VERENIGING VZVZ
ZORGAANBIEDERS VOOR ZORGCOMMUNICATIE

87

Den Haag, 28 februari 2017

Betreft: reactie op Memo Consultatie Wet GDI en Uniforme Set van Eisen eID

Geachte heer, mevrouw,

U hebt ons voorafgaand aan de internet consultatie enkele vragen gesteld in uw Memo Consultatie Wet GDI en Uniforme Set van Eisen eID.
Wij hebben daar waar het mogelijk is uw vragen beantwoord.

Met vriendelijke groet,

[redacted]

VZVZ < Oude Middenweg 55, 2491 AC Den Haag < Postbus 30920, 2500 GX Den Haag <
< www.vzvz.nl < T 070 317 34 00 < E info@vzvz.nl < KvK 54271851 <

vZVZ

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?

Zorgaanbieders, VZVZ en overige organisaties, als (sub)bewerker van persoonsgegevens, die in het kader van de wet BSN gebruik in de zorg het BSN mogen verwerken.

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.

Hier zien we een risico v.w.b. een wildgroei aan koppelvlakken. Idealiter is het koppelvlak, waarmee de ontsluiting met de verschillende erkende authenticatiestelsels geregeld wordt, generiek van aard waardoor we kunnen spreken van één koppelvlak. (Standaardisatie) Het idee van een multi-middelenaanpak op de genoemde betrouwbaarheidsniveaus dragen wij een warm hart toe daar het een aantal fundamentele problemen kan helpen oplossen.

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

??

Algemeen

Toepassing: bestuurorganen en aangewezen organisaties

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

Begrijpelijk

5. Welke informatiebehoefte heeft u?

??

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

Met name duidelijke communicatie, die hen gerust stelt dat de keuze voor een authenticatiemiddel geen gevolgen heeft voor toegang tot overheidsdiensten of diensten van aangewezen organisaties.

Standaards (voor alle bestuursorganen)

Toepassing: bestuurorganen

7. Waaraan dient een zorgvuldig en transparant proces (punt 4) te voldoen?
n.v.t.

8. Hoe ziet u de relatie tussen de binnen uw sector van toepassing zijnde standaards (punt 6) en de voor de eerste tranche voorgenomen standaards (punt 7)?
n.v.t.

9. Wat zijn de te verwachten effecten van het verplicht stellen van de Standaarden (punt 7). Is de uitvoering hierop voldoende toegerust?
n.v.t.

Toegang tot elektronische dienstverlening

Toepassing: bestuurorganen en aangewezen organisaties

10. De verplichte aansluiting (reikwijdte wet) geldt niet alleen voor bestuursorganen, maar ook voor daartoe aangewezen private organisaties. (punt 8). Welke gevolgen en effecten schat u in?

De gevolgen zijn overzichtelijk en te managen echter er is een significante impact. Zorgaanbieders zullen op termijn gebruik moeten maken van erkende middelen op het juiste betrouwbaarheidsniveau. Dit vergt aanpassingen aan zowel centrale infrastructuren, zoals het Landelijk Schakelpunt als aan decentrale infrastructuren, zoals aanwezig bij de individuele zorgaanbieders. Tevens zal de toegang van patiënten, zoals benoemd in de uniforme set van eisen 1.0, tot zowel de centrale als decentrale dienstverlening middels erkende middelen moeten verlopen. Goed geregelde authenticatie en standaardisatie zijn randvoorwaardelijk voor het welslagen

11. Om welke organisaties zou dit wat u betreft gaan?

Zorgaanbieder, VZVZ

12. Is de uitvoering hier voldoende op toegerust? Welke consequenties ziet u voor uw organisatie en veld?

Er zal een significante inspanning moeten worden geleverd. In eerste instantie zullen o.a. patiënten, die toegang willen krijgen tot de eigen medische data via een portaal, moeten worden voorzien van erkende middelen. Hiervoor zullen centrale componenten, zoals het Landelijk Schakelpunt, aanpassing behoeven. In de verdere toekomst zullen zorgverleners i.p.v. een UZI- middel toegang moeten kunnen krijgen tot medische data middels één van de erkende middelen. Dit vergt ook aanpassingen in zowel de decentrale als de centrale infrastructuren.

Werking, betrouwbaarheid en beveiliging

Toepassing: bestuurorganen en aangewezen organisaties

13. 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?

  Om eenzelfde niveau van betrouwbaarheid te kunnen waarborgen is dit noodzakelijk. En de overheid legt geen voorkeursmiddel op aan de burger.

- Heeft dit betrekking op de periodieke IB-audits?

  Ja, met name vanwege de onduidelijkheid of het straks de bedoeling is om per erkend stelsel (DigiD, iDIN, Idensys) een audit te moeten houden. Idealiter komt er een generieke audit.

- Hoe verhoudt dit zich met de huidige regels rondom het gebruik van DigiD?

  In de huidige situatie hebben we te maken met een vergelijkbare maatregel. Impact is niet in te schatten vanwege het feit dat deze pas kenbaar wordt na de totstandkoming van de AMvB.

14. Wat is de mogelijke invloed van dit punt op uw organisatie?
In punt 14 wordt aangegeven dat ontsluitende diensten **niet** de verplichting krijgen tot het ontsluiten van alle erkende middelen (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?
??

Financieel

Toepassing: bestuurorganen en aangewezen organisaties

15. Er wordt vanuit gegaan dat de in 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?
  Ja

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
- Vraagt deze doorbelasting veel van uw administratieve proces?
  Ja

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?

Vragen naar aanleiding van de Uniforme Set van Eisen

Toepassing: bestuurorganen 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?

  Het is belangrijk om hierover volledig transparant te zijn, zodat patiënten bekend zijn met de eventuele risico's en de maatregelen die zijn getroffen om deze risico's te mitigeren. Communicatie is hierbij essentieel. Wij vinden bijvoorbeeld het idee dat financiële instellingen straks inzage zouden kunnen krijgen in de loginformatie van de authenticatie bij een zorgaanbieder. Een gevoelig privacy-onderwerp dat bespreekbaar moet worden gemaakt.

- Hoe verwacht u dat uw cliënten hiertegen aankijken?

  Zolang cliënten en patiënten een geïnformeerde keuze kunnen maken, waarbij ze hun privacy belang kunnen afwegen tegen het gebruiksgemak, voorzien we geen problemen.

- Verwacht u een verschil in de perceptie hierover wanneer het een publieke authenticatiedienst (DigiD) of private authenticatiedienst betreft?

  Ja, DigiD is een bekende en al vertrouwde merknaam. Vertrouwen is in de zorg een belangrijk goed en de verwachting is dat de optie om van DigiD gebruik te kunnen maken zal bijdragen aan de gebruikersacceptatie. Verder is de angst voor misbruik van informatie door de overheid minder dan bij private organisaties.

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?

  Onze verwachting is dat dit in eerste instantie niet gerealiseerd zal worden. Private leveranciers willen eerst een significante business case zien alvorens dit soort functionaliteit te ontwikkelen. Het is geen specifiek issue dat authenticatie

betreft. Het betreft immers een behoefte die een veel breder terrein van diensten in de zorg beslaat.

18. De Uniforme Set van Eisen bevatten eisen over de technische koppeling tussen uw organisatie (als dienstverlener) en de ontsluitende diensten5. 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?
  Ja
- 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?

  In het meest ideale geval wordt het koppelvlak generiek, echter verwachten we geen grote problemen als dit niet zo zal zijn.

Tot slot

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