Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

27 529 Informatie- en Communicatietechnologie (ICT) in de Zorg

Nr. 146

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 17 februari 2017

De vaste commissie voor Volksgezondheid, Welzijn en Sport heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Volksgezondheid, Welzijn en Sport over de brief van 14 november 2016 inzake Afschrift brief aan de Eerste Kamer over het ontwerp van het Besluit elektronische gegevensverwerking door zorgaanbieders.

De vragen en opmerkingen zijn op 14 december 2016 aan de Minister van Volksgezondheid, Welzijn en Sport voorgelegd. Bij brief van 16 februari 2017 zijn de vragen beantwoord.

De voorzitter van de commissie,
Lodders

Adjunct-griffier van de commissie,
Sjerp

kst-27529-146
ISSN 0921 - 7371
's-Gravenhage 2017

Inhoudsopgave

I. Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen van de PvdA-fractie

De leden van de PvdA-fractie hebben met belangstelling kennisgenomen van het ontwerp van het besluit elektronische gegevensverwerking door zorgaanbieders. Voor genoemde leden staat voorop dat patiënten zelf over hun eigen medische gegevens moeten beschikken en dat uitwisseling hiervan altijd vanuit het patiëntbelang moet worden gedaan. Zij hebben nog enkele aanvullende vragen over verschillende punten uit het concept besluit.
De leden van de PvdA-fractie lezen in de brief van de Minister over het concept besluit, dat om aan het belang van «privacy enhanching technologies» tegemoet te komen, een artikel is opgenomen over het steeds bezig blijven met het verbeteren van de informatiebeveiliging en bescherming van persoonsgegevens. Genoemde leden begrijpen dit belang, zij hebben echter signalen van experts uit het veld te horen gekregen dat de angst bestaat dat door de toevoeging van dit artikel nog niet de beoogde doelen zullen worden bereikt, gezien het niet ingaat op de verantwoording van de uitvoering hiervan. Aan wie dient de verantwoording te worden afgelegd over de constante poging tot verbetering van de informatiebeveiliging? Op welke manier denkt de Minister dat de doelen worden bereikt wanneer er geen toezichthouder in het spel is om de bevordering van de bescherming van persoonsgegevens te bewerkstelligen? Op welke manier acht de Minister het mogelijk om een dergelijke toezichthouder te benoemen voor de uitvoering van dit artikel? Welke partij is volgens de Minister de aangewezen partij hiervoor? Is dit een taak voor de Autoriteit Persoonsgegevens? Zo ja, hoe moet deze worden ingevuld en kan zij dit naast haar andere taken uitvoeren? Zo nee, waarom niet?
De leden van de PvdA-fractie hebben hiernaast nog vragen over de verhouding van dit voorliggende besluit ten opzichte van de aankomende behandeling van de Wet Inlichtingen- en Veiligheidsdiensten (WIV). Zij horen signalen dat door in te zetten op netwerkbeveiliging niet wordt gekozen voor een privacy enhancing technologies (PET) en ook niet voor databescherming by design, bij al het meest basale aspect van het gebruik van uitwisselingssystemen: de beveiliging van de verbindingen. Genoemde leden horen van experts dat dit in directe tegenspraak is met wat de Minister stelt te willen bereiken met artikel 6. Hoe luidt de reactie van de Minister op dit punt? Klopt het dat dit feit ook een (huis)arts veel extra geld kost? Monitort hiernaast het nationaal cyber security centrum (NCSC) het netwerk waarover deze data-uitwisselingen plaatsvinden? Of vindt anderszins stevige controle, ook vooraf, plaats? Zo ja, op welke wijze?

Vragen en opmerkingen van de SP-fractie

De leden van de SP-fractie hebben met interesse kennisgenomen van de wijzigingen in het Besluit elektronische gegevensverwerking door zorgaanbieders. Zij willen graag van de Minister puntsgewijs een overzicht van wat er precies gewijzigd is en waarom. Genoemde leden willen er op wijzen dat het dossier van het uitwisselen een langslepende is en dat de Kamer immer heeft aangegeven betrokken te willen zijn en vinden het jammer dat de Minister het eerder aan de Tweede Kamer

gepresenteerde besluit wijzigt zonder uitleg te geven waarom de wijzigingen doorgevoerd zijn.
De leden van de SP-fractie begrijpen dat het besluit is aangepast naar aanleiding van de wetsbehandeling in de Eerste Kamer. Dat er nu is opgenomen dat organisaties voortdurend bezig moeten zijn met het verbeteren van de informatiebeveiliging en de bescherming van persoonsgegevens is logisch. Maar waarom wordt er niet duidelijk gemaakt of en zo ja, aan wie de zorginstelling en de software-ontwikkelaar hierover verantwoording moeten afleggen. Zou het niet slim zijn om daarover iets op te nemen in het besluit? Deze leden vragen om een reactie van de Minister op dit punt.
De leden van de SP-fractie wijzen er op dat niet geheel duidelijk is wie de rol krijgt in het bevorderen van de zogenoemde privacy enhancing technologies (PET's). Deelt de Minister de mening dat bij een toezicht rol voornamelijk moet worden gekeken naar de mogelijkheden van de techniek met betrekking tot het toepassen van PETs in plaats van naar de norm? Kan de Minister hierop ingaan? Kan de Minister laten weten wie er in art 3.3 de zorgserviceprovider autoriseert? Deze leden vragen hoe de netwerkbeveiliging zich verhoudt tot de, schijnbaar, onbeveiligde data bij PET's. Kan de Minister hierop ingaan?
De leden van de SP- fractie zouden graag willen weten wat de samenhang is tussen het besluit en andere wetgeving die bijvoorbeeld mogelijkheden geven tot hacken. Is het voor de Minister evident dat medische gegevens daar nooit en te nimmer onder mogen komen te vallen? Zou ja, is de Minister dan bereid dit op te nemen in het besluit?
Tot slot willen de leden van de SP-fractie vragen hoe het besluit samenhangt met het onderzoek naar patiëntauthenticatie (PrivacyCare en PBLQ) dat wijst op het feit dat er nog geen zicht is op het benodigde betrouwbaarheidsniveau van de huidige authenticatiemiddelen. Wat gaat het besluit hieraan veranderen? Kan de Minister hierop ingaan?

II. Reactie van de Minister

Met belangstelling heb ik kennis genomen van de aanvullende vragen van een aantal fracties van uw Kamer over de brief van 14 november 2016 over het ontwerp van het Besluit elektronische gegevensverwerking door zorgaanbieders.

Artikel 6 uit het besluit regelt dat de zorgaanbieder als verantwoordelijke voor een zorginformatiesysteem en de verantwoordelijke voor een elektronisch uitwisselingssysteem, steeds bezig moeten blijven met het verbeteren van de informatiebeveiliging en bescherming van persoonsgegevens. De leden van de fracties van de ***PvdA*** *en van de* ***SP*** *vragen aan wie organisaties hierover verantwoording moeten afleggen.*

Dit besluit is een AMvB op basis van artikel 26 Wet bescherming persoonsgegevens (Wbp). In het besluit worden nadere regels gesteld aan elektronische verwerking van persoonsgegevens door zorgaanbieders. De toezichthoudende taak van de AP, neergelegd in artikel 51 lid 1 Wbp, is niet beperkt tot het terrein van de Wbp, maar strekt zich ook uit tot algemene maatregelen van bestuur zoals deze. De Autoriteit Persoonsgegevens (AP) houdt dus ook toezicht op het Besluit elektronische gegevensverwerking door zorgaanbieders.
Op verzoek van de AP moet de zorgaanbieder zich verantwoorden over de toepassing van hetgeen in artikel 6 is genoemd. Artikel 6 uit het besluit is in feite een nadere invulling van artikel 13 van de Wbp over passende beveiliging, er is dan ook geen sprake van een nieuwe taak. Overigens ben ik naar aanleiding van de motie Bredenoord in overleg met de AP over intensivering van het toezicht op elektronische uitwisseling van medische gegevens, onder de huidige wetgeving maar ook onder de

Algemene Verordening Gegevensbescherming vanaf mei 2018. Mocht de kwaliteit van zorg in gevaar komen dan is er daarnaast een rol weggelegd voor de Inspectie Gezondheidszorg (IGZ). De AP en de IGZ hebben een protocol waarin ze hun samenwerking en taakverdeling hebben vastgelegd.

*De leden van de **PvdA**-fractie vragen naar de verhouding van dit voorliggende besluit ten opzichte van het wetvoorstel voor een Wet op de Inlichtingen- en Veiligheidsdiensten (WIV).*
*De leden van de **SP**-fractie vragen wat de samenhang is tussen het besluit en andere wetgeving die bijvoorbeeld mogelijkheden geven tot hacken. Zij doelen daarmee waarschijnlijk eveneens op het wetsvoorstel voor een Wet op de inlichtingen- en veiligheidsdiensten (WIV). Zij vragen of de Minister bereid is in het besluit te regelen dat medische gegevens hiervan worden uitgezonderd.*

Het wetsvoorstel voor een Wet op de inlichtingen en veiligheidsdiensten geeft de wettelijke kaders voor de inlichtingen- en veiligheidsdiensten. Het wetsvoorstel legt vast onder welke omstandigheden deze diensten mogen binnentreden in een geautomatiseerd werk (hacken) van een persoon of organisatie die in onderzoek is. De in het voorliggende besluit gestelde eisen doen daar niets aan af en zullen ook na inwerkingtreding van voornoemd wetsvoorstel blijven gelden. Deze wettelijke kaders van het wetsvoorstel WIV lijken mij helder, en ik zie dan ook geen reden dat medische gegevens van dit wettelijk kader uitgezonderd worden.

*De leden van de fractie van de **PvdA** vragen een reactie op de signalen dat door in te zetten op netwerkbeveiliging, niet wordt gekozen voor privacy enhancing technology (PET) noch voor databescherming by design. Ook de leden van de **SP**-fractie vragen hoe netwerkbeveiliging zich verhoudt tot PET's. Daarnaast vragen zij een reactie op hun overtuiging dat het toezicht zich moet toespitsen op de mogelijkheden van de techniek bij het toepassen van PET in plaats van op de beveiligingsnormen.*

In het licht van de Algemene Verordening Gegevensbescherming (AVG) en de Wet bescherming persoonsgegevens (Wbp), moeten de zorgaanbieders en beheerders van elektronische uitwisselingssystemen passende maatregelen treffen voor de verwerking van (bijzondere) persoonsgegevens (zoals medische gegevens). Dat kunnen maatregelen rond netwerkbeveiliging zijn (of andere maatregelen die voortvloeien uit de NEN-normen), maar ook maatregelen die er juist voor zorgen dat er zo min mogelijk persoonlijke informatie uitgewisseld wordt. Het treffen van beveiligingsmaatregelen en het inzetten van PET's en databescherming by design zijn dan ook niet contrair, maar complementair aan elkaar. Het is ook niet zo dat als er gebruik gemaakt wordt van PET, geen andere beveiligingsmaatregelen meer nodig zijn en dat data onbeveiligd over de lijn mogen gaan. Om in het kader van toezicht op de Wbp en AVG te bepalen of de genomen beveiligingsmaatregelen passend zijn, moet dan ook naar beide type maatregelen gekeken worden: zowel de inzet van PET als het voldoen aan beveiligingsnormen.
Een privacy impact assessment (PIA) – een effectbeoordeling van gegevensbescherming – geeft inzicht wat voor een bepaalde gegevensverwerking passende beveiligingsmaatregelen zijn. Het uitvoeren van een PIA wordt onder meer bij grootschalige verwerking van bijzondere categorieën van persoonsgegevens onder de AVG verplicht. Het krachtens de wet normaliseren van de NEN-normen ontslaat de zorgverlener er niet van ook andere maatregelen te treffen om de risico's te minimaliseren. De Autoriteit Persoonsgegevens toetst hier samen met de IGZ op.

*De leden van de fractie van de **PvdA** vragen of het juist is dat PET de (huis)arts veel extra geld kost.*

Ook nu al dienen artsen en zorginstellingen op grond van de Wbp passende beveiligingsmaatregelen te treffen voor verwerkingen van (bijzondere) persoonsgegevens. De NEN-7510, NEN-7512 en NEN-7513 worden nu als veldnorm gebruikt bij de beoordeling van een «passend beveiligingsniveau». Tevens gelden de NEN-7510 en NEN-7512 reeds op grond van de wet gebruik burgerservicenummer in de zorg. Deze nu al bestaande normen worden nu bij AMvB tot de algemene norm verheven voor passende beveiliging. Informatiebeveiliging en bescherming van persoonsgegevens zouden daarom voor artsen en zorginstellingen geen nieuwe kostenpost moeten zijn.

*De leden van de fractie van de **PvdA** vragen of het Nationaal Cyber Security Centrum (NCSC) het netwerk waarover data-uitwisselingen plaatsvinden monitort.*

Het is de verantwoordelijkheid van verwerkers van persoonsgegevens zelf om te kijken of de gegevensverwerkingen, waaronder data-uitwisselingen over het netwerk, passend beveiligd zijn. Het is ook hun verantwoordelijkheid om waar nodig goede afspraken te maken met de netwerkaanbieders in goede bewerkerovereenkomsten. Daarbij kan de verwerker de netwerkaanbieder bijvoorbeeld vragen om vooraf en periodiek aan te tonen dat de beveiliging op orde is of eisen stellen aan logging. Het NCSC monitort of controleert deze uitwisselingssystemen en netwerken niet; het is aan de verwerker(s) om dit te doen. Ook de Zorg-Cert, het computer emergency response team voor de zorg, monitort dergelijke uitwisselingssystemen niet. Wel kunnen beide partijen, Zorg-Cert en NCSC, een rol spelen bij de oplossing van netwerk- of informatiebeveiligingsincidenten in de zorgsector of elders, waarbij de primaire verantwoordelijkheid overigens bij de verwerker dan wel bewerker blijft.

*De leden van de **SP**-fractie willen graag puntsgewijs een overzicht van wat er precies gewijzigd is in het Besluit elektronische gegevensverwerking door zorgaanbieders en waarom.*

Ten opzichte van het ontwerpbesluit zoals dat in november 2013 aan uw Kamer is gezonden, is het ontwerpbesluit zoals dat nu is toegezonden op diverse punten aangepast, als gevolg van ontwikkelingen die zich in die periode hebben voorgedaan. Ik zal die wijzigingen puntsgewijs toelichten:

- *Artikel 2 – functionaris voor de gegevensbescherming*
  Het tweede lid is aangepast naar aanleiding van de inwerkingtreding van de Wet kwaliteit, klachten en geschillen zorg en naar aanleiding van de definitieve tekst van de Algemene Verordening Gegevensbescherming, waarin geen grens van 250 werknemers is opgenomen.
- *Artikel 3 – normen*
  Artikel 5 uit het ontwerpbesluit van 2013 is geïntegreerd in artikel 3. In artikel 3 staan nu alle bepalingen bij elkaar over het voldoen aan de NEN. In het eerste en tweede lid wordt naast NEN 7510 ook NEN 7512 genoemd omdat NEN 7512 een nadere uitwerking van NEN 7510 betreft.
  Het nieuwe vierde lid vervangt de bepaling die in artikel 2 van het Besluit gebruik burgerservicenummer in de zorg (Besluit bsn-z) is opgenomen (Stb. 2014, 282). In artikel 8, tweede lid, van de Wet cliëntenrechten bij elektronische verwerking van gegevens, is een wettelijke grondslag opgenomen voor het verwerken van het bsn door de beheerder van een elektronisch uitwisselingssysteem. Vanwege die wettelijke grondslag zal de bepaling in het Besluit bsn-z, met de

inwerkingtreding van de wet komen te vervallen. In artikel 3, vierde lid wordt nu opgenomen aan welke eisen die beheerder moet voldoen.
- *Artikel 4 – termen en definities*
  Toegevoegd zijn verwijzingen naar NEN 7512 en NEN 7513.
- *Artikel 5 – eisen aan logging*
  Dit artikel 5 is gelijk aan artikel 7 als opgenomen in het ontwerpbesluit van 2013. Het voormalige artikel 5 is zoals gezegd opgenomen in artikel 3. Artikel 6 kon bij nader inzien vervallen omdat hetgeen daar werd bepaald al ligt besloten in het feit dat men moet voldoen aan NEN 7510.
- *Artikel 6 – verbeteren informatiebeveiliging*
  Dit artikel is toegevoegd omdat de technieken voor informatiebeveiliging en bescherming van persoonsgegevens zich steeds blijven ontwikkelen. Om te zorgen dat de beveiliging van systemen zoveel mogelijk up-to-date blijft, moeten de verantwoordelijken voor de gebruikte systemen blijvend aandacht houden voor vernieuwingen en het al dan niet doorvoeren van die vernieuwingen kunnen verantwoorden. De AP kan die verantwoording bij zijn toezicht gebruiken.
- *Artikel 7 – uitgave NEN*
  Deze bepaling is gelijk aan artikel 8 van het ontwerpbesluit uit 2013.
- *Artikel 8 en 9 – wetstechnische aanpassingen*
  In artikel 8 en artikel 9, tweede lid, zijn enkele wetstechnische aanpassingen opgenomen in verband met de wijziging van de citeertitel van de Wet gebruik bsn in de zorg.

*De leden van de **SP**-fractie vragen wie de zorgserviceprovider autoriseert (Artikel 3.3).*

In artikel 3 wordt aan de verantwoordelijke voor een elektronisch uitwisselingssysteem en aan de zorgaanbieder de eis gesteld dat zij zorgen voor een veilig en zorgvuldig gebruik van hun systemen overeenkomstig het bepaalde in NEN 7510 en NEN 7512. Dit betekent dat zij moeten voldoen aan organisatorische eisen en dat zij ervoor zorg moeten dragen dat de gebruikte systemen voldoen aan de technische eisen. Op grond hiervan moet ook de zorgserviceprovider door een onafhankelijke instantie worden geautoriseerd, zodat duidelijk is dat de zorgserviceprovider voldoet aan de NEN7512. Een dergelijke instantie kan bijvoorbeeld een auditor zijn die ook de elektronische uitwisselingssystemen kan beoordelen.
*Tenslotte de vraag van de leden van de **SP**-fractie naar de samenhang tussen het besluit en het onderzoek van PrivacyCare en PBLQ naar het betrouwbaarheidsniveau dat nodig is voor (bijvoorbeeld) veilige toegang tot medische gegevens.*

Het besluit heeft betrekking op specifieke organisatorische, functionele en technische eisen waaraan moet worden voldaan wil er sprake zijn van veilige elektronische gegevensuitwisseling. Niet alleen de uitwisseling moet veilig gebeuren, ook de toegang tot persoonlijke en medische gegevens moet aan eisen voldoen. Daarvoor zijn authenticatiemiddelen nodig op voldoende hoog betrouwbaarheidsniveau. Om te bepalen wat voor de zorg kwalificeert als «authenticatiemiddelen op voldoende hoog betrouwbaarheidsniveau» heb ik een onafhankelijk onderzoek laten uitvoeren door PrivacyCare/PBLQ. Het onderzoek naar het betrouwbaarheidsniveau voor patiëntauthenticatie onderschrijft het belang dat er middelen beschikbaar komen op het hoogste betrouwbaarheidsniveau. In overleg met de zorgsector, verenigd in het Informatieberaad, wordt een strategie ontwikkeld om het gebruik van beschikbare authenticatiemiddelen op het betrouwbaarheidsniveau substantieel in de zorg aan te jagen en te faciliteren en op termijn toe te groeien naar patiëntauthenticatie op

het hoogste betrouwbaarheidsniveau zodra deze middelen breed beschikbaar komen.