(91)

Zorginstituut Nederland

Ministerie van VWS

[redacted]

Zorginstituut Nederland
Informatiemanagement
Databeheer, Informatiebeleid
& Architectuur

Eekholt 4
1112 XH Diemen
Postbus 320
1110 AH Diemen
www.zorginstituutnederland.nl
info@zinl.nl

[redacted]

memo

Consultatie Wet Generieke Digitale Infrastructuur en Uniforme Set van Eisen eID

Datum
28 februari 2017

Onze referentie
2017007179

[redacted]

Hierbij treft u de reactie aan van Zorginstituut Nederland (hierna: het Zorginstituut) op het concept wetsvoorstel voor de Wet Generieke Digitale Infrastructuur (hierna WGDI).

Wij hebben er voor gekozen het format van uw memo van 20 januari 2017 te hanteren voor het geven van onze reactie. In bijlage 1 hebben wij de door u geformuleerde vragen zo goed mogelijk trachten te beantwoorden. Verder hebben wij de door u opgestelde samenvatting van de WGDI toegevoegd in bijlage 2. Waar nodig verwijzen wij bij de beantwoording naar die bijlage.

Verder is van belang te vermelden dat wij er voor hebben gekozen de WGDI vooral te beschouwen vanuit het perspectief van het Zorginstituut als bestuursorgaan, dus als adressant van de verplichtingen. Hoewel wij vanuit onze taken op diverse terreinen[1] ook belang hebben bij de vraag wat de WGDI betekent voor andere partijen in het zorgdomein hebben we er vooralsnog van af gezien ons in die aspecten te verdiepen. De belangrijkste reden daarvoor is dat al deze partijen ook zelf hun zienswijze naar voren kunnen brengen in de consultatie.

Voordat we ingaan op uw vragen willen we enkele opmerkingen van meer algemene aard maken:

a) Wij vinden dat het zorgdomein groot belang heeft bij een goed werkende, veilige authenticatie op een hoger betrouwbaarheidsniveau dan het huidige DigiD. Verankering in de WGDI kan zorgen voor zekerheid, duidelijkheid en een gelijk speelveld waar het gaat om de te hanteren authenticatiemiddelen. Dat zal volgens ons grote en positieve effecten kunnen hebben in de zorg, zowel in de zorgverlening in engere zin als in

[1] Denk bijvoorbeeld aan onze taak als ketenregisseur in de informatievoorziening langdurige zorg en aan onze taken op het gebied van de kwaliteit van zorg.

Zorginstituut Nederland
Informatiemanagement
Databeheer, Informatiebeleid
& Architectuur

Datum
28 februari 2017

Onze referentie
2017007179

allerhande ondersteunende en administratieve processen. Wij verwachten kansen op efficiencywinst en een stimulans voor innovatie van dienstverlening.
Ook de gedachte achter een multimiddelenaanpak (vermindering kwetsbaarheid) vinden wij goed en waardevol.

b) Dit gezegd hebbende. Wij hebben na bestudering van de wettekst en MvT (in het korte tijdsbestek dat wij daarvoor hadden) nog veel vragen en onzekerheden.

Het Zorginstituut is een 'kleine dienstverlener' waar het gaat om dienstverlening waarvoor authenticatie noodzakelijk is. Desalniettemin voorzien wij dat wij vanwege de acceptatieplicht een behoorlijke inspanning met mogelijk forse kosten moeten leveren. Het beeld dat we met meerdere partijen moeten contracteren om alle erkende middelen te kunnen faciliteren roept bij ons bepaald niet het beeld van 'ontzorging' op.

Ook is voor ons niet duidelijk hoe de multimiddelenaanpak van de grond gaat komen: hoe wordt gewaarborgd dat er bij de inwerkingtreding van de wet een voldoende aanbod van authenticatiemiddelen en toegangsdienstverleners is om daadwerkelijk van een multimiddelenaanpak en van een werkende markt te kunnen spreken? Als er bij inwerkingtreding maar één of twee middelen beschikbaar zijn dan zal de markt over dat aanbod verdeeld worden. Voor nieuwkomers die na de inwerkingtreding de markt willen betreden zal het dan niet eenvoudig zijn een positie te verwerven.

Het wetsvoorstel is niet coherent qua toepassingsbereik en doelgroepen. De verplichting om bepaalde standaarden te hanteren richt zich op een andere doelgroep dan de verplichtingen rond authenticatie.
Daarnaast maakt het feit dat erg veel onderwerpen nog bij lagere regelgeving geregeld gaan worden het moeilijk om de gevolgen voor onze organisatie (en voor andere partijen in het zorgdomein) goed in te schatten.

Wij sturen onze reactie vooralsnog niet rechtstreeks aan het Ministerie van Binnenlandse Zaken. We gaan er van uit dat u onze reactie op zorgvuldige wijze met de reacties van andere partijen in de zorg zult bundelen tot een gezamenlijke reactie die recht doet aan de impact van de WGDI op het zorgdomein.

Hoogachtend,

Zorginstituut Nederland
Informatiemanagement
Databeheer, Informatiebeleid
& Architectuur

Datum
28 februari 2017

Onze referentie
2017007179

Bijlage 1

1 Te beantwoorden vragen

1.1 Vragen vanuit BZK

1. *Welke (categorieën van) BSN-gerechtigde organisaties zouden, gelet op de aard van hun dienstverlening, moeten worden aangewezen, opdat ze - evenals bestuursorganen in de zin van art. 1:1, eerste lid, onder a, Awb - binnen de werkingssfeer van het wetsvoorstel komen te vallen?*

   Gezien de aard van de binnen het zorgdomein verwerkte gegevens lijkt het ons logisch dat behalve de bestuursorganen ook de zorgaanbieders en zorgverzekeraars binnen de werkingssfeer van het wetsvoorstel komen te vallen.
   Wij onderschrijven dan ook uw conclusie (bijlage 2, onderdeel 2.2.) dat organisaties die op dit moment onder de *Wet BSN in de Zorg* vallen ook onder de WGDI dienen te vallen en dus op aangeven van de eigen Minister opgenomen moeten worden in de bijlage van de WGDI.

2. *De betekenis en gevolgen van de acceptatieplicht, mede in relatie tot interoperabiliteit, tarifering en de uitfasering van DigiD-laag/basis en de ambitie om bestuursorganen zo eenvoudig mogelijk aan te kunnen laten sluiten op de verschillende erkende authenticatiemiddelen.*

   De impact van de verplichting om authenticatie op niveau substantieel of hoog te kunnen faciliteren zal voor Zorginstituut Nederland naar verwachting *op korte termijn* beperkt zijn. Wij maken op dit moment geen gebruik van DigiD voor dienstverlening, aangezien we geen elektronische diensten aan burgers verlenen waarvoor (veilige en betrouwbare) authenticatie noodzakelijk is.
   Bij deze inschatting (op korte termijn geen of weinig impact) gaan wij er ook van uit dat wij geen acties hoeven uit te voeren voor de communicatie met bedrijven/rechtspersonen (betreft onder andere processen als subsidieverlening, gegevensleveringen zorgaanbieders aan kwaliteitsregister, levering dossiers farmaceutische bedrijven in het kader van geneesmiddelenbeoordeling). Wij maken voor deze communicatie nu al gebruik van e-Herkenningsmiddelen, en die zullen, aldus de MvT (onderdeel 4.7), worden aangewezen als erkende middelen op grond van de WGDI.

   Op langere termijn voorzien wij wél een betekenisvolle impact. Wij zullen na inwerkingtreding van de WGDI mogelijk op termijn toch gehouden zijn om voor de communicatie met burgers de authenticatiemiddelen op niveau substantieel en hoog te faciliteren.
   In het wetsvoorstel (artikel 23, vierde lid) wordt aangegeven dat DigiD laag en midden binnen 3 jaar na inwerkingtreding van de WGDI zullen worden uitgefaseerd. Publieke authenticatiemiddelen zijn er dan alleen nog op niveau substantieel en hoog[2]. Dat zou voor het Zorginstituut betekenen dat, daar waar een burger gebruik maakt van zijn wettelijk recht om digitaal te

[2] NB Wij missen op dit punt een heldere uitleg over de ratio van het uitfaseren van DigiD laag en midden: is de aanname dat na inwerkingtreding iedere burger in beginsel een authenticatiemiddel op niveau substantieel of hoog heeft en DigiD laag/midden dus simpelweg niet meer nodig is?

Zorginstituut Nederland
Informatiemanagement
Databeheer, Informatiebeleid
& Architectuur

Datum
28 februari 2017

Onze referentie
2017007179

communiceren met een bestuursorgaan, en er authenticatie nodig is (bijvoorbeeld omdat verstrekking van persoonsgegevens of bedrijfsgevoelige informatie aan de orde kan zijn), de toepassing van de middelen op niveau substantieel en hoog de enige optie is.

3. *De onderwerpen die in de uitvoeringsregelgeving zullen worden geregeld en de daarbij te betrekken overwegingen.*

   Zie de algemene opmerking hierover in onderdeel b van de brief.

Vragen vanuit VWS

1.2 Algemeen
Toepassing: bestuursorganen en aangewezen organisaties

4. *Wat vindt u van de begrijpbaarheid van de wetsteksten en de toelichtingen?*

   Authenticatie bij digitale dienstverlening is geen eenvoudige materie. Wij begrijpen ook dat wetteksten en toelichtingen noodzakelijkerwijs een relatief hoog abstractieniveau moeten hebben.
   Tegelijkertijd is bij het onderwerp digitale communicatie, met name in de zorg, vertrouwen het kernbegrip. Burgers moeten er op kunnen vertrouwen dat hun gegevens veilig zijn en blijven. Als de oplossingen die worden ingezet om die veiligheid te bereiken alleen voor technisch specialisten te begrijpen zijn is dat nadelig voor het vertrouwen en het draagvlak bij de burgers.
   Wij vinden vanuit deze optiek de toelichting voor verbetering vatbaar: een concretere uitleg over de verschillen tussen de betrouwbaarheidsniveau's laag, midden, substantieel en hoog is wenselijk: wat zit er achter die betrouwbaarheidsniveau's? Moet ik als burger naar de notaris voor niveau hoog? Ook een praktische beschrijving van het authenticatieproces vanuit het perspectief van de burger zou helpen: hoe werkt dat als je inlogt met DigiD laag, of met een middel op niveau hoog?

   Een wetstechnische opmerking: het begrip gebruiker is niet gedefinieerd, maar komt terug in de definitiebepaling (artikel 1). Uit de MvT blijkt dat hiermee de burger is bedoeld, in de zin van burgers en bedrijven. Het zou helder zijn als de wet dit begrip ook definieert dan wel in plaats van het begrip gebruiker de terminologie burgers of bedrijven wordt toegepast. Het begrip gebruiker is nu te abstract en kan nu ook op andere partijen in de keten slaan. Opgemerkt zij dat in artikel 18 wel het begrip burger wordt gebruikt. Dat is dus de gebruiker uit de definitiebepaling in artikel 1 en daaronder vallen dus ook bedrijven?

5. *Welke informatiebehoefte heeft u?*

   Zie het antwoord op vraag 4. Verder hebben wij vooral behoefte aan informatie over de criteria op grond waarvan de indeling naar betrouwbaarheidsniveau moet plaatsvinden en aan informatie over de kosten waarmee wij rekening moeten houden.

6. *Welke informatiebehoefte verwacht u dat uw cliënten gaan hebben?*

Zorginstituut Nederland
Informatiemanagement
Databeheer, Informatiebeleid
& Architectuur

Datum
28 februari 2017

Onze referentie
2017007179

n.v.t. (zie antwoord op vraag 2)

1.3 Standaards (voor alle bestuursorganen)
Toepassing: bestuursorganen

7. *Waaraan dient een zorgvuldig en transparant proces (Bijlage 2, punt 4) te voldoen?*

   Geen opmerkingen

8. *Hoe ziet u de relatie tussen de binnen uw sector van toepassing zijnde standaards (Bijlage 2, punt 6) en de voor de eerste tranche voorgenomen standaards (Bijlage 2, punt 7)?*

   Zie antwoord op vraag 9.

9. *Wat zijn de te verwachten effecten van het verplicht stellen van de standaarden (Bijlage 2, punt 7). Is de uitvoering hierop voldoende toegerust?*

   De impact van het verplicht stellen van de genoemde standaarden voor de toegankelijkheid van websites en voor de informatiebeveiliging zal voor ons naar verwachting beperkt zijn. We voldoen al aan deze standaarden.
   De effecten voor ons als organisatie zijn dus beperkt.
   Toch roept het wetsvoorstel bij ons vragen op:

   -Waarom worden specifiek de in de MvT genoemde standaarden verplicht gesteld, en niet andere standaarden die op de pas-toe-of-leg-uit lijst van het Forum Standaardisatie staan?

   -Hoe wordt voorkomen dat de verplichtstelling bij AMVB leidt tot verstarring? Een verwijzing in de AMVB naar een standaard XYZ, versie 1.2 van datum xx-xx-xxxx kan ertoe leiden dat de ontwikkeling van de uitvoeringspraktijk wordt belemmerd indien een nieuwe versie van de standaard pas na wijziging van de AMVB mag worden toegepast.
   De laatste zin van de artikelsgewijze toelichting bij artikel 2, derde lid wijst in die richting.

   -Specifiek over de standaard toegankelijkheid: een punt dat bij ons zorgt voor onduidelijkheid is de vraag hoe wij moeten omgaan met het vanaf onze website direct linken naar PDF-documenten die zijn gemaakt en worden gehost door derden. Onder de WCAG 2.0 worden deze gezien als webpagina's op onze website, maar in de praktijk kan het daarbij dus heel goed gaan om documenten die zijn gemaakt door partijen die niet onder de werkingssfeer van de WGDI vallen[3], zoals bijvoorbeeld (koepels van) zorgverleners. Wat moeten we dan doen: deze verwijzingen verwijderen en daarmee mensen informatie onthouden (bijvoorbeeld patiëntversies van medische richtlijnen)? Of de richtlijn overtreden, en wel verwijzen naar deze documenten? En wat is in dat laatste geval dan de sanctie?

[3] Als wij het goed zien vallen de zorgaanbieders, met uitzondering van de academische ziekenhuizen, niet onder de reikwijdte van artikel 2.

Zorginstituut Nederland
Informatiemanagement
Databeheer, Informatiebeleid
& Architectuur

Datum
28 februari 2017

Onze referentie
2017007179

-Informatiebeveiliging: verplichtstelling van de genoemde standaarden is volgens ons strijdig met de algemene notie in de Baseline Informatiebeveiliging Rijk en met de NEN/ISO-27001 en 27002 dat maatregelen worden genomen op basis van risicoprofielen. Verplichtstelling bij AMVB kan er aan bijdragen dat de nadruk komt te liggen op naleving van de regels (compliance) in plaats van op het voorkomen van informatiebeveiligingsrisico's.

-In het algemene deel van de MvT wordt (pag 11) gesteld dat een standaard die bij AMVB verplicht gesteld wordt van de pas-toe-of-leg-uit lijst zal worden afgevoerd. De artikelsgewijze toelichting bij artikel 2, derde lid (pag 56) lijkt echter te suggereren dat een standaard zowel in een AMVB als op de pas-toe-of-leg-uit lijst kan voorkomen. Dat is verwarrend.

1.4 Toegang tot elektronische dienstverlening
Toepassing: bestuursorganen en aangewezen organisaties

10. *De verplichte aansluiting (reikwijdte wet) geldt niet alleen voor bestuursorganen, maar ook voor daartoe aangewezen private organisaties. (Bijlage 2, punt 8). Welke gevolgen en effecten schat u in?*
11. *Om welke organisaties zou dit wat u betreft gaan?*
12. *Is de uitvoering hier voldoende op toegerust? Welke consequenties ziet u voor uw organisatie en veld?*

We hebben er zoals aangegeven voor gekozen om de WGDI voor nu vooral te bezien vanuit ons eigen organisatieperspectief. We gaan er van uit dat de betreffende private organisaties zelf prima in staat zijn een reactie op bovenstaande vragen te geven. Zie ook de voetnoot in de brief.

1.5 Werking, betrouwbaarheid en beveiliging
Toepassing: bestuursorganen en aangewezen organisaties

13. *Bijlage 2, punt 13 opent de mogelijkheid dat ook private aangewezen organisaties regels opgelegd krijgen met betrekking tot de werking, betrouwbaarheid en beveiliging van hun dienstverlening.*
    - *Hoe interpreteert u de wet op dit punt?*
    - *Heeft dit betrekking op de periodieke IB-audits?*
    - *Hoe verhoudt dit zich met de huidige regels rondom het gebruik van DigiD?*

    Zie ons antwoord bij onderdeel 1.4.

14. *Wat is de mogelijke invloed van dit punt op uw organisatie?*
    In Bijlage 2, punt 14 wordt aangegeven dat ontsluitende diensten ***niet*** *de verplichting krijgen tot het ontsluiten van alle erkende middelen (Bijlage 2, punt 11). Voor de dienstverleners bestaat er echter wel de acceptatieplicht voor alle erkende middelen. Dit betekent dus dat uw organisatie met meerdere contractpartijen (ontsluitende diensten) te maken gaat krijgen. Wat voor impact zal dit op uw organisatie hebben? Is de uitvoering voldoende toegerust op een dergelijke acceptatieplicht? Wat zijn eventuele effecten en consequenties voor uw organisatie?*

Zorginstituut Nederland is, waar het gaat om elektronische dienstverlening aan burgers en bedrijven, een 'kleine dienstverlener'. Dat zal waarschijnlijk ook zo blijven. Het is daarom voor ons zeer van belang dat wij in staat worden gesteld om op zo eenvoudig mogelijke wijze aan de acceptatieverplichting kunnen voldoen. Contracteren met meerdere ontsluitende diensten, om het palet compleet te kunnen krijgen, past daar beslist niet bij.
Wij vinden het zeer wenselijk dat tegenover onze verplichting alle erkende middelen te accepteren een verplichting voor de ontsluitende diensten staat om alle erkende middelen te faciliteren.
Wij denken dat we in het zorgdomein niet de enige partij zijn waarvoor dit een belangrijk punt is.

1.6 Financieel
Toepassing: bestuursorganen en aangewezen organisaties

15. *Er wordt vanuit gegaan dat de in Bijlage 2, punt 1 genoemde lasten lager zullen zijn dan de baten die gegenereerd worden. Het gebruik van een generieke, betrouwbare infrastructuur zou door een toename in digitale ontsluiting en lagere risico's door hogere betrouwbaarheid baten genereren.*

    - *Heeft een u een inschatting van de mogelijke aansluitkosten?*

      Nee

    - *Heeft u een inschatting van de mogelijke doorlopende kosten voor de ontsluitende diensten?*

      Nee

    - *Onderschrijft u de aanname dat de baten die gegenereerd worden opwegen tegen bovengenoemde lasten?*

      Gelet op de antwoorden op de vorige twee vragen: wij zien niet in hoe wij die aanname (die in de MvT ook niet verder wordt onderbouwd) vanuit het perspectief van onze organisatie zouden kunnen onderschrijven. Wellicht zal er binnen het totale stelsel wel sprake kunnen zijn van efficiencyvoordelen, maar voor ons is volstrekt onduidelijk hoe groot die voordelen zouden kunnen zijn, en waar ze neerslaan. Wat wel duidelijk is is dat voor ons als organisatie de kosten-batenbalans hoogstwaarschijnlijk negatief zal zijn. Ons beeld is dat we, terwijl we nota bene nu geen dienstverlening aanbieden waarvoor authenticatie vereist is, na inwerkingtreding van de WGDI als organisatie te maken krijgen met extra kosten (waarvan de hoogte onbekend is). Baten zien wij vooralsnog niet voor onze organisatie.

16. *Publieke dienstverleners hebben de mogelijkheid de door ontsluitende diensten doorberekende kosten te verhalen op de gebruikers.*
    - *Heeft u de mogelijkheid op eenvoudige wijze deze lasten door te belasten aan de gebruiker?*

      Nee, bij het Zorginstituut zal vooralsnog geen sprake zijn van structurele,

substantiële digitale dienstverlening aan burgers. Hooguit zullen we ten behoeve van incidentele gevallen gehouden zijn authenticatie te faciliteren.
Wij zien geen mogelijkheid om in die situaties de kosten te verhalen op de gebruikers.

- *Vraagt deze doorbelasting veel van uw administratieve proces?*

  n.v.t.

17. *Omdat de overheid een level-playing field tussen alle erkende authenticatiemiddelen wil én een acceptatieplicht instelt, is de onderhandelingsvrijheid voor het maken van prijsafspraken met dienstverleners beperkt.*
    - *Verwacht u veel administratieve last en kosten voor de totstandkoming van prijsafspraken met ontsluitende diensten?*
    - *Wat is uw visie op de mogelijke bepaling van vaste tarieven of maximum tarieven?*

    Hier kan Zorginstituut Nederland op dit moment geen uitspraak over doen.

1.7 Vragen naar aanleiding van de Uniforme Set van Eisen Toepassing: bestuursorganen en aangewezen organisaties

De Uniforme Set van Eisen zijn eisen waaraan aanbieders van erkende elektronische authenticatiemiddelen moeten voldoen. Uw organisatie zal, afhankelijk van uw doelstelling, waarschijnlijk niet zelf hoeven voldoen aan deze eisen. Desondanks hebben deze eisen wel invloed op waar uw organisatie en uw cliënten mee te maken gaan krijgen. Hierover gaan de volgende vragen.

16. *De Uniforme Set van Eisen verplichten publieke en private aanbieders van erkende authenticatiemiddelen om een inloghistorie te bewaren en inzichtelijk te maken voor de gebruiker, uw cliënt. Deze historie houdt bij wanneer met een bepaald middel bij welke dienst is ingelogd. Rationale achter deze eis is dat het geven van inzage in het eigen gebruik ook een mogelijk misbruik inzichtelijk kan maken voor de gebruiker. Anderzijds ontstaat door deze eis een verzameling profilerende gegevens van de gebruiker bij de authenticatiedienst.*
    - *Hoe kijkt uw organisatie aan tegen dit privacyvraagstuk?*
    - *Hoe verwacht u dat uw cliënten hiertegen aankijken?*
    - *Verwacht u een verschil in de perceptie hierover wanneer het een publieke authenticatiedienst (DigiD) of private authenticatiedienst betreft?*

    Het begrip Uniforme set van eisen komt maar 1 keer voor in de MvT (p.46). Uit de betreffende passage in de MvT wordt niet duidelijk wat wel uit uw vraagstelling duidelijk wordt. Wellicht dat de MvT een duidelijker omschrijving kan geven wat de Uniforme Set van Eisen is. En dat in de privacyparagraaf daar aandacht aan kan worden besteed. Maar ook p. 18 van de MvT onder inzage register zou hier aandacht aan kunnen worden besteed. Overigens: de beschrijving in de MvT van hetgeen de burger ter inzage krijgt lijkt ons vanuit de huidige privacywetgeving te beperkt.

Vanuit de privacywetgeving is het ook nu al noodzakelijk om een (in)loghistorie op gegevens te bewaren. Betrokkenen hebben het recht om hier inzage in te vragen. Het Zorginstituut heeft niet veel inzageverzoeken ontvangen op basis van de huidige privacywetgeving.
Ten aanzien van de mogelijkheid tot profilering door publieke en private authenticatiediensten geldt dat het noodzakelijk is dat wet- en regelgeving concreet is in het verbod daarop. De komende Algemene Verordening Gegevensbescherming (AVG) geeft hier al abstracte regels voor. Het zou echter goed zijn als deze regels nader geconcretiseerd worden voor authenticatiediensten. Daarbij kunnen dan ook regels worden gesteld over de maximumbewaartermijn van loggegevens. Deze regels kunnen bij de burger voor meer vertrouwen in deze diensten zorgen.

17. *De Uniforme Set van Eisen bevatten geen eisen aan de toegankelijkheid van erkende middelen voor gebruik door mensen met beperkingen. De eerste tranche van de wGDI zal naar verwachting wel eisen aan de toegankelijkheid van websites stellen (zie de sectie over Standaarden).*
    - *Verwacht u dat publieke en private leveranciers van authenticatiemiddelen uit eigen beweging tegen redelijk kosten middelen zullen ontwikkelen die ook bruikbaar zijn voor mensen met beperkingen?*

      Hier kan het Zorginstituut nu geen uitspraak over doen.

18. *De Uniforme Set van Eisen bevatten eisen over de technische koppeling tussen uw organisatie (als dienstverlener) en de ontsluitende diensten[4]. Deze eisen en specificaties zijn beschreven van pagina's 60 tot 72.*
    - *Zijn de eisen en specificaties op dit punt voldoende duidelijk voor u en uw leverancier(s) om op basis hiervan de technische koppelingen te realiseren?*
    - *Zo nee, welke aanvullende ondersteuning heeft u en/of uw leverancier nodig?*
    - *De technische koppeling kan per ontsluitende dienst verschillen. Aangezien een acceptatieplicht beoogd wordt, betekent dit dat uw organisatie naar verwachting meerdere technische koppelingen moet implementeren. Welke belasting vraagt dit van uw organisatie?*

      Hier kan het Zorginstituut nu geen uitspraak over doen.

1.8 Tot slot

19. *Wat zijn eventueel andere overwegingen of opmerkingen die u over de Wgdi of de Uniforme Set van Eisen nog wilt meegeven?*

    Geen opmerkingen.

[4] Ontsluitende diensten heten Toegangsdiensten in de Uniforme Set van Eisen (pp 19).

Zorginstituut Nederland
Informatiemanagement
Databeheer, Informatiebeleid
& Architectuur

Datum
28 februari 2017

Onze referentie
2017007179

Bijlage 2

2 Samenvatting Wet Generieke Digitale Infrastructuur

2.1 Algemeen

De wetstekst zelf omvat 10 pagina's, de memorie van toelichting (inclusief de artikelsgewijze toelichting) bedraagt in totaal 78 pagina's. BZK heeft een oplegbrief ter begeleiding van de consultatie opgesteld met een korte samenvatting van de wet en een aantal te beantwoorden vragen.

De opzet van de wet is vergeleken met de oorspronkelijke intentie hiervan sterk aangepast: BZK en EZ hebben besloten voor de eerste tranche van de wet alleen de onderdelen *standaards* en *authenticatie en identificatie* op te nemen.

2.2 Reikwijdte van de wet

Artikel 3 geeft aan dat de volgende organisaties onder onderdelen van de wet vallen:

- **Bestuursorganen**;
- Bij besluit **aangewezen organisaties**.
  Aangewezen organisaties zijn door de Minister aan te wijzen categorieën van organisaties die krachtens wettelijk voorschrift gerechtigd zijn het burgerservicenummer te gebruiken en elektronische diensten verlenen waarvoor veilige en betrouwbare authenticatie noodzakelijk is.
  Aangewezen organisaties worden in de bijlage van de wet opgenomen.

Artikel 3 lid 4 geeft aan dat aangewezen organisaties die gebruik maken van het burgerservice nummer eveneens aangewezen kunnen worden voor toepassing van de artikelen in de hoofdstukken 2 tot en met 6.

Onze interpretatie hiervan is als volgt:

- Organisaties die niet conform de Wgdi zijn aangewezen vallen vanzelfsprekend niet onder de wet *en kunnen daarom in de toekomst geen gebruik maken van de nieuwe substantieel en hoog beveiligde middelen*;
- Indien men nu via de Wet BSN in de Zorg gebruik maakt van de huidige publieke authenticatie en identificatiemiddelen (DigiD) en in de toekomst van de nieuwe publieke middelen gebruik wenst te maken dan kan dat alleen als aangewezen organisatie;

Onze conclusie is dat organisaties die op dit moment onder de *Wet BSN in de Zorg* vallen ook onder de Wgdi dienen te vallen en dus op aangeven van de eigen Minister opgenomen moeten worden in de bijlage van de Wgdi.

2.3 Standaarden (artikel 2)

1. Het onderwerp standaarden is alleen van toepassing voor alle **bestuursorganen** en niet voor aangewezen organisatie;
2. Het gaat specifiek om *open standaarden* van de *pas toe – leg uit*[5] lijst;

[5] https://www.forumstandaardisatie.nl/lijst-open-standaarden

3. Via een *Algemene Maatregel van Bestuur* (AMvB) kan een standaard verplicht gesteld worden indien dit noodzakelijk en proportioneel is voor werking en betrouwbaarheid van de dienstverlening;
4. Opname geschiedt via een zorgvuldig en transparant proces;
5. Zodra een standaard via een AMvB verplicht is wordt deze van de *pas toe – leg uit lijst* afgevoerd.
6. Sectorale standaarden mogen niet belemmerend of concurrerend werken in het bovensectorale verkeer;
7. Voor de 1ste tranche van de wet verwacht men de volgende standaarden verplicht te stellen:
    - **Toegankelijkheid** websites. Men is van plan de Europese toegankelijkheidstandaard ETSI EN 301 549 aan te wijzen als een verplicht toe te passen standaard. Hiermee wordt Webrichtlijnen versie 2.0 van de pas toe leg uit lijst afgehaald;
    - **Informatieveiligheid**: De veiligheidsstandaarden TLS 1.2, DNSSEC, DKIM, SPF en Digikoppeling 2.0, komen in aanmerking om bij algemene maatregel van bestuur te worden verplicht.

2.4 Toegang tot elektronische dienstverlening (artikelen 3 t/m 6)

8. De verplichte aansluiting geldt zowel voor de **bestuursorganen** en de **aangewezen organisaties** die elektronische diensten verlenen aan burgers of ondernemers waarvoor een veilige en betrouwbare authenticatie essentieel is. In praktijk komt dit voor het zorgdomein neer op alle organisaties die op dit moment eveneens onder de wet *BSN in de Zorg* vallen;
9. Onder de wet gaan vallen middelen met beveiliging *substantieel* en *hoog* (eID). Het huidige DigiD met beveiliging laag (gebruikersnaam en wachtwoord) en midden (gebruikersnaam en wachtwoord plus SMS) valt niet onder de Wgdi;
10. Er wordt een termijn van 3 jaar na inwerkingtreding van de wet gehanteerd voor het uitfaseren van DigiD laag en midden. De beoogde inwerkingtreding van de wet is 1 januari 2019;
11. Er is sprake van een multimiddelen strategie. Er is een *acceptatieplicht* voor dienstverleners van erkende authenticatie en identificatiemiddelen. Dit geldt ook voor Europees erkende middelen (eIDAS). Dit betekent dat een dienstverlener ervoor dient te zorgen dat hij alle erkende middelen aankan;
12. Het publieke middel mag alleen in het publieke (overheids) domein gebruikt worden;

2.5 Werking, betrouwbaarheid en beveiliging (artikelen 7 t/m 9)

13. Artikel 8 biedt de grondslag voor vaststelling van regels over de *werking*, *betrouwbaarheid* en *beveiliging* van de toegang tot elektronische diensten door *bestuursorganen* en *aangewezen organisaties*;
14. Het is vooralsnog niet de verwachting dat *ontsluitende diensten*[6] ieder erkend middel van iedere erkende authenticatiedienst zullen ontsluiten.
15. Er is een verplichting voor bestuursorganen en aangewezen organisaties om jaarlijks een verklaring van een onafhankelijke auditor over te leggen aan de

[6] Ontsluitende dienst: partij die het elektronisch verkeer tussen een bestuursorgaan of aangewezen organisatie en erkende authenticatiediensten, machtigingsdiensten en attributendiensten routeert teneinde toegang tot elektronische dienstverlening te faciliteren. N.B.: de Uniforme Set van Eisen hanteert hiervoor de term "Toegangsdienst". Ontsluitende dienst en toegangsdienst beschouwt VWS als hetzelfde.

minister.

2.6 Toezicht en handhaving (artikelen 10 t/m 16)

16. De betrokken minister kan toezichthouders aanwijzen voor de naleving van de krachtens deze wet gestelde regels door bestuursorganen op het niveau van de Rijksoverheid (ministeries en zelfstandige bestuursorganen) en door de aangewezen organisaties;
17. Bestuursorganen en aangewezen organisaties, erkende authenticatiediensten, erkende machtigingsdiensten, erkende attributendiensten en erkende ontsluitende diensten verstrekken aan Onze Minister desgevraagd de gegevens en inlichtingen die hij nodig heeft om maatregelen te kunnen nemen om compromittering van de veilige en betrouwbare toegang tot elektronische dienstverlening te voorkomen of beëindigen;

2.7 Financiële bepalingen (artikelen 17 t/m 21)

18. Voor de financiering van het voorgestelde eID-stelsel, zoals ook neergelegd in dit wetvoorstel, gelden de volgende uitgangspunten:
    1. Publieke dienstverleners betalen voor:
        - de aanpassing van hun eigen, interne ICT-infrastructuur,
        - de diensten van de ontsluitende diensten (en daarmee ook voor de diensten van de overige erkende diensten, via deze ontsluitende diensten);
    2. Gebruikers (burgers en bedrijven) kunnen kosten voor de aanschaf van een middel in rekening gebracht worden. Dat gebeurt in ieder geval voor de kosten van het e-rijbewijs en e-NIK;
    3. De kosten van de instandhouding van de generieke voorziening, het BSN-K, en van het publiekrechtelijke verankerde stelsel van toezicht op erkende partijen worden door het Rijk gedragen, maar kunnen door het Rijk doorberekend worden. Voor de inwerkingtreding van de wet wordt (bij algemene maatregel van bestuur) bepaald of en in hoeverre (een gedeelte van) deze kosten ook daadwerkelijk doorberekend worden;
    4. Van de rechtspersonen die een aanvraag tot erkenning van hun ontsluitende diensten en middelen doen zal in beginsel door het Rijk een vergoeding voor de kosten van de afwikkeling van de aanvraag gevraagd worden;

De ontwikkelingen binnen het stelsel en de verdere uitwerking van mogelijke doorbelasting zorgen ervoor dat veel nog niet is uitgewerkt en pas op een later stadium via algemene maatregel van bestuur wordt uitgewerkt. Deze wet creëert de mogelijkheid dit op deze wijze te doen.