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)

X

VERSLAG VAN EEN NADER SCHRIFTELIJK OVERLEG

Vastgesteld 24 april 2017

De vaste commissie voor Volksgezondheid, Welzijn en Sport[1] heeft kennisgenomen van de reactie van de Minister van Volksgezondheid, Welzijn en Sport van 21 februari 2017 op de schriftelijke vragen van de commissie[2] naar aanleiding van het bij brief van 14 november 2016 aangeboden ontwerp van het Besluit elektronische gegevensverwerking door zorgaanbieders.[3] Naar aanleiding daarvan van zijn op 29 maart 2017 enige nadere vragen gesteld.

De Staatssecretaris van Volksgezondheid, Welzijn en Sport heeft op 21 april 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)*, Van Strien (PVV), Bruijn (VVD) *(vice-voorzitter)*, P. van Dijk (PVV), Gerkens (SP), Atsma (CDA), Bredenoord (D66), D.J.H. van Dijk (SGP), Don (SP), Van Hattem (PVV), Nooren (PvdA), Oomen-Ruijten (CDA), Prast (D66), Schnabel (D66), Wezel (SP), Klip-Martin (VVD) Baay-Timmerman (50PLUS).

[2] Verslag schriftelijk overleg van 21 februari 2017 (Kamerstukken I 2016/17, 33 509, W).

[3] Kamerstukken I 2016/17, 33 509, U en bijlage.

kst-33509-X
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, 29 maart 2016

De commissie voor Volksgezondheid, Welzijn en Sport (VWS) heeft met belangstelling kennisgenomen van uw reactie van 21 februari 2017 op de schriftelijke vragen van de commissie[4] naar aanleiding van het bij brief van 14 november 2016 aangeboden ontwerp van het Besluit elektronische gegevensverwerking door zorgaanbieders.[5] De leden van de fracties van **PVV** en **SP** leggen u nog graag enige nadere vragen voor.

De leden van de **PVV-**fractie hebben enkele vragen naar aanleiding van het verslag schriftelijk overleg van 21 februari jl. Op pagina 7 wordt het volgende gesteld: «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.» De leden van de PVV-fractie vernemen graag aan welke concrete criteria deze verantwoording zal worden getoetst.

In antwoord op de vraag van de leden van de PVV-fractie (pagina 4 van het verslag) naar de plaats van het tijdens de deskundigenbijeenkomst gesuggereerde veiligere systeem, gebaseerd op pseudoniemen – waarbij door de heer Verheul werd opgemerkt dat de verwijsindex in het Landelijk Schakelpunt (LSP) een risico vormt voor de privacygegevens van patiënten; de verwijsindex zou onwenselijk en niet-noodzakelijk zijn en de gegevens zouden in verkeerde handen kunnen vallen – wordt op pagina 9 van het verslag opgemerkt dat deze suggesties «meer in den brede» opgepakt en verwerkt zijn. Kunt u concreet en specifiek aangeven hoe deze verwerking heeft plaatsgevonden? Biedt het ontwerpbesluit nog steeds ruimte voor het gebruik van een dergelijke risicovolle verwijsindex? Is in de verwerking van de suggesties nu wel een systeem, gebaseerd op pseudoniemen als uitgangspunt genomen?

«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», zo valt op de zelfde pagina te lezen. Hoe krijgt de handhaafbaarheid van deze verplichting in de praktijk vorm? Wat zijn handhaafbare criteria voor een passende beveiliging van het systeem, zoals gesteld op pagina 8?

Tot slot hebben de leden van de PVV-fractie nog een vraag over de subsidieregeling Versnellingsprogramma Informatie-uitwisseling Patiënt en Professional[6] (VIPP) die afgelopen december door het Ministerie van VWS is opengesteld. In enkele artikelen op de website Zorg-ICT Zorgen wordt gesteld dat deze subsidieregeling van 105 miljoen euro een verkapte vorm van staatssteun zou zijn aan het Landelijk Schakelpunt (LSP).[7] Kan worden uitgesloten dat hier sprake is van staatssteun aan het LSP? Kunt u aangeven of door deze subsidieregeling het LSP wordt bevoordeeld ten opzichte van alternatieve systemen? De leden van de

---

[4] Verslag schriftelijk overleg van 21 februari 2017 (Kamerstukken I 2016/17, 33 509, W).
[5] Kamerstukken I 2016/17, 33 509, U en bijlage.
[6] Staatscourant 2016, nr. 68985.
[7] https://www.zorgictzorgen.nl/politisering-lsp-door-105-miljoen-euro-verkapte-staatssteun-vws/

PVV-fractie vernemen ook graag of deze subsidieregeling niet in strijd is met de door de Eerste Kamer aangenomen motie-Tan c.s.[8]?

Ook de leden van de fractie van de **SP** hebben naar aanleiding van het verslag schriftelijk overleg nog enkele vragen. Op pagina 7 wordt gesteld dat de «stand der techniek en wetenschap» wordt opgevat «als het hoogste niveau van technische ontwikkeling dat op een bepaald moment is bereikt». Echter, er staat ook dat er eerst «brede overeenstemming» bereikt moet zijn; vervolgens worden op pagina 10 de NEN-normen, als algemeen passende beveiligingsmaatregelen, als afdoende aangemerkt. Op pagina 9 valt te lezen dat u het «in den brede» oppakken en verwerken van opmerkingen van de heer Verheul (niet van alle deskundigen in de deskundigenbijeenkomst, overigens) als afdoende beschouwt, en de AMvB op het gebied van informatieveiligheid en privacy toereikend acht. Tegelijkertijd geven de NEN-normen geen duidelijkheid over de eisen van privacy-by-design zoals deze voortkomen uit de Algemene verordening gegevensbescherming (AVG). Ook zegt een NEN- norm weinig over de beveiliging op zich, maar meer over de processen rondom de beveiliging. Een en ander leidt ertoe dat dat het huidige niveau van beveiliging als voldoende wordt aangemerkt. Is dat wat u ook beoogt te zeggen? De leden van de SP-fractie krijgen dit graag nader toegelicht.

Zij zijn bovendien erg verbaasd over de opmerking op pagina 10 dat het opnemen van bepaalde technieken en instrumentatie zoals uptime-garanties of end-to-end versleuteling een remmende werking zouden hebben op innovatie. Hoe komt u tot deze uitspraak? Wordt hiermee bedoeld dat een goede beveiliging en gebruikersvriendelijkheid niet innovatief zijn? Welke innovatie zou hierdoor belemmerd worden? End-to-end versleuteling en authenticatie behoort zonder meer tot het hoogste niveau van technische ontwikkeling, daar kan geen enkele twijfel over bestaan. Deelt de regering deze visie van de leden van de SP- fractie? Zo nee, waarom niet en welke technologie kan dan als beter worden beschouwd? Zo ja, waarom wordt deze beveiliging dan niet geëist, tenminste als minimumeis?

De Inspectie voor de Gezondheidszorg (IGZ) ziet 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 de zorg. De IGZ kan in dat kader aanwijzingen geven die de zorgaanbieder *moet* opvolgen (pagina 7 en 8). Betekent dit dat de IGZ over informatiebeveiliging gaat? Zo ja, op welke wijze is de IGZ voor deze taak geëquipeerd? De leden van de fractie van de SP willen ook graag weten hoe de Autoriteit Persoonsgegevens (AP) dan nog betrokken is bij dit proces. Kan dit leiden tot tegenstrijdige aanwijzingen? In de ogen van deze fractieleden ziet de IGZ toe op de gezondheidszorg en de AP op de dataprotectie. Bovendien is de AP een onafhankelijk instituut. Waarom is ervoor gekozen om deze taak bij de IGZ neer te leggen en niet bij het onafhankelijke instituut, de AP?

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* (pagina 9 en10). De NEN 7512 bevat een algemene beschrijving van een vertrouwensmodel waarin bepaalde niveaus van beveiliging worden genoemd die bij communicatie tussen partijen in de zorg behaald kunnen of moeten worden, afhankelijk van het soort gegevens dat uitgewisseld

[8] Kamerstukken 2010/11, 31 466, X.

moet worden. Bij die beschrijving hoort geen omschrijving van (criteria voor) wat een gekwalificeerd netwerk of een gekwalificeerde zorgserviceprovider zou moeten zijn, noch hoe een «uitwisselingssysteem» (dit behelst veel méér dan alleen communicatie / netwerksystemen) zou moeten autoriseren. De NEN-normen zeggen niets over de implementatie en niets over een «kwalificatie» voor een netwerk of zorgserviceprovider. De enige plekken waar in de NEN 7512 «gekwalificeerd» staat, gaat het over gekwalificeerde certificaten voor elektronische handtekeningen.

Het is van belang is dat het netwerk en de zorgserviceprovider voldoen aan de NEN-normen (gekwalificeerd zijn), zo staat op pagina 9 te lezen. «Om die reden mag een zorgaanbieder alleen gebruik maken van een uitwisselingssysteem dat is geautoriseerd op basis van de in NEN 7512 vastgelegde criteria.» De leden van de SP-fractie vernemen graag hoe men een uitwisselingssysteem kan autoriseren op basis van de criteria die in NEN 7512 zijn vastgelegd.

In reactie op de vraag naar de Wet op de inlichtingen- en veiligheidsdiensten (WIV) wordt gesteld dat de WIV er niet op gericht is om zwakheden in de systemen toe te staan; er is echter ook geen verplichting zwakheden te delen ten einde die snel te dichten. Bent u van mening dat een mogelijk lek, dat tot gevolg kan hebben dat zorggegevens in verkeerde handen dreigen te vallen, onmiddellijk gedicht dient te worden, dus ook door de veiligheids- en inlichtingendiensten? Zo ja, op welke wijze wordt gegarandeerd dat dit ook gebeurt?

De leden van de SP-fractie krijgen tot slot nog graag nader toegelicht hoe de regering privacy-by-design wil stimuleren, want zij zien hiertoe nog geen duidelijke stimulans.

De leden van de commissie voor Volksgezondheid, Welzijn en Sport zien uw reactie met belangstelling tegemoet en ontvangen deze graag uiterlijk 28 april 2017.

De voorzitter van de vaste commissie voor Volksgezondheid, Welzijn en Sport,
M.J.T. Martens

BRIEF VAN DE MINISTER VAN VOLKSGEZONDHEID, WELZIJN EN SPORT

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 21 april 2017

Met belangstelling heb ik kennis genomen van de nadere vragen die een aantal leden van de vaste commissie voor Volksgezondheid, Welzijn en Sport heeft gesteld naar aanleiding van mijn reactie van 21 februari 2017 op de schriftelijke vragen van de commissie over het bij brief van 14 november 2016 aangeboden ontwerp van het Besluit elektronische gegevensverwerking door zorgaanbieders.

De verantwoordelijken van een zorginformatie- of uitwisselingssysteem moeten zich kunnen verantwoorden tegenover de toezichthouders over hun oordeel of er al dan niet extra maatregelen nodig zijn. De leden van de fractie van de PVV vragen op basis van welke criteria de toezichthouders dit beoordelen. De toezichthouders toetsen aan de geldende wet- en regelgeving en hanteren de geldende NEN-normen. Het is aan de toezichthouders invulling en vorm te geven aan hun toezichthoudende taak.

De leden van de fractie van de PVV vragen hoe de suggestie van de heer Verheul is verwerkt, of het ontwerpbesluit nog ruimte biedt voor een verwijsindex als die van het LSP en of nu een systeem gebaseerd op pseudoniemen als uitgangspunt is genomen. Ook vragen zij hoe de verplichting voor zorgaanbieders om maatregelen te nemen om de kans op hacken zo klein mogelijk te maken vorm krijgt.
Het besluit is gericht op alle elektronische uitwisselingssystemen en niet geschreven met een specifiek systeem als uitgangspunt. Vandaar dat opmerkingen van de heer Verheul over één bepaald systeem niet specifiek, maar meer in zijn algemeenheid zijn meegenomen bij het opstellen van het besluit.
Met de wet Cliëntenrechten bij elektronische verwerking van gegevens en het besluit worden de randvoorwaarden vastgelegd voor elektronische gegevensuitwisseling. Hiermee worden heldere, algemene kaders en grenzen geboden zonder het tot op detailniveau «dicht te spijkeren». Zo blijft er ruimte voor voortschrijdend inzicht, nieuwe technologische ontwikkelingen en innovatieve oplossingen waarop de zorgaanbieders hun maatregelen kunnen treffen en de toezichthouders hun criteria kunnen aanpassen. Bijvoorbeeld als het gaat om maatregelen tegen hackers. Het Nationaal Cyber Security Centrum publiceert concrete en gedetailleerde richtlijnen en ook zorgserviceproviders worden aangemoedigd deze richtlijnen te volgen.
De in artikel 3 van dit besluit genoemde auditors kunnen dit toetsen. Deze richtlijnen worden met het voortschrijden van de techniek bijgewerkt.

De leden van de fractie van de PVV stellen een aantal vragen over de subsidieregeling voor het Versnellingsprogramma Informatie-uitwisseling Patiënt en Professional.
Het doel van het Versnellingsprogramma Informatie-uitwisseling Patiënt en Professional is dat mensen zelf over hun medische gegevens kunnen beschikken. Zij kunnen deze gegevens gebruiken bij de zorg voor zichzelf en ze desgewenst met andere zorgverleners delen. De patiënt krijgt hiermee de optimale regie over zijn gegevens.
Het is een subsidie aan ziekenhuizen, die hiermee hun eigen werkprocessen anders kunnen gaan inrichten zodat zij gegevens op een gestandaardiseerde manier gaan opslaan (via de zorginformatiebouwstenen van

Registratie aan de Bron), de gegevens beter benutten in het contact tussen patiënt en arts en hun ICT-infrastructuur op orde brengen.
Om ervoor te zorgen dat de patiënt de gegevens ook daadwerkelijk kan gebruiken en delen is het van belang dat er gebruik gemaakt wordt van standaarden. In de VIPP-subsidieregeling is zo veel als mogelijk gebruik gemaakt van zorgstandaarden die in gebruik zijn, omdat dit optimaal bijdraagt aan interoperabiliteit en bovendien kansen op fouten in de informatie minimaliseert. Daarbij is aangegeven dat er ook gebruik gemaakt mag worden van nieuwere standaarden, zoals de standaarden die in het kader van MedMij worden ontwikkeld, zodat mensen in 2020 in een persoonlijke gezondheidsomgeving zelf op een veilige manier hun medische gegevens kunnen beheren.
Als patiënten zelf op een gestandaardiseerde wijze over hun gegevens kunnen beschikken kunnen zij deze uitwisselen met andere zorgverleners, zonder dat hier een landelijk of regionaal schakelpunt aan te pas komt. De subsidie is daarom geen verkapte staatssteun aan het Landelijk Schakelpunt en niet in strijd met de motie Tan.

De leden van de PVV-fractie verwijzen in hun vragen naar de website Zorg-ICT Zorgen, waar staat dat de eisen die specifiek aan het onderdeel medische gegevens worden gesteld het gebruik van het LSP bevorderen. Zoals hierboven aangegeven staat in de regeling dat er van bestaande – of nieuwere standaarden – gebruik mag worden gemaakt. Eén van de standaarden die daarbij genoemd wordt is de informatiestandaard medicatieproces v6.12.2. Dit is een standaard die zorgbreed wordt ingevoerd om een eenduidige uitwisseling van medicatiegegevens mogelijk te maken en op die manier het aantal medicatiefouten in de zorg verder terug te dringen. Ik vind dit een belangrijke verbetering van de patiëntveiligheid. Volgens Zorg-ICT Zorgen zijn in deze standaard eisen opgenomen die overeenkomen met de technische infrastructuur van het LSP. Dit zijn eisen waar ook andere systemen voor uitwisseling van gegevens aan kunnen voldoen. Omdat het mij niet gaat om deze specifieke infrastructuur maar om veiligheid en om standaardisatie, wordt in het Informatieberaad gewerkt aan een nieuwere versie van deze standaard die infrastructuuronafhankelijk is.

De leden van de fractie van de SP zien graag een toelichting op het verslag schriftelijk overleg van 21 februari jl. waarin wordt gesteld dat de stand der techniek en wetenschap wordt opgevat als het hoogste niveau van technische ontwikkeling dat op een bepaald moment is bereikt, dat de NEN-normen als algemeen passende beveiligingsmaatregelen gelden en dat over de NEN-normen brede overeenstemming moet zijn bereikt. De leden van de SP-fractie merken op dat de NEN-normen geen duidelijkheid geven over de eisen van privacy-by-design die voortkomen uit de Algemene verordening gegevensbescherming (AVG) en dat een NEN-norm weinig zegt over de beveiliging op zich.
Zoals hierboven eerder geschetst vormen de bepalingen uit het besluit heldere kaders en randvoorwaarden voor veilige elektronische gegevens-uitwisseling zonder tot op detailniveau bepaalde technieken voor te schrijven. Dat is een bewuste keuze, zou dat wel gebeuren dan is de wet en/of het besluit niet voldoende toekomstbestendig. Er moet ruimte zijn en blijven voor innovatie, juist om de stand der techniek en wetenschap te kunnen toepassen. De nadruk van de NEN-normen – die overigens op dit moment worden herzien – zijn inderdaad iets meer gericht op informatie-beveiliging dan op privacy, daarnaast is en blijft de Wet bescherming persoonsgegevens (Wbp) onverkort van toepassing. Op basis hiervan mag worden verwacht dat principes als doelbinding, dataminimalisatie (zowel in verzamelen van persoonsgegevens als in het gebruik hiervan), transparantie en het gebruik van privacy-enhancing technologieën (waarvan pseudonimisering er één is) worden toegepast.

De leden van de fractie van de SP vragen naar de reden van de opmerking in het verslag schriftelijk overleg dat het opnemen van bepaalde technieken niet innovatief zou zijn.
Inderdaad, end-to-end versleuteling behoort op dit moment tot het hoogste niveau van technische ontwikkeling. Maar dat kan over een tijdje weer iets anders zijn. Juist daarom spreken we van passende beveiligingsmaatregelen gebaseerd op de geldende stand van wetenschap en techniek. Zou je specifieke technieken benoemen dan bestaat de kans dat men na implementatie daarvan onvoldoende oog houdt voor vernieuwende technieken en geen prikkel ervaart te blijven innoveren. Ik heb dus niet bedoeld te zeggen dat bepaalde technieken een rem vormen op de innovatie.

De leden van de fractie van de SP vragen nader toe te lichten hoe zowel de IGZ als de AP in het kader van de informatiebeveiliging in de zorg toezicht kunnen houden.
De stelling van deze leden dat de IGZ toeziet op de gezondheidszorg en de AP op de dataprotectie is geheel juist. De AP houdt óók toezicht op de beveiliging van persoonsgegevens in de zorg. Naast de Wet bescherming persoonsgegevens toetst de AP dus ook aan bijvoorbeeld het Besluit elektronische gegevensverwerking door zorgaanbieders. De IGZ houdt toezicht op goede zorg op grond van de Wet kwaliteit, klachten en geschillen in de zorg (Wkkgz). Vanuit die hoedanigheid kan de IGZ informatiebeveiliging betrekken in haar toezicht indien de kwaliteit van zorg in het geding is als gevolg van het onveilig omgaan met medische persoonsgegevens. De IGZ hanteert daarbij ook de NEN-normen.
Indien persoonsgegevens daadwerkelijk zijn ingezien door derden die niet bevoegd waren tot kennisneming, komt de meldplicht van artikel 34a Wbp in beeld en zal de verantwoordelijke moeten bezien of hij de Autoriteit Persoonsgegevens in kennis dient te stellen van het datalek en in sommige gevallen, conform de Wbp en conform artikel 10, derde lid, Wkkgz, ook de cliënten van wie de gegevens zijn gelekt. Zorgaanbieders moeten er voor zorgen dat zij die regels naleven, ook als zij werk uitbesteden aan een zorgserviceprovider. De Inspectie voor de Gezondheidszorg heeft op grond van o.a. de Wkkgz en de Wet BIG een rol als de kwaliteit van zorg in het geding is als gevolg van het onveilig omgaan met (bijzondere, de gezondheid betreffende) persoonsgegevens. Een datalek is geen calamiteit als bedoeld in artikel 11 eerste lid Wkkgz en valt dan ook niet onder de meldplicht van zorgaanbieders in die wet, maar moet op grond van de meldplicht datalekken worden gemeld aan de AP. Dat neemt niet weg dat de IGZ graag meldingen inzake datalekken (bij zorginstellingen en solistisch werkende zorgverleners) van de AP wil ontvangen. De IGZ ziet deze meldingen dan als signaal en gebruikt dit voor haar risico-gebaseerde toezicht. De IGZ en de AP hebben voor deze eventuele overlap in de toezichthoudende taken een samenwerkingsprotocol afgesloten.

De leden van de fractie van de SP vragen hoe een elektronische uitwisselingssysteem geautoriseerd kan worden op basis van de criteria die in NEN 7512 zijn vastgelegd.
Aantonen dat de elektronische gegevensuitwisseling goed beveiligd is en voldoet aan de NEN 7512 kunnen verantwoordelijken zelf doen (zelfverklaring) of door een onafhankelijke externe auditor laten vaststellen. De NEN7512 schrijft voor dat de gegevensuitwisseling geclassificeerd moet zijn op een aantal aspecten (vertrouwelijkheid, integriteit, etc.). Een auditor kan vaststellen (of de verantwoordelijke verklaart zelf) of de classificatie inderdaad is uitgevoerd, of de bijbehorende maatregelen zijn geïmplementeerd, en hoe effectief die maatregelen dan zijn.

In reactie op het antwoord op de vraag naar de Wet op de inlichtingen- en veiligheidsdiensten (WIV) vragen de leden van de SP-fractie mijn mening over de stelling dat een mogelijk lek, dat tot gevolg kan hebben dat zorggegevens in verkeerde handen dreigen te vallen, onmiddellijk gedicht dient te worden, dus ook door de veiligheids- en inlichtingendiensten. Door het kabinet is bij brief van 8 november 2016 aan de Voorzitter van de Tweede Kamer der Staten-Generaal (Kamerstukken II 2016/17, 26 643, nr. 428) ingegaan op het gebruik van onbekende kwetsbaarheden in hardware en software. Daarbij is ook nadrukkelijk aandacht besteed aan de inzet van wettelijke bevoegdheden voor de nationale veiligheid. Zo is daar geschetst onder welke uitgebreide waarborgen de diensten de bevoegdheid tot het binnendringen van geautomatiseerde werken mogen toepassen, maar ook is daarbij een eerder door het kabinet ingenomen standpunt herhaald waar het gaat om de omgang met door de diensten in het kader van de uitvoering van een wettelijke bevoegdheid geconstateerde kwetsbaarheden die de belangen van de gebruikers van internet kunnen schaden. In dat geval zullen de diensten de belangendragers informeren, echter wettelijke bepalingen (zoals de wettelijke plicht tot bronbescherming en bescherming actueel kennisniveau) of operationele redenen kunnen aan het melden van die kwetsbaarheden(tijdelijk) in de weg staan. Op de toepassing van de bevoegdheid kan toezicht worden uitgeoefend door de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten.

De leden van de SP-fractie krijgen tot slot nog graag nader toegelicht hoe de regering privacy-by-design wil stimuleren, want zij zien hiertoe nog geen duidelijke stimulans.
De noodzaak tot het toepassen van privacy-by-design principes volgt rechtstreeks uit de geldende regelgeving rondom privacy, de Wbp en straks de Algemene Verordening Gegevensbescherming (AVG). Sinds 2013 is het kabinetsbeleid dat bij nieuwe regelgeving waarin gegevensverwerkingen worden geregeld en bij overheidsverwerkingen in grote ICT-systemen een Privacy Impact Assessment (PIA) moet worden gedaan als onderdeel van het integraal afwegingskader voor wetgeving en beleid (IAK). Dat betekent dat reeds bij de ontwikkelingen van de regels of een nieuw systeem de risico's voor privacy integraal worden beoordeeld, wat kan leiden tot het nemen van technische en organisatorische maatregelen. Hiermee wordt privacy by design gestimuleerd. In de aanloop naar de implementatie van de AVG wordt van lopende en startende trajecten concreet nagegaan of deze AVG-proof zijn en dus of de privacy by design principes zijn toegepast. In de ontwikkeling van het nieuwe rijksmodel voor een gegevensbeschermingseffectbeoordeling (voorheen PIA) in de zin van de AVG wordt ook aandacht besteed aan het principe van privacy by design.
De privacy-by-design principes maken bovendien als beleidskader integraal onderdeel uit van NORA: de Nederlandse Overheid Referentie Architectuur die de overheid zichzelf oplegt, maar die ook gebruikt worden voor afgeleide dochterarchitecturen in de verschillende domeinen. Voor de zorg worden deze uitgangspunten bijvoorbeeld ook doorvertaald in en naar de programma's die onder de vlag van het Informatieberaad worden ontwikkeld. Daarmee wordt toepassing van deze kaders binnen het gehele BSN-domein gestimuleerd.
De NORA bevat voor alle relevante onderwerpen naast kaders, standaarden en bouwstenen een begrippenkader en afgeleide praktische handreikingen voor de toepassing hiervan. Zo ook op het terrein van privacy en privacy-by-design[9].

[9] Zie bijvoorbeeld voor handreikingen in de http://www.noraonline.nl/wiki/View_Privacy en http://www.noraonline.nl/wiki/NORA_Gebruikersraad/2017-01-17

Ook het Centrum Informatiebeveiliging en Privacybescherming (CIP), het expertisecentrum voor informatiebeveiliging en privacybescherming van, voor en door overheidsorganisaties heeft handreikingen beschikbaar[10]. Het CIP heeft zich ontwikkeld tot een publiekprivate netwerkorganisatie, waar ook deskundige marktorganisaties als kennispartners aan deelnemen. CIP ontwikkelt overdraagbare producten in eerste instantie gericht op overheidsorganisaties en de marktpartijen die in de rol van leverancier of ketenpartner betrokken zijn bij de overheid, maar die ook voor derden beschikbaar zijn. Op deze manier wordt kennis over Privacy-by-design vergroot.

Ik hoop uw vragen hiermee afdoende te hebben beantwoord.

De Staatssecretaris van Volksgezondheid, Welzijn en Sport,
M.J. van Rijn

[10] https://www.cip-overheid.nl/