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: Zorggroep Alliade
[redacted]

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

- *N.v.t. voor Alliade*

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

- *Als zorggroep zullen we digitale toegang voor externen tot onze diensten moeten faciliteren via erkende publieke en private authenticatiemiddelen op betrouwbaarheidsniveau substantieel en hoog. Hierbij is het vooral van belang dat er een acceptatieplicht geldt (we zullen alle erkende middelen moeten accepteren). Deze taak is helder, echter alle gevolgen nog niet te overzien.*

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

- *Wij zullen dit niet zelfstandig uit kunnen voeren – hiervoor is specialistische kennis en expertise benodigd. Dit zal in nog grotere mate gelden voor kleinere zorgorganisaties – in die zin is Alliade nog in staat een heleboel zelf te regelen. Het heeft uiteraard invloed op de prioriteitstelling – wanneer dit een 'must-do' wordt zal dit ten koste gaan van andere initiatieven. Aan de andere kant juichen wij een gestandaardiseerde, veilige en uniforme wijze van toegang voor alle externe partijen toe.*
- *Van groot belang is de acceptatieplicht in combinatie met de multimiddelenaanpak. Dit betekent dat alle aangewezen organisaties alle erkende middelen zullen moeten accepteren. Wanneer er zeer veel erkende middelen komen en wij zaken moeten doen met alle verschillende partijen die deze middelen leveren ontstaat een onwerkbare situatie. Het is dus zaak dat wij slechts met 1 ontsluitende dienst te maken krijgen, die vervolgens ervoor zorgt dat alle erkende authenticatiediensten aangesloten worden. Op dit moment staat in de tekst*

*dat ontsluitende diensten **niet** de verplichting krijgen tot ontsluiting van alle erkende middelen. I.c.m. de acceptatieplicht is dat een zeer onwenselijke situatie.*
- *Op dit moment is onvoldoende helder wat de uitvoering van automatisering vraagt. Welke gegevens moeten in welk formaat uitgewisseld worden? Wat betekent invoering voor de reeds in gebruik zijnde authenticatiemiddelen, kunnen de nieuwe diensten bijvoorbeeld bestaande Microsoft B2C inlogmethodes vervangen? Dit is nieuw terrein voor Alliade.*

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

- *Verwacht effect is dat het voor onze cliënten, verwanten en andere externe partijen eenvoudiger en eenduidiger wordt om in te loggen bij Alliade en diensten af te nemen. Wanneer burgers altijd dezelfde authenticatiedienst kunnen gebruiken om bij zowel overheid als zorgverzekeraars en zorgorganisaties in te loggen is dat beter dan een versnipperde situatie.*
- *Het effect van de wet voor Alliade zal zijn dat we ingericht moeten zijn om de implementatie en beheer van de nieuwe wijze van authenticatie, waarbij wij ervan uitgaan dat we uiteindelijk met 1 ontsluitende dienst te maken krijgen. We zullen expertise op moeten bouwen of aan moeten nemen op dit gebied en onze ondersteunende diensten (o.a. helpdesk) zal ingericht moeten zijn om vragen rondom inloggen via alle verschillende authenticatiediensten te kunnen beantwoorden.*
- *De wet heeft impact op alle diensten die wij kunnen leveren. Van toegang tot de zorgdossiers door cliënten/verwanten tot het aanvragen van diensten van de medische dienst.*
- *Neveneffecten kunnen zijn dat reeds bestaande wijze van authenticatie overbodig raken (desinvestering) of slecht samen gaan met de geboden geboden oplossingen. Single Sign On is erg belangrijk voor ons, dus het moet voorkomen worden dat externen naast de inlog via erkende authenticatiediensten nogmaals in moeten loggen in zorgdossiers of anderszins.*

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

- *Alliade maakt op dit moment nog geen gebruik van DigID. Lange tijd was dit niet toegestaan, wat nu juist omdraait naar een verplichting tot gebruik van erkende authenticatiemiddelen. Geen slechte zaak, maar de acceptatieplicht zal voor de meeste zorgorganisaties alleen werkbaar zijn wanneer er een ontkoppelpunt is via 1 ontsluitende dienst. Wij gaan er vanuit dat erkenning betekent dat er gebruik gemaakt van de geaccordeerde standaarden, dus dat het moeten ondersteunen van verschillende authenticatiediensten op zich werkbaar blijft.*
- *Wanneer er een verschillende tariefstructuur geldt voor de diverse authenticatiediensten is het van belang waar de kosten vallen. Wij willen dat er voor onze cliënten/verwanten in ieder geval de keuze is om een gratis, veilige (erkende) authenticatiedienst te gebruiken. Wanneer zij kiezen voor een andere dienst waarvoor kosten verschuldigd zijn, is dat hun keuze. Wanneer iedere aangeboden dienst kosten voor de externe partij met zich meebrengt hebben we daar moeite mee en zouden we dit in ieder geval als organisatie willen kunnen afkopen o.i.d. Alliade wil daarnaast geen administratieve last van het doorbelasten van kosten naar de externe partijen.*

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

- *Op basis van de huidige informatie is dit koffiedik kijken. Een beschikbare referentie betreft de implementatie van DigID bij een collega zorginstelling, welke rond de 50K gekost zou hebben. Dit betreft derhalve de eenmalige kosten voor de implementatie van 1 authenticatiedienst.*
- *Dergelijke kosten voor ontsluiting van alle erkende authenticatiediensten via 1 ontsluitende dienst worden voor onze organisatie wel proportioneel geacht. Wanneer dergelijke kosten voor iedere erkende dienst betaald moeten worden (acceptatieplicht!) wordt het disproportioneel.*
- *Andere kosten kunnen betreffen het laten functioneren van de oplossingen met het applicatielandschap van Alliade (bijv. ondersteuningsplannen en medische dossiers) en desinvesteringen op bestaande oplossingen.*
- *Structurele kosten betreffen het beheer van de oplossing en de uitbreiding aan support die wij zullen moeten geven aan de externe partijen.*

2. Handhaafbaarheid

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

- *N.v.t. voor Alliade*

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

- *Toezicht betreft m.i. met name toezicht vanuit de optiek van privacy en informatiebeveiliging. De uitvoerbaarheid van de wet valt of staat daarbij met de kwaliteit van het proces rondom erkenning van authenticatiediensten. Wanneer er vooraf voldoende zekerheid is dat er op juiste wijze omgegaan wordt met persoonlijke data, dan zal de handhaafbaarheid voldoende zijn. Is daar twijfel over en kan veiligheid niet voldoende duidelijk gemaakt worden aan de externe partijen, dan zal uitvoerbaarheid en handhaafbaarheid een groter probleem vormen.*
- *Wat nog te onduidelijk is waar de verantwoordelijkheden liggen voor het functioneren van de diensten. Op het moment dat een dienst niet functioneert, zal de leverancier van de dienst daarop aangesproken moeten worden, maar de cliënt/verwant zal dit via ons als zorginstelling doen aangezien zij klant zijn bij ons. Dit proces behoeft detaillering.*
- *Alliade heeft kennis beschikbaar binnen functies CISO (Concern Information Security Officer) en DPO (Data Protection Officer). Technische kennis en expertise is minder voor handen op dit nieuwe gebied rondom eID.*