Ministerie van Volksgezondheid,
Welzijn en Sport

> Retouradres Postbus 20350 2500 EJ Den Haag

De Voorzitter van de Eerste Kamer
der Staten-Generaal
Postbus 20017
2500 EA Den Haag

Bezoekadres:
Parnassusplein 5
2511 VX Den Haag
T 070 340 79 11
F 070 340 78 34
www.rijksoverheid.nl

Ons kenmerk
1085361-160519-MEVA

Bijlage(n)
-

Uw kenmerk
156848 54u

Correspondentie uitsluitend richten aan het retouradres met vermelding van de datum en het kenmerk van deze brief.

Datum 21 februari 2017
Betreft Commissiebrief Eerste Kamer inzake Ontwerpbesluit elektronische gegevensverwerking door zorgaanbieders

Geachte voorzitter,

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.

Hoogachtend,

de minister van Volksgezondheid,
Welzijn en Sport,

mw. drs. E.I. Schippers