Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2016–2017

33 509 Wijziging van de Wet gebruik burgerservicenummer in de zorg, de Wet marktordening gezondheidszorg en de Zorgverzekeringswet (cliëntenrechten bij elektronische verwerking van gegevens)

W

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 21 februari 2017

De vaste commissie voor Volksgezondheid, Welzijn en Sport[1] heeft kennisgenomen van het bij brief van 14 november 2016 aangeboden ontwerp van het Besluit elektronische gegevensverwerking door zorgaanbieders.[2]
Naar aanleiding daarvan is op 18 januari 2017 een brief gestuurd aan de Minister van Volksgezondheid, Welzijn en Sport.

De Minister heeft op 21 februari 2017 gereageerd.

De commissie brengt bijgaand verslag uit van het gevoerde schriftelijk overleg.

De griffier van de vaste commissie voor Volksgezondheid, Welzijn en Sport,
De Boer

[1] Samenstelling:
Ten Hoeve (OSF), Koffeman (PvdD), Kuiper (CU), De Vries-Leggedoor (CDA), Flierman (CDA), Barth (PvdA), Beuving (PvdA), Ganzevoort (GL), De Grave (VVD), Martens (CDA) (*voorzitter*), Bruijn (VVD) (*vice-voorzitter*), Gerkens (SP), Kops (PVV), Atsma (CDA), Bredenoord (D66), Dercksen (PVV), Van Dijk (SGP), Don (SP), Van Hattem (PVV), Krikke (VVD), Nooren (PvdA), Oomen-Ruijten (CDA), Prast (D66), Van Rooijen (50PLUS), Schnabel (D66), Wezel (SP), Klip-Martin (VVD)

[2] Kamerstukken I 2017/17, 33 509, U en bijlage.

kst-33509-W
ISSN 0921 - 7371
's-Gravenhage 2017

BRIEF VAN DE VOORZITTER VAN DE VASTE COMMISSIE VOOR VOLKSGEZONDHEID, WELZIJN EN SPORT

Aan de Minister van Volksgezondheid, Welzijn en Sport

Den Haag, 18 januari 2017

De commissie voor Volksgezondheid, Welzijn en Sport (VWS) heeft met belangstelling kennisgenomen van het bij brief van 14 november 2016 aangeboden ontwerp van het Besluit elektronische gegevensverwerking door zorgaanbieders.[3] De leden van de fracties van **VVD** en **PvdA**, daarin gesteund door de fracties van **CDA**, **D66**, **SP**, **GroenLinks**, **SGP** en **50PLUS**, zijn van mening dat de meeste artikelen van het Besluit voor zich spreken en in lijn zijn met de eerder aangeboden informatie en de wetsbehandeling van de Wet cliëntenrechten bij elektronische verwerking van gegevens[4]; er is echter nog één artikel dat vragen oproept, namelijk artikel 6. De leden van de fracties van **D66**, **PVV** en **SP** hebben naar aanleiding van het aangeboden Besluit elektronische gegevensverwerking door zorgaanbieders nog enige aanvullende vragen en opmerkingen.

Vergewis- en verantwoordingsplicht

De leden van de fracties van **VVD** en **PvdA**, leggen naar aanleiding van artikel 6 – mede namens de hierboven genoemde fracties – nog graag de volgende vragen voor. Volgens dit artikel moeten de zorgaanbieder die verantwoordelijk is voor een zorginformatiesysteem en de verantwoordelijke voor een elektronisch uitwisselingssysteem, zich steeds vergewissen van de laatste stand van de wetenschap en techniek met betrekking tot informatiebeveiliging en de bescherming van persoonsgegevens. In de nota van toelichting staat dat het van belang is dat de verantwoordelijken steeds op de hoogte blijven van de nieuwe ontwikkelingen en zo nodig verbeteringen in hun systemen moeten doorvoeren. Deze leden zijn benieuwd hoe de regering zich dit voorstelt. Hoe ver reikt deze verantwoordelijkheid? Waar ligt de begrenzing van de wetenschappelijke ontwikkelingen en de techniek? Hoe kan door de betrokkenen beoordeeld worden welke ontwikkelingen zo relevant zijn, dat zij gebruikt moeten worden om de systemen te verbeteren en hoeveel tijd krijgen de zorgaanbieder en de verantwoordelijke voor de aanpassing van een elektronisch uitwisselingssysteem? Normaliter zijn er periodiek updates van systemen. De leden van deze fracties hebben vanuit het veld vernomen dat die «laatste stand van de techniek» altijd wordt geïncorporeerd in sectorale normen en standaarden, die weer een nadere concretisering vormen van de algemene verplichting in de Wet bescherming persoonsgegevens. Betekent dit dat het toereikend is als de zorgaanbieder en de verantwoordelijke voor een elektronisch uitwisselingssysteem zich vergewissen van de sectorale normen en standaarden en zich verantwoorden over hoe zij omgaan met deze normen en standaarden?

Als er nieuwe oplossingen zijn die tot fundamentele systeemwijzigingen moeten leiden, is de implementatie van deze oplossingen veelal een arbeids- en kostenintensief traject. Bij de behandeling van het wetsvoorstel in de Eerste Kamer heeft de Minister op een vraag van de fracties van de PvdA en VVD geantwoord dat de betrokkenen een redelijke termijn moeten krijgen om veranderingen door te voeren. Wat verstaat de regering in dit verband onder een redelijke termijn?

---

[3] Kamerstukken I 2017/17, 33 509, U en bijlage.
[4] Kamerstuknummer 33 509.

In artikel 6 is tevens opgenomen dat de zorgaanbieder en de verantwoordelijke voor een elektronisch uitwisselingssysteem, zich moeten verantwoorden voor de toepassing van de laatste stand van de wetenschap en techniek met betrekking tot informatiebeveiliging en de bescherming van persoonsgegevens bij de inrichting en het gebruik van hun systemen. Noch in het artikel, noch in de nota van toelichting wordt aangegeven hoe en aan wie verantwoording afgelegd moet worden. Bij dit wetsvoorstel zijn twee toezichthouders betrokken: de Inspectie voor de Gezondheidszorg (IGZ) en de Autoriteit Persoonsgegevens. In de toelichting wordt voor de rolverdeling verwezen naar een samenwerkingsprotocol dat deze organisaties in 2006 hebben gesloten. Zover deze leden kunnen overzien, geeft dit samenwerkingsprotocol op dit punt geen uitsluitsel. Wel is met de recent in werking getreden Algemene verordening gegevensbescherming «accountability» als een belangrijk nieuw beginsel geïntroduceerd. Verantwoordelijken moeten zich verantwoorden richting betrokkenen (individuen wiens persoonsgegevens worden verwerkt); richting samenwerkingspartners, verstrekkende en ontvangende partijen en bewerkers; richting interne en externe toezichthouders (accountants, raden van toezicht of commissarissen, Autoriteit Persoonsgegevens en IGZ). In de verordening moeten verantwoordelijken (raden van bestuur doorgaans) zich verantwoorden over de effectieve werking van de getroffen maatregelen om de verordening aantoonbaar na te kunnen leven. De leden van deze fracties vragen of de verantwoordingsplicht betrekking heeft op al deze partijen.

Zo ja, hoe kan worden voorkomen dat de uitvoeringslasten van de betrokken partijen toenemen? In de nota van toelichting geeft de regering namelijk aan dat dit besluit geen gevolgen heeft voor de administratieve lasten en de nalevingskosten. Deze leden zien graag toegelicht hoe de regering tot deze conclusie is gekomen, in het licht van het gegeven dat ten gevolge van artikel 6 de betrokkenen extra inspanningen moeten leveren en kosten moeten maken om zich te vergewissen van relevante ontwikkelingen in de technologie en wetenschap en op basis daarvan eventuele wijzigingen moeten doorvoeren, en zich moeten verantwoorden over de gemaakte keuzes. Bovendien wordt van de zorgaanbieder verwacht dat deze een interne toezichthouder, een functionaris voor de gegevensbescherming, aanstelt, zo staat in de toelichting bij artikel 2.

De leden van de fractie van **D66** ontvangen nog graag een reactie op het volgende. Artikel 6 van de voorgenomen algemene maatregel van bestuur (AMvB) luidt momenteel: «De zorgaanbieder als verantwoordelijke voor een zorginformatiesysteem en de verantwoordelijke voor een elektronisch uitwisselingssysteem, vergewissen zich steeds van de laatste stand van de wetenschap en techniek met betrekking tot informatiebeveiliging en de bescherming van persoonsgegevens, en verantwoorden zich over de toepassing daarvan bij de inrichting en het gebruik van hun systemen». Onduidelijk blijft aan wie die verantwoording moet worden afgelegd, hoeveel inspanning redelijk en billijk is om te voldoen aan de vergewisplicht, en wat de sanctie is bij het niet nakomen van die verantwoording. De leden van de fractie van D66 vragen om een reactie op dit punt.

In het aangepaste artikel 6 van het ontwerpbesluit staat dat zorgaanbieders zich moeten vergewissen van de laatste stand van de wetenschap en techniek met betrekking tot informatiebeveiliging en de bescherming van persoonsgegevens en zich moeten verantwoorden over de toepassing daarvan in hun systemen. Noch het artikel, noch de artikelsgewijze toelichting maken expliciet duidelijk op welke wijze dit vergewissen en verantwoorden plaats moet vinden. De leden van de **PVV**-fractie krijgen graag verduidelijkt hoe dit in de praktijk georganiseerd zal worden. Op welke wijze en bij wie moet verantwoording worden afgelegd? Hoe en

door wie wordt deze bepaling gehandhaafd en welke sancties zijn er aan niet-naleving verbonden?

Gegevensuitwisseling

Met de gewijzigde motie-Bredenoord c.s.[5] wordt de regering opgeroepen «dataprotectie-by-design» als uitgangspunt te nemen bij de elektronische verwerking van medische gegevens. Alhoewel een eerste aanzet hiertoe gedaan wordt middels de artikelen 3 en 6, menen de leden van de fractie van **D66** dat het in de huidige vorm nog niet toereikend is.

In artikel 3 worden de eisen waaraan een systeem moet voldoen, geformuleerd in technische (NEN-) normen. De regering zou aanvullend ook niet technisch geformuleerde dwingende ontwerpprincipes kunnen stellen aan het systeem, bijvoorbeeld: «In het systeemontwerp wordt bij iedere afweging de bescherming van persoonsgegevens meegenomen» of «In het ontwerpproces wordt in overleg met artsen bepaald welke essentiële gegevens opgeslagen moeten kunnen worden in het systeem. Uitsluitend deze essentiële gegevens worden opgeslagen». Deze leden ontvangen graag uw reactie hierop. Zij wijzen er overigens op dat in artikel 3, vierde lid, sub b het College bescherming persoonsgegevens wordt vermeld. Dit moet de Autoriteit Persoonsgegevens zijn.

In de aanbiedingsbrief staat dat de aanpassingen van de ontwerpAMvB mede naar aanleiding van de deskundigenbijeenkomst met de Eerste Kamercommissie voor VWS zijn opgesteld. Tijdens de deskundigenbijeenkomst werd door de heer Verheul (RU/KeyControls) opgemerkt dat de verwijsindex in het Landelijk Schakelpunt (LSP) een risico vormt voor de privacygegevens van de patiënten. Deze verwijsindex zou volgens Verheul onwenselijk en niet-noodzakelijk zijn; gegevens kunnen in verkeerde handen terecht komen.[6] Daarbij gaf hij te kennen dat ook een veiliger systeem mogelijk is, gebaseerd op pseudoniemen. De leden van de **PVV**-fractie vernemen graag of dit in de deskundigenbijeenkomst gesuggereerde veiligere systeem een plaats heeft gekregen binnen de nu in deze AMvB voorgestelde NEN-normen.

Tevens gaf deze deskundige aan dat het huidige LSP-systeem niet meer gebruikelijk is vanwege de risico's van ontsleuteling op een centrale plek. Wordt middels de nu voorgestelde AMvB centrale ontsleuteling uitgesloten?

Een ander kritiekpunt van zijn kant was dat de NEN-norm 7510 geen beveiligingsnorm is, maar een norm voor informatiemanagementsystemen. Tijdens het plenaire debat heeft de Minister gezegd dat de opmerkingen van de experts hieromtrent in de voorliggend AMvB zijn meegenomen.[7] Heeft er nog terugkoppeling plaatsgevonden met betreffende experts? Zo ja, bent u van mening dat de AMvB op het gebied van informatieveiligheid en privacy nu wel als toereikend kan worden beschouwd?

De leden van de PVV-fractie willen graag weten welke specifieke waarborgen de AMvB biedt ten aanzien van de informatieveiligheid. Welk beschermingsniveau tegen hacken wordt middels deze AMvB geboden?

De afgelopen tijd zijn diverse organisaties in het zorgdomein getroffen door datalekken en privacyschendingen, waarbij zorggegevens van

[5] Kamerstukken I 2016/17, 33 509, R.
[6] Kamerstukken I 2015/16, 33 509, p. 18–19.
[7] Handelingrn I 216/17, nr. 1, item 9, p. 26.

duizenden patiënten in verkeerde handen terecht zijn gekomen, zoals bij de GGZ in Gelderland[8], de gemeente Amersfoort[9] en het Isala Ziekenhuis in Zwolle[10]. In deze gevallen is sprake van het elektronisch verwerken van bestanden met daarin gegevens van een groot aantal patiënten. De leden van de PVV-fractie vernemen graag in hoeverre de richtlijnen in de voorliggende AMvB een bijdrage kunnen leveren aan het voorkomen van zulke grootschalige lekken van patiëntengegevens.

Kan worden uitgesloten dat de in deze ontwerpAMVB gestelde richtlijnen een belemmering kunnen vormen ten aanzien van de uitvoering van de aangenomen motie-Teunissen c.s. (het blijven bestaan van de decentrale mogelijkheid van bij de zorgaanbieder vastgelegde toestemmingen en autorisaties)?[11]

De leden van de fractie van de **SP** vragen waarom gekozen wordt voor het op deze wijze uitwisselen van elektronische gegevens. In feite wordt met artikel 3 het gebruik van een bepaald soort gekwalificeerd netwerk opgedrongen aan de artsen: er staat namelijk dat een netwerk «geautoriseerd» moet zijn. Wie bepaalt welk netwerk geautoriseerd moet zijn? Dat is toch de verantwoordelijke voor een elektronisch uitwisselingssysteem? Bepaalt de Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ) straks welk netwerk de arts moet kiezen? Dat staat haaks op de uitspraak van de Minister dat zij systeemonafhankelijk wil ontwikkelen. Waarom wordt gekozen voor gekwalificeerde netwerkproviders? Wat is hier het voordeel van? Hoe draagt dit bij aan de kwaliteit en veiligheid? De leden van deze fractie krijgen hierop graag een toelichting.

Met «end-to-end»- beveiliging, maar sowieso met elk redelijk beveiligd systeem tegenwoordig, is het niet meer nodig om op het – ouderwetse – model van «netwerkbeveiliging» in de zin van beveiliging van de koperen, glasvezel of virtuele draad door de netwerkprovider te leunen, maar versleutel je gewoon de getransporteerde data van punt tot punt (end-to-end). Waarom is gekozen voor netwerkbeveiliging – feitelijk de laagst mogelijke vorm van beveiliging – en niet voor «end-to-end»-beveiliging?

De leden van de fractie van de SP vernemen ook graag waarom gekozen is voor gekwalificeerde zorgserviceproviders. Wat is hier het voordeel van en hoe draagt dit bij aan de kwaliteit en veiligheid? Zij constateren dat de NEN-normen waaraan moet worden voldaan, zijn opgenomen in het ontwerpbesluit. Veel eisen staan echter al in wetgeving. Waarom is gekozen voor een dubbeling? De leden van deze fractie vragen waarom de regering niet volstaat met een verwijzing naar de NEN-normen en daarnaast alleen enkele zaken expliciteert die niet in de NEN-norm staan. Zo missen deze leden een garantie op de uptime. Hebt u overwogen dit toe te passen? Deze leden zouden graag een uptime- garantie van ruim 99% toegevoegd zien. Verder kan de eis van minimaal een «point-to-point»-versleuteling een toevoeging zijn die naar de mening van deze leden de NEN-normen verheldert en betere beveiliging aanjaagt, zonder de onnodig concrete eis van gebruik van een gekwalificeerde zorgservice-provider te stellen.

---

[8] http://www.gelderlander.nl/regio/de-vallei/gegevens-duizenden-ggz-cli%C3%ABnten-op-straat-door-datalek-1.6714485

[9] http://www.ad.nl/amersfoort/ontvanger-datalek-heeft-bestanden-gewist~a89cf2a1/

[10] http://www.nu.nl/binnenland/4332366/patientgegevens-isala-ziekenhuis-straat-diefstal-laptop.html

[11] Kamerstukken I 2016/17, 33 509, T herdruk.

Als laatste willen de leden van de SP-fractie nog graag de nieuwe Wet op de inlichtingen- en veiligheidsdiensten[12] in herinnering brengen. Wat is de visie van de regering op de reikwijdte van de voorgestelde medewerkingsplicht en de mogelijkheid die dit wetsvoorstel biedt om «backdoors» in systemen in te bouwen? Hoe kan de veiligheid van de data gegarandeerd worden wanneer het bewust openhouden moet worden ingebouwd? En hoe makkelijk wordt het om taps te plaatsen in het netwerk van een zorgserviceprovider, als informatie dit netwerk niet («point-to-point» of «end-to-end») versleuteld passeert? Ziet u hierin aanleiding om een «end-to-end»- encryptie op te nemen in het voorstel?

De leden van de commissie voor Volksgezondheid, Welzijn en Sport zien uw reactie met belangstelling tegemoet en ontvangen deze graag uiterlijk 15 februari 2017.

De Voorzitter van de vaste commissie voor Volksgezondheid, Welzijn en Sport,
Maria J.T. Martens

[12] Voorstel van wet (Kamerstukken II 2016/17, 34 588, nr. 2).

BRIEF VAN DE MINISTER VAN VOLKSGEZONDHEID, WELZIJN EN SPORT

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 21 februari 2017

Met belangstelling heb ik kennis genomen van de vragen die een aantal leden van de vaste commissie voor Volksgezondheid, Welzijn en Sport heeft gesteld over het ontwerp van het Besluit elektronische gegevensuitwisseling door zorgaanbieders dat ik u bij brief van 14 november 2016 heb aangeboden.

De meeste vragen hebben betrekking op artikel 6 van het besluit. Dit artikel stelt dat verantwoordelijken voor zorginformatiesystemen en systemen voor elektronische gegevensuitwisseling zich steeds vergewissen van de laatste stand van de wetenschap en techniek met betrekking tot informatiebeveiliging en de bescherming van persoonsgegevens en zich verantwoorden over de toepassing daarvan.

De leden van de fracties van VVD en PvdA vragen zich af hoe ver die verantwoordelijkheid reikt en hoe zij kunnen beoordelen welke verbeteringen moeten worden doorgevoerd. Zij vragen of het toereikend is als de zorgaanbieder en de verantwoordelijke van een elektronisch uitwisselingssysteem zich vergewissen van de sectorale normen en standaarden. De leden van de fracties van D66 en PVV stellen de vraag aan wie verantwoording moet worden afgelegd over het voldoen aan de laatste stand van de techniek en wat de sanctie is bij het niet nakomen van de verantwoording. De leden van de PVV-fractie vragen daarbij nog hoe dat vergewissen moet plaatsvinden.
De «stand der techniek en wetenschap» is niet eenduidig vastgelegd. Doorgaans wordt het opgevat als het hoogste niveau van technische ontwikkeling dat op een bepaald moment is bereikt. Dit niveau wordt vervolgens, met enige vertraging, vertaald en vastgelegd in normen. Europese en andere normen geven een redelijke weergave van de stand van de techniek en wetenschap, omdat over die normen brede overeenstemming is bereikt. Van de verantwoordelijke voor een informatie- of uitwisselingssysteem wordt verwacht dat hij ten minste zijn maatregelen in lijn brengt met deze binnen de sector overeengekomen en in dit geval wettelijk vastgelegde NEN-normen. Het wil niet zeggen dat per definitie het hoogste niveau van technische ontwikkeling geïmplementeerd moet worden. Dat is afhankelijk van zijn risico-afweging. De verantwoordelijke voor een zorginformatie- of uitwisselingssysteem zal periodiek moeten beoordelen, zo stellen de NEN-normen, of vanuit een risico-afweging en nieuwe technologische ontwikkelingen extra maatregelen nodig zijn. De verantwoordelijke moet zich hierover kunnen verantwoorden tegenover de toezichthouders.
In de praktijk betekent dit dat een zorgaanbieder er voor zorgt dat zijn ICT- en beveiligingsdeskundigen op de hoogte blijven van de nieuwste ontwikkelingen en plannen maken en uitvoeren om die technieken te gaan benutten. Die implementatieplannen kunnen onderdeel zijn van de verantwoording.
De Autoriteit Persoonsgegevens (AP) ziet toe op het nemen van passende technische en organisatorische maatregelen, waaronder toetsing van de wijze waarop de zorgaanbieder zijn systemen aanpast aan de laatste stand van wetenschap en techniek. De AP kan daarbij een bestuurlijke boete van max. 820.000 euro opleggen. Ook de Inspectie voor de Gezondheidszorg (IGZ) ziet in het kader van risicogestuurd toezicht toe op de naleving van relevante wet- en regelgeving op het gebied van informatiebeveiliging in

de zorg, voor zover die raakt aan kwaliteit en veiligheid van zorg. De IGZ kan in dat kader aanwijzingen geven die de zorgaanbieder moet opvolgen.

Op grond van de Algemene verordening gegevensbescherming (AVG) moeten verantwoordelijken zich verantwoorden richting betrokkenen. De leden van de fracties van VVD en PvdA vragen hoe ver de verantwoordingsplicht van artikel 6 reikt.
Zowel Artikel 6 van het besluit als artikel 5 van de AVG waarin de verantwoordingsplicht is opgenomen zijn breed geformuleerd. Artikel 6 uit het besluit is in feite een nadere invulling van artikel 13 van de Wbp over passende beveiliging. De Autoriteit Persoonsgegevens (AP) houdt toezicht op het besluit (en vanaf mei 2018 op de AVG). Op verzoek van de AP moet de zorgaanbieder zich verantwoorden over de toepassing van hetgeen in artikel 6 van het besluit is genoemd.
Mocht de zorg in gevaar komen dan is daarnaast een rol weggelegd voor de IGZ. Afgezien van mogelijke verantwoording aan de toezichthouders, moeten partijen zich op grond van AVG inderdaad breder kunnen verantwoorden. Zij kunnen dit zichtbaar maken in hun beleids- en implementatieplannen.

De leden van de fracties van VVD en PvdA vragen wat een redelijke termijn is om systeemveranderingen door te voeren.
Wat een redelijke termijn is, zal niet eenduidig zijn, maar afhangen van de inspanning die nodig is om veranderingen door te voeren. Uitgangspunt is dat partijen – net als nu – verantwoordelijk zijn voor een passende beveiliging van hun systemen, dat verandert niet.

De leden van de fractie van D66 vragen hoe kan worden voorkomen dat de uitvoeringslasten van de betrokken partijen toenemen, zij moeten zich immers vergewissen van de laatste stand van de techniek, wijzigingen doorvoeren en een functionaris voor de gegevensbescherming aanstellen.
Verantwoording met betrekking tot de informatiebeveiliging als bedoeld in artikel 6 betekent niet dat direct de best beschikbare technieken moeten worden doorgevoerd. De verantwoording houdt ook in dat – gelet op de te maken kosten en afschrijving van gebruikte systemen – duidelijk wordt gemaakt op welke termijn bepaalde wijzigingen worden doorgevoerd. Het goed beveiligen van privacygevoelige gegevens is een al bestaande plicht die inderdaad de nodige en blijvende inspanningen vergt. Artikel 6 is daar een nadere invulling van en het goed op de hoogte blijven van de relevante ontwikkelingen en daarop anticiperen, zal uiteindelijk wellicht leiden tot een kostenreductie.

De leden van de fractie van D66 vragen een reactie op de suggestie om ook niet technisch geformuleerde ontwerpprincipes te stellen.
Op basis van de Wbp ligt er al een verplichting voor zorginstellingen om zowel passende technische als ook organisatorische maatregelen te treffen. Onder die laatste valt ook het meenemen van de privacy by design-principes (zoals dataminimalisatie) waar de leden van de fractie van D66 waarschijnlijk op doelen. Daarnaast worden organisaties bij de implementatie van de AVG verplicht om de bescherming van persoonsgegevens vanaf het begin in het ontwerpproces van registraties of systemen mee te nemen. De uitvoering van een Privacy Impact Assessment (PIA), die ook ingaat op de privacy by design-maatregelen die voorzien zijn, wordt gezien als een vanzelfsprekende maatregel bij de bouw van systemen en het aanleggen van databestanden. Ik acht dan ook geen aanvullende verplichting nodig.

De leden van de fractie van D66 wijzen er op dat in artikel 3, vierde lid, sub b de Autoriteit Persoonsgegevens vermeld moet worden in plaats van het College bescherming persoonsgegevens.

Hoewel het College bescherming persoonsgegevens in het maatschappelijk verkeer inmiddels wordt aangeduid als de Autoriteit Persoonsgegevens, wordt in de Wbp en de daarop gebaseerde regelgeving zoals het voorliggende besluit, nog gesproken van het College bescherming persoonsgegevens. Met de implementatie van de Algemene verordening gegevensbescherming zal dit worden aangepast.

De leden van de fractie van de PVV vragen of de suggesties van de heer Verheul en andere experts die aanwezig waren bij de deskundigenbijeenkomst die uw Kamer organiseerde, zijn overgenomen in het besluit. Ook vragen zij welke waarborgen de AMvB biedt ten aanzien van informatieveiligheid en welk beveiligingsniveau tegen hacken is geboden.
De suggesties van de deskundigen zijn inderdaad verwerkt in het nu voorliggende besluit. De leden van de PVV-fractie noemen enkele voorbeelden van zaken die specifiek betrekking hebben op één van de systemen voor elektronische gegevensuitwisseling. Dit besluit richt zich niet op een specifiek systeem maar stelt randvoorwaarden zodat gegevens veilig kunnen worden uitgewisseld. De opmerkingen van de heer Verheul en andere experts zijn dan ook meer in den brede opgepakt en verwerkt.
Met de toevoeging van artikel 6 aan het besluit ben ik van mening dat de AMvB op het gebied van informatieveiligheid en privacy als toereikend kan worden beschouwd.
Wat betreft het beveiligingsniveau tegen hacken: het besluit schrijft geen specifiek beschermingsniveau tegen hacken voor, maar verplicht zorgaanbieders maatregelen te nemen om de kans op hacken zo klein mogelijk te maken.

De leden van de fractie van de PVV vragen in hoeverre de richtlijnen in de AMvB een bijdrage kunnen leveren aan het voorkomen van lekken van patiëntengegevens.
Het voldoen aan deze normen betekent niet dat incidenten volledig te voorkomen zijn. Waterdichte beveiliging is feitelijk niet mogelijk en bovendien komen er ook incidenten voort uit bijvoorbeeld menselijke omissies of vergissingen. Door de systemen en organisatie op orde te hebben en dit ook periodiek te toetsen, wordt het risico op dit type incidenten wel zo klein mogelijk.

In antwoord op de vraag of kan worden uitgesloten dat de in deze AMVB gestelde richtlijnen een belemmering vormen voor de uitvoering van de aangenomen motie-Teunissen c.s. (het blijven bestaan van de decentrale mogelijkheid van bij de zorgaanbieder vastgelegde toestemmingen en autorisaties) het volgende.
Zoals eerder aangegeven richt deze AMvB zich (net als de wet) niet op specifieke systemen. Er worden geen systemen van uitgesloten. Dat geldt evenzeer voor de optie om de bij de zorgaanbieder vastgelegde toestemmingen en autorisaties decentraal vast te leggen.

Wat zijn de implicaties van het feit dat zorgaanbieders gebruik moeten maken van een gekwalificeerd netwerk, zo vragen de leden van de fractie van de SP. Dit wekt bij de leden van genoemde fractie de indruk dat een bepaald gekwalificeerd netwerk wordt opgedrongen. Ook vragen zij naar de reden waarom gekozen is voor gekwalificeerde zorgserviceproviders.
Van «gedwongen winkelnering» is geen sprake: de wet en de AMvB stellen geen bepaald systeem noch een bepaald netwerk verplicht. Wel stelt de AMvB eisen aan de beveiliging. 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. Gebruik maken van een gekwalificeerd netwerk en dito

zorgserviceprovider maken daar deel van uit. Het is aan de zorgaanbieder of verantwoordelijke voor het elektronisch uitwisselingssysteem zelf te bepalen welk netwerk of welke zorgserviceprovider hij kiest. Hierbij is van belang dat het netwerk en de zorgserviceprovider voldoen aan de NEN normen (gekwalificeerd zijn). Om die reden mag een zorgaanbieder alleen gebruik maken van een uitwisselingssysteem dat is geautoriseerd op basis van de in de NEN 7512 vastgestelde criteria. Dit is opgenomen als waarborg voor een veilige uitwisseling. De autorisatie kan plaatsvinden door een onafhankelijke auditor.

De leden van de fractie van de SP vragen waarom is gekozen voor netwerkbeveiliging en niet voor «end-to-end»-beveiliging.
Netwerkbeveiliging is een containerbegrip. Hieronder wordt een aantal soorten technische maatregelen geschaard zoals inzetten van firewalls, authenticatie-maatregelen, maar ook encryptie van de gegevens die over het netwerk gaan. De keuze voor het begrip netwerkbeveiliging, omvat dan ook maatregelen als end-to-end encryptie. Het is zaak dat, vanuit een risicoafweging, passende beveiligingsmaatregelen worden genomen, waarvan netwerkbeveiliging er één is.

De leden van de SP-fractie willen weten waarom wordt verwezen naar NEN-normen die al elders in wetgeving zijn opgenomen. Ook zouden zij juist een garantie op de uptime en een eis voor point-to-point versleuteling toegevoegd willen zien.
Het Besluit elektronische gegevensverwerking door zorgaanbieders verplicht tot toepassing van de NEN-normen bij alle elektronische uitwisseling van gegevens uit zorgdossiers én alle zorginformatiesystemen, dus ook voor intern gebruik. Nu worden de NEN-normen al wel als algemene passende beveiligingsmaatregelen gezien in het licht van de naleving van de Wet bescherming persoonsgegevens, maar zijn deze feitelijk alleen verplicht daar waar in de zorg van het BSN gebruikt wordt gemaakt. Na inwerking is de reikwijdte van de verplichting verbreed. Ook is aan de verplichting de NEN 7513 toegevoegd. In het Besluit zijn verder alleen regels opgenomen voor zover naast die NEN normen en de bestaande regelgeving nadere regels voor de gegevensuitwisseling tussen zorgaanbieders nodig zijn, of ten opzichte van de NEN normen enige explicitering nodig is.
Het is aan de zorgverleners om passende beveiligingsmaatregelen te treffen op basis van een risico-afweging en gebaseerd op de geldende stand van wetenschap en techniek. Door heel specifiek in te zetten op bepaalde technieken en instrumentatie (zoals de door de leden van de fractie genoemde uptime-garantie en end-to-end versleuteling) wordt het risico geïntroduceerd dat beschikbare veiligere technieken niet geïmplementeerd worden, omdat reeds voldaan is aan het in de wet benoemde. Dit is niet in het belang van de patiënt wiens gegevens het betreft. Een ander risico is juist dat de innovatie naar veiligere technologieën geremd wordt, daar waar deze wel gewenst zijn, als in den brede bijvoorbeeld de cybersecurity-risico's toenemen.

Als laatste vragen de leden van de SP-fractie naar de relatie met en de visie op de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (WIV).
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. Dit wetsvoorstel houdt niet in dat systemen ten behoeve van de inlichtingen- en veiligheidsdiensten bewust

open gehouden moeten worden. De in het voorliggende besluit gestelde eisen blijven ook na inwerkingtreding van de WIV gewoon van toepassing.

De Minister van Volksgezondheid, Welzijn en Sport,
E.I. Schippers