Memo

62

Nederlandse Zorgautoriteit

Aan
Ministerie van Volksgezondheid, Welzijn en Sport

Van
Nederlandse Zorgautoriteit

Telefoonnummer [redacted]

E-mailadres [redacted]

Kenmerk
-

Onderwerp
Reactie NZa op uitvoeringstoets wetsvoorstel Wgdi

Datum
29 maart 2017

1. Inleiding

Op 22 december 2016 is een openbare internetconsultatie gestart voor de 'Wet Generieke Digitale Infrastructuur (Wgdi). Het doel van deze consultatie is om burgers, bedrijven, en instellingen te informeren over de voorbereiding van de wet en hen gelegenheid te bieden om op het conceptwetsvoorstel te reageren. De Nederlandse Zorgautoriteit (NZa) is een zelfstandig bestuursorgaan en levert digitale dienstverlening aan burgers en bedrijven. Dit betekent dat het voorliggende conceptwetsvoorstel van toepassing zal zijn op onze werkzaamheden. Het CIO Office VWS heeft aangeboden om een op het zorgdomein gerichte uitvoeringstoets richting het ministerie van Binnenlandse Zaken en Koninkrijksrelaties te coördineren. Hiervan maken wij graag gebruik. Via dit memo reageren wij daarom op het wetsvoorstel en de toelichting en de vragen die daarbij vanuit de CIO Office VWS aan ons zijn gesteld.

2. Vragen uitvoeringstoets en reactie NZa

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?
   De Nederlandse Zorgautoriteit (NZa) is een zelfstandig bestuursorgaan. De NZa valt daarmee onder het bereik van de Wgdi. Wij hebben geen oordeel over de vraag welke andere BSN-gerechtigde organisaties onder het bereik van het wetsvoorstel zouden moeten vallen. Met betrekking tot BSN aangewezen organen/organisaties in de zorg zie onze reactie onder vragen 10 en 11.

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.
   Verplichte contractering van een in theorie onbegrensd aantal aanbieders, zoals het wetsvoorstel voorstelt, heeft als risico dat de kosten hiervan op voorhand niet zijn te overzien. Het doel (namelijk het voorkomen van een wildgroei aan authenticatiemiddelen door centraal en bij wet te regelen dat burgers en bedrijven met één of enkele middelen overal terecht kunnen) onderschrijven we van harte. Vanuit het willen voorkomen van een single point of failure (voorbeeld DigiD) is het ook te verdedigen dat er tenminste twee authenticatiemiddelen centraal worden erkend en verplicht.
   Het effect op de NZa is potentieel groot. Het wetsvoorstel heeft als direct gevolg dat wij moeten betalen voor al deze diensten. En dat

wij ervoor moeten zorgen dat al onze digitale communicatie verloopt via een systeem van e-herkenning/ DigiD. Hierop zijn wij nog niet helemaal ingericht. Zoals eerder vermeld, we weten niet over hoeveel authenticatiemiddelen het gaat. En we hebben per authenticatiemiddel geen beeld van de aansluitkosten. We verwachten dat deze kosten significant zijn in verhouding tot ons ICT budget. Daarnaast gelden deze effecten niet alleen voor ons, maar ook voor alle zorgaanbieders die digitale diensten moeten of willen aanbieden aan burgers of medebehandelaars. Dat betreft tienduizenden zorgaanbieders voor wie diezelfde eisen gelden.

3. De onderwerpen die in de uitvoeringsregelgeving zullen worden geregeld en de daarbij te betrekken overwegingen.
   Een reactie hierop wordt verderop in dit memo nader toegelicht.

4. Wat vindt u van de begrijpbaarheid van de wetsteksten en de toelichtingen?
   Ter verbetering van de leesbaarheid en begripsvorming van "de uniforme Set van Eisen" hebben wij de volgende suggesties:
   - Bij de omschrijving van de functionaliteit een duidelijke overkoepelende omschrijving met enkele figuren ter illustratie van de procesgang op functioneel niveau (Zoals op pagina 19 van de memorie van toelichting wel is getracht, maar in onze ogen nog niet is geslaagd).
   - Ook bij de user cases zouden visualisaties de cases begrijpelijker maken.
   - We missen met name duidelijkheid over de relatie Dienstverlener en Toegangsdienst.
   - De regeling bepaalt niet duidelijk wat 'aangewezen organisaties' zijn. De benaming in deze bepaling sluit dan ook niet naadloos aan op de reikwijdtebepaling van art 2 lid 1 en zou moeten zijn: de onder artikel 2 lid genoemde organisaties; andere optie is om de in artikel 2 lid 1 genoemde organisaties te definiëren in artikel 1.

5. Welke informatiebehoefte heeft u?
   De Wgdi zal nog nader worden uitgewerkt in algemene maatregelen van bestuur. Om voldoende gerichte input te kunnen leveren zou de NZa graag direct betrokken blijven bij de totstandkoming van deze algemene maatregelen van bestuur.

6. Welke informatiebehoefte verwacht u dat uw cliënten gaan hebben?
   Onder cliënten verstaan wij in dit verband partijen en organisaties die direct en indirect met onze werkzaamheden te maken hebben. Het gaat dan onder meer om ziektekostenverzekeraars, zorgaanbieders en consumenten (burgers). Deze cliënten zullen duidelijkheid willen hebben op welke wijze ze toegang krijgen tot de diensten van de NZa en via welke middelen. Hierbij spelen toegankelijkheid en informatiebeveiliging een belangrijke rol.

7. Waaraan dient een zorgvuldig en transparant proces (punt 4) te voldoen?
   Met betrekking tot de open standaarden merken we het volgende op. Belangrijk is een tijdige aankondiging met voldoende ruimte voor inkoop, vanwege een eventuele aanbesteding, en implementatietijd voor het verplicht worden van de standaard. Eventuele implementatieprojecten moeten tijdig in de meerjarenplanningen en begrotingen van organisaties kunnen worden opgenomen. De orde

van grootte van de projecten leent zich namelijk niet voor een ad-hoc planning of bekostiging.
Daarnaast is van belang dat wij actief kunnen deelnemen aan een discussie over het opnemen van de open standaard, hetzij direct via een open forum hetzij via directe of indirecte vertegenwoordiging in een commissie. Op deze manier kan worden stilgestaan bij de wenselijkheid en haalbaarheid van een eventueel in te voeren nieuwe open standaard. Uitgangspunt daarbij zou moeten zijn dat het mogelijk moet zijn om beargumenteerd af te wijken van de standaard, uiteraard in overleg met de auditerende instantie.
Een te strikt afgedwongen standaard heeft namelijk als risico dat deze onvoldoende passend is en daardoor mogelijk onuitvoerbaar.

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)?
In onze sector (de zorg) worden de Webrichtlijnen 2.0 op dit moment als standaard beschouwd. De genoemde beveiligingsstandaarden worden door ons inmiddels als standaard-eis gesteld aan leveranciers voor nieuwe toepassingen (maar aan deze eis wordt in de praktijk nog niet volledig voldaan). DigiKoppeling wordt nog niet gebruikt door de NZa. Inmiddels is wel voorzien in een project om aan te sluiten op een Basisregistratie.

9. Wat zijn de te verwachten effecten van het verplicht stellen van de standaarden (punt 7). Is de uitvoering hierop voldoende toegerust?
Vanuit architectuuroogpunt is het gewenst dat alle aanbieders dezelfde standaarden hanteren. Met betrekking tot de Toegankelijkheidsstandaard ETSI EN 301 549 geldt dat op het hoofddomein van de NZa vanaf 2017 een nieuwe website wordt gerealiseerd waarbij de toegankelijkheidseisen uitgangspunt zijn bij het ontwerp.
Naast de nza.nl website (hoofddomein) heeft de NZa nog 9 speciale websites en webapplicaties. Hiervoor is nu geen herbouw voorzien in het kader van toegankelijkheidseisen. Wanneer deze sites moeten voldoen aan de open standaarden is naar schatting tussen de 20.000 - 50.000 euro nodig per applicatie/website. Voor diverse speciale domeinen en sites, is geen herbouw of redesign voorzien en levert een verplichte aanpassing extra kosten op die we gezien het gebruik en doelgroepen van deze domeinen waarschijnlijk niet zouden maken. We zullen hier meerdere leveranciers (ongeveer 5) mee aan het werk moeten zetten om bestaande sites alsnog te laten voldoen. De geraamde kosten hiervoor zijn, zo volgt uit bovenstaande, (voorzichtige schatting) 250.000 euro.
Voor wat betreft de eisen aan informatiebeveiliging van websites, zijn de standaarden al ons uitgangspunt en zijn we bezig met een programma om te zorgen dat we voldoen, zo mogelijk al in 2017. Ook hier zijn extra kosten mee gemoeid, ongeveer 35.000 euro.
De genoemde bedragen in dit antwoord zijn een eerste inschatting.

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?
Deze wet kan grote effecten hebben voor daartoe aangewezen private organisaties in onze sector (de zorg), omdat het om een grote hoeveelheid (kleine) zorgaanbieders gaat. Het kan een rem op digitale dienstverlening zijn, bijvoorbeeld omdat voor bestaande

praktijken de investeringskosten (te) hoog kunnen zijn. Zowel de verantwoordelijkheid als de kosten zijn niet goed te voorzien door en voor dit type zorgaanbieders. De mate waarin zorgaanbieders digitale diensten aanbieden of gebruik maken van digitale platforms om gegevens uit te wisselen, verschilt zowel binnen als tussen beroepsgroepen. De voorgestelde vormgeving van authentificatie-vereisten vraagt een opschaling van de serviceverlening die er in veel regio's nog niet is. Het leidt niet tot noemenswaardige besparing en zeker niet op korte termijn. Als er sprake is van gedwongen investeringen door de zorgaanbieders, dan heeft dat mogelijk een opwaarts effect op de hoogte van de tarieven van de door hen geleverde zorg.
De voorgestelde Wgdi raakt de relatie van de NZa met zorgaanbieders, zorgverzekeraars, zorgkantoren en andere bestuursorganen. Hier wordt in de vragen 14, 15 en 16 nader op ingegaan

11. Om welke organisaties zou dit wat u betreft gaan?
Alle zorgverleners die digitale service willen/moeten aanbieden. Voor bijv. apothekers is het een must, omdat patiënt –en medicatiegegevens gedeeld moeten kunnen worden met andere zorgverleners in de keten. Voor een beroepsgroep als tandartsen zal het eerder een keuze zijn om patiënten de mogelijkheid te bieden online afspraken te maken en foto's of verwijzingen te delen. In sommige beroepsgroepen zijn er al diensten ontstaan die het digitale verkeer ondersteunen. Zo maakt een aantal huisartsen gebruik van Zorgdomein dat allerhande digitale diensten ondersteunt, zoals digitale verwijzingen naar het ziekenhuis of apotheek. Voor deze groep heeft de wet effect op de provider. Echter door de vormgeving van de verantwoordelijkheden kunnen providers in principe alle kosten verhalen op de afnemers. Wanneer de kosten hierdoor sterk stijgen, treft het daarom ook de aangesloten zorgverleners.

12. Is de uitvoering hier voldoende op toegerust? Welke consequenties ziet u voor uw organisatie en veld?
Nee. Het gaat om grote hoeveelheid aansluitingen en de expertise op dit gebied ontbreekt veelal binnen de zorgsector. Voor de NZa is het een nieuwe dienst, er is tot op heden geen gebruik gemaakt van Digid of van eHerkenning.

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?
    Derden worden gehouden aan dezelfde eisen als de (semi)overheid.

    - Heeft dit betrekking op de periodieke IB-audits?
    Wanneer er een deugdelijke borging van de BIV (Beschikbaarheid, Integriteit en Vertrouwelijkheid van de gegevensvoorziening) moet plaatsvinden dan ontkom je niet aan een TPM (third party memorandum) op basis van een geldende norm.

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

Deze regels zijn exact hetzelfde, alleen zullen de aanbieders diverser zijn en niet allemaal even geneigd zijn zich te conformeren aan een kostbaar controleproces.

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?
Wanneer de NZa, in de rol van dienstverlener, alle aangeboden ontsluitende en geaccrediteerde diensten dient te accepteren leidt dit tot een grote beheerslast voor de NZa.
Verder zien wij het volgende mogelijke risico. Wanneer commerciële partijen zich kunnen gaan mengen in authenticatie diensten dan bestaat er een grotere kans op misbruik vanwege een toename van het aantal aanbiedende partijen.

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?

    Op dit moment kunnen wij geen enkele inschatting maken van de mogelijke aansluitkosten, maar wij houden er rekening mee dat we een significant deel van ons beschikbare budget hier voor moeten besteden. Dit is o.a. gebaseerd op eerdere inschatting voor aansluiting op e-herkenning en het noodzakelijke maatwerk wat in de betreffende, achterliggende applicaties verricht moest worden.

    - Heeft u een inschatting van de mogelijke doorlopende kosten voor de ontsluitende diensten?
    De doorlopende kosten zullen niet alleen gaan bestaan uit eventueel abonnementsgeld of (nog onbekende) kosten per authenticatie, maar ook aan kosten voor beheer en ondersteuning van onze eindgebruikers die mogelijk problemen ervaren bij het inloggen/gebruik maken van de betreffende applicatie. Tenzij dit door de Toegangsdienst voor rekening wordt genomen. We hebben dit nog niet helder uit de documentatie kunnen halen.

    - Onderschrijft u de aanname dat de baten die gegenereerd worden opwegen tegen bovengenoemde lasten?
    Wij vragen ons af op de baten opwegen tegen de lasten. De baten zijn kwalitatief, namelijk meer veiligheid, betrouwbaarheid en mogelijk wat meer gemak voor burgers en bedrijven op het moment van aanmelden voor een dienst. Maar het is lastig dit af te zetten tegen de financiële lasten. Het lijkt aannemelijk dat als er één generieke oplossing wordt aangeboden op een gestandaardiseerde infrastructuur, dat dit goedkoper in aanschaf en gebruik zal zijn, dan wanneer iedere organisatie dit voor zich gaat regelen. Echter het voorgestelde stelsel is zo uitgebreid en moet zoveel doelen dienen, dat we ons afvragen of de totale som hiervoor in een business case te gieten is. Ten slotte verstoort het verplichte karakter van de wet

het normale proces van afweging van risico's, kosten en opbrengsten die organisaties doorlopen voordat zij besluiten te investeren.

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. De NZa heeft geen mogelijkheid om de kosten door te belasten op de gebruiker. Hier kunnen wij ons dus geen beeld van vormen.

    - Vraagt deze doorbelasting veel van uw administratieve proces?
    Ja. Ons administratieve proces kent namelijk geen mogelijkheden om zaken in rekening te brengen. Hier kunnen wij ons geen beeld van vormen.

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?
    Het reguleren van deze sector, waar de kosten nog onbekend zijn, is lastig. Dit behoeft nadere uitwerking voordat de contracteerverplichting gaat gelden. Alternatieven zijn, bijvoorbeeld:
    - *de contracteerverplichting te laten vervallen;*
    - *concurrentie mogelijk te maken door bijvoorbeeld een minimumeis van drie dienstverleners te stellen;*
    - *de verantwoordelijkheid bij de overheid leggen via een hub (via de hub wordt de toegang verleend, vergelijk de route voor buitenlanders t.b.v. eIDAS).*

    - Wat is uw visie op de mogelijke bepaling van vaste tarieven of maximum tarieven?
    In de huidige constructie met een contracteerverplichting is het noodzakelijk om vaste of maximumtarieven vast te stellen. Het ontbreekt namelijk aan inzicht in de kosten.

18. De Uniforme Set van Eisen verplicht 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?
    In zijn algemeenheid merken we op dat, door de brede inzetbaarheid van de dienst en de diversiteit van taken van de NZa, deze vraag niet eenduidig valt te beantwoorden. Vanuit beveiligingsperspectief kan de NZa zich vinden in deze rationale, omdat dit leidt tot een middel om misbruik tegen te gaan, wat het vertrouwen van de gebruiker kan versterken.

Met betrekking tot het privacy aspect van meldingen van fraude is echter denkbaar, dat de melder wel interesse heeft in juiste registratie van persoonsgegevens (voor terugkoppeling en mogelijke feiten controle) maar geen interesse heeft om de metadata van de melding terug te zien in logging. Zo kan namelijk bij de melder het beeld ontstaan dat deze gegevens breed(er) beschikbaar zijn. Daarbij geldt dat de eis van het loggen van het gebruik van het authenticatiemiddel gevolgen voor de privacy kan hebben, omdat het enkele feit dat er contact is met een arts kan worden beschouwd als een medisch persoonsgegeven. De kans bestaat daarom dat met het wetsvoorstel zoals het nu luidt, deze informatie ook buiten de relatie tussen arts patiënt kan komen te liggen.

- Hoe verwacht u dat uw cliënten hiertegen aankijken?
Zie antwoord hierboven.

- Verwacht u een verschil in de perceptie hierover wanneer het een publieke authenticatiedienst (DigiD) of private authenticatiedienst betreft?
Onze verwachting is dat publieke authenticatiediensten (DigiD) hierin meer vertrouwen zullen wekken bij de gebruiker dan private authenticatiediensten.

19. 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 kunnen wij ons geen beeld van vormen.

20. De Uniforme Set van Eisen bevatten eisen over de technische koppeling tussen uw organisatie (als dienstverlener) en de ontsluitende diensten. 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?
    Onze leverancier bestudeert de Uniforme Set van Eisen, maar heeft in een eerste reactie laten weten geen problemen te voorzien ten aanzien van de realisatie.

    - Zo nee, welke aanvullende ondersteuning heeft u en/of uw leverancier nodig?
    Zie antwoord hierboven.

    - 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?
    Een openeinderegeling waarbij we koppelingen moeten leggen met een onbekend aantal toegangsdiensten lijkt ons onuitvoerbaar en

ook niet noodzakelijk. Gezien de doelen van de wet zou het voldoende zijn een zeer beperkt aantal toegangsdiensten te erkennen (maximaal 3), en aan hen de verantwoordelijkheid voor het verbinden met de authenticatiediensten te geven.

21. Wat zijn eventueel andere overwegingen of opmerkingen die u over de Wgdi of de Uniforme Set van Eisen nog wilt meegeven?
Het doel van de wet kan volgens ons ook worden behaald als de overheid volstaat met het aanbieden van uitsluitende de drie geschetste authenticatiemiddelen. Wij missen de onderbouwing voor de noodzaak van de multimiddelenaanpak, in het bijzonder de onderbouwing voor opnemen van private authenticatiemiddelen daarbinnen. We zien hoge risico's van deze aanpak in de vorm van onnodige complexiteit en hoge kosten.
Verder lijkt het stelsel flexibel opgezet in de zin dat het is gericht op het kunnen uitbreiden van authenticatiemiddelen en dienstverleners met ontkoppeling op het dienstenniveau. Maar het uitvoeringswerk - op de lagen daaronder - zal niet makkelijk om te buigen zijn naar andere standaarden of technieken waarmee dezelfde doelen veiliger en/of goedkoper kunnen worden behaald.
Veel van de problematiek die de wet tracht op te lossen, heeft de karakteristieken van de toepassingsmogelijkheden van "Blockchains". Het gaat in de aard om betrouwbare en vertrouwelijke communicatie. Blockchain techniek kan een rol spelen als alternatieve techniek binnen het voorgestelde stelsel eID en, voor sommige diensten, mogelijk als alternatief voor een voor het stelsel zelf. We vragen of een dergelijke techniek (Blockchain) is onderzocht als alternatief voor het bereiken van de doelen van het wetsvoorstel.
Wij missen een helder inzicht in de planning van de realisatie van het voorziene stelsel. Voor de planning is van belang dat het gaat om wijzigingen van een ketendienst met veel afhankelijkheden. Implementatie binnen de organisatie is daarom pas opportuun wanneer een koppeling kan worden gemaakt en kan worden getest met een Toegangsdienst die in productie is.
Voor de implementatie zou een gefaseerde invoering wellicht nuttig, zo niet noodzakelijk zijn. Daarbij kan worden begonnen met een eenvoudiger structuur - met minder middelen en dienstverleners – dat kan worden uitgebreid en aangepast.
Wat te doen wanneer het toch is misgegaan en een persoon zich succesvol voor een ander uitgeeft? In het geschetste stelsel lijkt geen centraal punt te zijn om melding te doen van zo'n situatie, waarbinnen dit kan worden opgelost.
Voor alle private partijen gelden in beginsel dezelfde beveiligingseisen als voor (semi)overheden. De groep zorgaanbieders is groot en divers. Met name voor de groepen kleinere zorgaanbieders (bijvoorbeeld eenmanszaken) is het treffen van de juiste beveiligingsmaatregelen geen primaire taak of deskundigheid. Zij kunnen daarom tegen beperkingen aan lopen. Het toezicht hierop kent daarmee ook beperkingen: welke eisen kunnen daadwerkelijk gesteld en gehandhaafd worden?
Een laatste aandachtspunt betreft een risico van overlap van toezicht; de Autoriteit Persoonsgegevens wat betreft de (beveiliging van) persoonsgegevens, de NZa wat betreft haar toezichtstaken met betrekking tot de verwerking van persoonsgegevens door ziektekostenverzekeraars. Mochten de toezichtstaken overlappen, dan dienen partijen hierover afspraken te maken, binnen het kader van het bestaande samenwerkingsprotocol.