: [redacted]

Naam organisatie: SZW/WBJA
Naam contactpersoo[redacted]
E-mail en telefoonnummer: [redacted]

1. Uitvoerbaarheid
a. Vraag voor departementen: Welke organisaties op uw beleidsdomeinen dienen de wet na te leven?

- *Geef aan welke onder uw departement ressorterende uitvoeringsorganisaties de Wet GDI gaan uitvoeren (a-bestuursorganen).*

SVB en UWV en het departement zelf, met inbegrip van Agentschap SZW en Inspectie SZW

- *Geef aan welke andere (categorieën van) organisaties onder de reikwijdte van de Wet GDI moeten vallen (zie art. 3 lid 2 Wgdi).*

Pensioenfondsen

b. Is het de organisatie(s) helder wat de opgedragen taak is?

- *Geef daarbij ook aan of er taken of verplichtingen zijn die voor een correcte uitvoering c.q. naleving verduidelijking behoeven.*

Voor klantcommunicatie is het een randvoorwaarde dat er vanuit de overheid en de dienstenaanbieders eigen communicatiecampagnes worden opgezet om de nieuwe authenticatiemiddelen onder de aandacht te brengen en duidelijk te maken waarvoor deze dienen en hoe ze werken. Te denken valt aan reclamespotjes en informatiewebsites. We achten het niet de verantwoordelijkheid van UWV en SVB om uit te leggen hoe de authenticatiemiddelen aangevraagd kunnen worden, werken en hoe technische problemen opgelost kunnen worden.

c. Zijn/ is de uitvoerende organisatie(s) voldoende toegerust voor een doeltreffende uitvoering van de wet GDI?

- *Geef aan of er voldoende capaciteit is, of dat de uitvoering verschuiving van prioriteiten of andere maatregelen vergt.*
- *Geef aan of uw organisatie op het gebied van de ICT voldoende is toegerust. Geef ook aan of voldoende helder is wat de uitvoering van de automatisering vraagt.*

Unaniem is de mening dat de wet nog zeer veel onduidelijkheden bevat. Er is behoefte aan duidelijkheid over aspecten die van invloed zijn op de uitvoerbaarheid rondom financiering, de acceptatieplicht versus een doorgifteplicht. Het is voor UWV en SVB naast niet beïnvloedbare financiële afspraken bij de acceptatieplicht, technisch onuitvoerbaar (en zeer onwenselijk) om tot groot aantal technische koppelingen te moeten komen. Er is zicht op de delegatiebepalingen en uitvoeringsregelingen nodig, welke, wanneer die beschikbaar komen stuk voor stuk op uitvoerbaarheid getoetst zullen moeten worden.

1. Impact van Wet GDI inschatten is vooralsnog lastig zo niet onmogelijk.
a. Het gaat om de eerste tranche van een wet in wording.
b. De resultaten van de internetconsultatie moeten nog verwerkt worden, wat voorligt is een 'openingsvoorstel'.
c. Veel lagere regelgeving (incl. AMvB's) moet nog worden opgesteld en zal meeste impact hebben op de uitvoering.
d. Het gedeelte over open standaarden lijkt het minst uitgewerkt.
e. Samenloop tussen wGDI en gerelateerde wetgeving (AVG-implementatie, eIDAS en MEBV) is onduidelijk.

2. Er is nog veel onduidelijk over de Identity & Access Management(IAM)-middelen.
a. Expertise: is er voldoende expertise bij overheid en markt voor invoering?
b. Timing: sluit iedereen tegelijkertijd aan, hoe wordt afgestemd met eIDAS?
c. Bekostiging: hoeveel gaat het kosten?
d. Dekkingsgraad: wat is de reikwijdte van ieder IAM-middel m.b.t. de klantgroepen?
e. Verplichting: hoeveel middelen moeten uitvoerders straks accepteren? Acceptatieplicht versus doorgifteplicht waarmee de dienstaanbieders worden ontzorgd en waar hier zwaar aan wordt gehecht.

Toelichting bij onduidelijke aspecten van Identity & Access Management(IAM)-middelen.
Ad c) bekostiging IAM-middelen
MR van 24-2-2017 is besloten profijtbeginsel toe te passen: uitvoerder die gebruik maakt van bijv. DigiD dient mee te betalen aan de kosten ervan. De beprijzing van de nog te ontwikkelen nieuwe IAM-middelen is onbekend, dat kostenbeheersing bemoeilijkt.

Ad d) dekkingsgraad IAM-middelen
Voorbeelden:
- Digid Substantieel is alleen beschikbaar voor Android-platform
- Digid Machtigen is voorlopig niet beschikbaar
- Digid, eHerkenning zijn niet bruikbaar voor mensen zonder Nederlands paspoort of BSN
- Digid, eHerkenning zijn niet bruikbaar voor Nederlands woonachtig in het buitenland
- Digid laag en midden worden op relatief korte termijn uitgefaseerd.

Ad e) verplichting IAM-middelen
Moeten uitvoerders als UWV en SVB in de toekomst alle inlogfunctionaliteitleveranciers faciliteren?

Onderliggende aannames bij punt 2:
a) vrije verkeer interne markt: verplicht voorschrijven van specifiek-Nederlandse inlogfunctionaliteit zou gezien kunnen worden als protectionistische handelsbarrière, de wet lijkt zelf uit te gaan van een Europese markt waarbij door andere lidstaten erkende middelen moeten worden toegelaten
b) multimiddelenstrategie Nederland: alle middelen, zowel publiek als privaat, die voldoen aan een vastgesteld Uniform Stelsel van Eisen, zijn toegestaan en worden door de overheid gefaciliteerd
c) eIDAS-verordening: de EU-lidstaten zijn verplicht om elkaars eID-functionaliteit te faciliteren
Kortom, private partijen die aan het gestelde Uniforme Stelsel van Eisen voldoen mogen niet buitengesloten worden door uitvoerders als UWV en SVB.

Mogelijke impact als bovenstaande tweede vraag correct is:
- Verplichte aanschaf: SVB/UWV moet alle bestaande varianten te ondersteunen van eHerkenning, Idensys (bijv. iDIN), et cetera. Ook kleine, nieuwe private clubjes met een gering volume.

- Extra werkzaamheden: zelfs al zou SVB/UWV dit via 1 makelaar laten gaan waarvoor SVB/UWV een of meerdere API's beschikbaar stelt, dan lijkt het nog nodig te zijn om:
  - o contracten met iedere private IAM-leverancier af te sluiten
  - o jaarlijkse audit te ondergaan per private IAM-leverancier
  - o ICT-aanpassingen e.d. om aansluiting mogelijk te maken

"Omdat niet duidelijk is op hoeveel ontsluitende diensten gerekend moet worden en ook de kosten hiervan nog niet bekend zijn, zijn de gevolgen voor (Europese) aanbesteding niet te bepalen en kan de benodigde capaciteit hiervoor evenmin worden ingeschat."
Het blijkt moeilijk in te schatten in hoeverre een makelaar die tussen de uitvoerder en de IAM-leverancier staat bovenstaande problematiek zou kunnen afvangen.

Generieke kosten
Kosten van de instandhouding van de generieke voorziening, het BSN-K en van het publiekrechtelijk verankerde stelsel van toezicht op erkende partijen kunnen door het Rijk worden doorberekend (aan wie en wat betekent dat voor tarief dat aan partijen in rekening wordt gebracht). Als een prijs per authenticatie aan UWV in rekening kan worden gebracht kan UWV daar niet op sturen. Er wordt hiervoor een aanpak (AMvB) voorgesteld. Van belang is dat hierin vooraf voldoende helderheid wordt gecreëerd.

Jaarlijkse audit
UWV moet aan de (digitale) voorkant in staat zijn om te onderkennen met welk authenticatieniveau een klant binnen komt. Vervolgens moet kunnen worden vastgesteld tot welke digitale kanalen een klant op basis van het gebruikte authenticatieniveau wel of niet toegang heeft. Hiervoor wordt een matrix gecreëerd. Iedere divisie/directie heeft een overzicht gemaakt van alle contactmomenten die wij nu met klanten hebben. Deze moeten in de matrix worden opgenomen met het bijbehorende authenticatieniveau. Bij het ontstaan van nieuwe contactmomenten en verdere digitalisering moet altijd gezorgd worden voor het updaten van de matrix.

- *Geef aan in hoeverre de voor de uitvoering benodigde werkprocessen voorhanden zijn.*

Implementatie/risico's/control
Als de integriteit van een authenticatiemiddel aangetast is (bijv. door een hack of datalek) dan heeft UWV ondanks de verplichting om erkende authenticatiemiddelen te accepteren altijd de mogelijkheid om de eigen bedrijfsvoering te beschermen en het authenticatiemiddel tijdelijk uit te sluiten. Geadviseerd wordt om dit in de MvT expliciet op te laten nemen, of onderdeel van de erkenningsprocedure te maken.
Voor de implementatie is het BSN-Koppelregister een zeer belangrijke schakel. Beschikbaarheid hiervan is dus cruciaal voor de implementatie van de generieke regels over elektronische authenticatie.

d. Wat zijn de verwachte effecten van de ontwerpwet voor uw organisatie of departement?

- *Geef aan wat de effecten van de ontwerpwet zijn op de digitale dienstverlening aan de burger en ondernemer.*
- *Geef aan welke producten of processen door de Wet GDI geraakt worden en wat de voordelen en nadelen van de ontwerpwet zijn.*
- *Geef aan of er ook mogelijke neven- en onvoorziene of onbedoelde effecten zijn.*

Machtigen
Voor rechtspersoon authenticatie is op dit moment nog niet helder wat er precies in de uniforme set van eisen komt te staan. UWV heeft begrepen dat hierin wel iets wordt opgenomen over horizontaal machtigen (ketenmachtigen; de ene juridische entiteit machtigt de andere) en verticaal machtigen (het binnen het bedrijf autoriseren van medewerkers om namens het bedrijf te handelen). Deze functionaliteit is voor UWV randvoorwaardelijk, in de huidige digitale werkgeversdienstverlening wordt veel gebruik gemaakt van horizontaal en verticaal machtigen. Wanneer de uniforme set van eisen voor rechtspersoon-authenticatie beschikbaar is willen we de uitvoering hiervan graag toetsen.

Momenteel verstrekt UWV voor toegang tot haar werkgeversportaal een eigen authenticatiemiddel. In dit middel is naast authenticatie ook de autorisatie voor medewerkers van een werkgever geregeld (vertikaal machtigen) en kunnen intermediairs worden gemachtigd (horizontaal machtigen). In de huidige eerste tranche van de Wet GDI is gebruik van dergelijke autorisatievoorzieningen (machtigingen) nog niet opgenomen. Zoals genoemd is het randvoorwaardelijk dat dit geregeld wordt in nog op te stellen uniforme set van eisen voor rechtspersonen. Deze voorzieningen worden in een vervolgtranche van Wet GDI opgenomen waarbij overheidsdienstverleners worden verplicht aan te sluiten op een generiek machtigingenregister. Dit betekent dat alles wat voor het bekend worden van genoemde vervolgtranche in het kader van machtigen gerealiseerd wordt, een mogelijke desinvestering is.

Werkgevers gevestigd in Nederland of in de grensstreek met Nederland kunnen voor een account op Werk.nl in aanmerking komen. Voor de werkgevers in de grensstreek is inloggen met een eID zeker aan te bevelen. Dit is iets wat ingeregeld moet gaan worden.

Het onderwerp machtigen is momenteel aan de orde in verschillende gremia die bij ontwikkeling van digitale dienstverlening voor burgers en ondernemers betrokken zijn (bv berichtenbox, Digipoort, Mijn Overheid voor Ondernemers). Wij adviseren nadrukkelijk de aandacht voor het onderwerp machtigen bij deze verschillende ontwikkelingen te combineren.

Aantal ontsluitende diensten
De concept Wet GDI biedt de mogelijkheid voor private partijen om authenticatiemiddelen aan te bieden middels een zogenoemde ontsluitende dienst. Middels de wet is UWV verplicht iedere ontsluitende dienst die door de Minister wordt erkend, te accepteren. Acceptatie van een ontsluitende dienst door UWV vergt een aanpassing aan de UWV systemen voor elektronische dienstverlening. In de concept wet is geen maximum gesteld aan het aantal ontsluitende diensten. In de praktijk moet blijken hoeveel private ontsluitende diensten zullen ontstaan. Volledige consequentie hiervan is dus op dit moment nog niet aan te geven.

Verder ontbreken op dit moment nog de kaders waarbinnen en de regels waarlangs doorbelasting van kosten voor het eID-stelsel door de private ontsluitende diensten aan de publieke dienstverleners plaatsvindt. Hiermee ontstaat in feite een 'open-eind' situatie die financiële onduidelijkheid en daarmee risico's voor de publieke dienstverleners oplevert. Wij dringen er dan ook op aan dat deze onduidelijkheid ruim voor invoering van de wet wordt weggenomen conform de mogelijkheden die hiervoor in artikel 21 (Tarifering) van de wet worden geboden.

Daarnaast betekent het ontstaan van meerdere ontsluitende diensten dat iedere publieke dienstverlener een overeenkomst met iedere individuele ontsluitende dienst moet afsluiten. Hoewel via de Wet GDI een publieke dienstverlener verplicht is de betreffende ontsluitende dienst te accepteren, is ons nog niet duidelijk in hoeverre het aanbestedingsrecht hierop van toepassing is.
Daarnaast vraagt het afsluiten van overeenkomsten met iedere ontsluitende dienst in inkoop-inspanning voor iedere publieke dienstverlener. Wij adviseren dan ook hierover gemeenschappelijke centrale afspraken te maken teneinde deze adminstratieve last overheidsbreed zoveel mogelijk te beperken.

Verhouding wGDI-Archiefwet
In het wetsvoorstel (artikel 9) worden regels aangekondigd met betrekking tot bewaartermijnen voor persoonsgegevens. Hiermee ontstaat mogelijk een discrepantie met bestaande wet- en regelgeving mbt bewaartermijnen en met name met de Archiefwet 1995 en mogelijk met Wob/Woo. (verder toelichting wordt gegeven in Bijlage 1).
UWV verzoekt om aanvullende informatie op te nemen in de Wet GDI en in de MvT over de verhouding tussen de Wet GDI en de Archiefwet 1995. Niet als dusdanig benoemd maar mogelijk wel verstandig is om in de MvT ook te vermelden wat de verhouding is tussen de Wet GDI en de Wob/Woo.

Uitvoerbaarheid verplicht stellen open standaarden
UWV heeft begrip voor de overwegingen van de minister om een grondslag te bieden om, bij algemene maatregel van bestuur, een verplicht toe te passen open standaarden aan te wijzen.

Aangegeven wordt dat open standaarden, die in aanmerking komen voor verplichte toepassing, zijn opgenomen in de 'pas-toe-of-leg-uit-lijst'. Waar mogelijk volgt UWV deze standaarden momenteel al. Indien verplicht alle standaarden gevolgd moeten worden heeft dat grote consequenties, veel standaard moeten gemigreerd worden met de nodige kosten. UWV gaat er dan ook vanuit dat bij het overwegen om een open standaard bij algemene maatregel van bestuur verplicht te stellen, er aan UWV gevraagd zal worden hiervoor een aparte uitvoeringstoets uit te voeren.

In de MvT worden voornemens kenbaar gemaakt om toegankelijkheids- en informatieveiligheidsstandaarden aan te wijzen als verplicht toe te passen standaard. Of en met welke consequenties uitvoering gegeven kan worden aan het verplicht toepassen van deze open standaarden moet blijken uit uitvoeringstoetsen die zullen volgen op het aankondigen van de hiertoe benodigde algemene maatregelen van bestuur.

Ten aanzien van de open standaarden waarvoor het voornemen kenbaar is gemaakt om verplicht aan te wijzen, kunnen we, onder voorbehoud van de nog uit te voeren uitvoeringstoetsen, aangeven:
- Toegankelijkheidsstandaard: In de MvT wordt het voornemen uitgesproken de Europese standaard ETSI EN 301 549 aan te wijzen als verplicht toe te passen standaard. Gezien de mate van gedetailleerdheid van deze standaard worden aanzienlijke consequenties bij implementatie voorzien.
- Informatieveiligheidsstandaarden: In de MvT wordt een aantal standaarden benoemd die in aanmerking komen om te worden verplicht.

e. Wat zijn de gevolgen van de acceptatieplicht van de erkende middelen?

- *Geef aan wat de gevolgen van de acceptatieplicht zijn, mede in relatie tot interoperabiliteit, tarifering, de uitfasering van DigiD-laag/basis en de ambitie om bestuursorganen en aangewezen organisaties zo eenvoudig mogelijk aan te kunnen laten sluiten op de diverse erkende authenticatiemiddelen.*

Zie hierboven

f. Wat zijn de ingeschatte kosten die nodig zijn voor uitvoering van de wet voor uw organisaties of departement?

- *Geef aan om welke type kosten (directe/indirecte kosten?) het gaat en of het eenmalige of structurele kosten zijn.*
- *Geef aan waarop de inschatting is gebaseerd en of de kosten als proportioneel kunnen worden beschouwd.*

De eenmalige kosten voor aanpassingen aan voorgestelde veiligheidsstandaarden en structurele kosten voor aanpassingen aan de voorgestelde veiligheidsstandaarden zijn in dit stadium nog niet in te schatten. Hetzelfde geldt voor eenmalige en structurele kosten voor aanpassingen aan voorgesteld toegankelijkheidsstandaarden.

Zoals hierboven betoogd zijn de eenmalige en structurele kosten voor aansluiting van ontsluitende diensten zonder nadere uitwerking van de delegatiebepalingen en het onderzoek naar tarifering niet objectief in te schatten.

Kosten voor uitvoeren van verplicht jaarlijkse audit.

2. Handhaafbaarheid

a. Vraag voor departementen: Welke organisaties of organisatieonderdelen zullen toezicht houden op een correcte uitvoering van de wet?

- *Geef voor uw departement aan welke organisatie of organisatieonderdeel toezicht houdt op de naleving van de Wet GDI (ihbz de artt. 5,8 en 16).*

Het toezicht op UWV en SVB is beperkt, en vooral vormgegeven in de P&C-cyclus. Het lijkt ons daarom niet de bedoeling dat de Inspectie SZW werkelijk toezicht gaat houden op de naleving van de artikelen 5, 8 en 16 van de Wet. Het lijkt meer voor de hand te liggen dat SVB en UWV hier in hun P&C-cyclus aandacht aan besteden en verantwoording over afleggen.

b. Wat is het oordeel van de toezichthoudende organisaties (of organisatieonderdelen) over de uitvoerbaarheid en handhaafbaarheid?

- *Geef daarbij ook aan of er taken of verplichtingen zijn die voor een correcte uitvoering c.q. naleving verduidelijking behoeven.*
- *Geef aan of de toezichthoudende organisatie of organisatieonderdeel over voldoende kennis en/of capaciteit beschikt.*
- *Geef aan wat de kosten van toezicht en handhaving zijn. Geef verder aan waarop deze inschatting is gebaseerd en of de kosten als proportioneel kunnen worden beschouwd.*

Gelet op voorgaande verwachten wij geen kosten voor het toezicht. Dit betekent overigens wel dat eventuele informatie ten behoeve van een evaluatie of andere inschatting van de effectiviteit op een andere wijze verkregen moet worden.