13
Datalek in de jeugdzorg

Aan de orde is het **debat** over **een datalek in de jeugdzorg**.

De **voorzitter**:
We gaan door met het volgende debat, het debat over een datalek in de jeugdzorg. Ik zoek de eerste spreker, mevrouw Westerveld van GroenLinks. We hadden echt bijna tien minuten geleden al moeten beginnen. Ik zie haar niet. Dan geef ik het woord maar aan de tweede spreker, de heer Edgar Mulder van de Partij voor de Vrijheid. Het woord is aan hem. De eerste spreker meldt zich nu alsnog. U moet meteen deze kant op komen, mevrouw Westerveld. Rechts afslaan. Iedereen kan het.

Mevrouw **Westerveld** (GroenLinks):
Voorzitter. Stel, je werd mishandeld door je vader. Iedere keer als je met een onvoldoende thuiskwam, kreeg je klappen. Deed je het deksel niet terug op de pot pindakaas, kreeg je klappen. Liet je je schoenen in de gang slingeren: klappen. Hierdoor ontvluchtte je thuis zo veel mogelijk. Op je 13de hing je op straat, op je 14de ging je drinken, op je 15de blowen en op je 16de werd je opgepakt voor winkeldiefstal. Inmiddels gaat het beter. Je gaat weer naar school en haalt daar voldoendes. Thuis komt soms iemand praten, waardoor je relatie met je ouders ook beter is.

Voorzitter. Dit zou zomaar een echt gebeurd verhaal kunnen zijn, van een familie die voor de buitenwereld doet alsof er niets aan de hand is, maar die in jeugdzorgland heel bekend is, want alle nare gebeurtenissen, mishandelingen, maar ook drank- en drugsgebruik en winkeldiefstal worden bijgehouden in een dossier. Stel nu dat dit dossier niet meer achter een beveiligingscode op een harde schijf te vinden is, maar gewoon op een openbare website staat, gekoppeld aan je naam en adres, samen met de verhalen van duizenden andere kinderen.

Voorzitter. Het zou rampzalig zijn voor dit gezin als ineens klasgenoten en buren hun meest gevoelige geheimen weten. En het internet vergeet niets. Dus zelfs als iemand volwassen is, kunnen verhalen uit het verleden hem of haar altijd blijven achtervolgen. Dit is een enorme inbreuk op de privacy, maar ook een breuk in het vertrouwen. Want jongeren moeten ervan kunnen uitgaan dat hun gegevens veilig zijn bij jeugdzorgaanbieders, helemaal als het om vertrouwelijke en vaak ook pijnlijke gegevens gaat.

Dit had ook echt kunnen gebeuren, want afgelopen week lazen we bij RTL Nieuws dat de dossiers van duizenden kinderen uit de jeugdzorg waren gelekt. Hierin wordt in detail beschreven hoe een jong meisje seksueel wordt misbruikt. Er worden problemen met drugs beschreven en verhalen over verwaarlozing en psychische stoornissen. Het waren geen hackers die nachtenlang op een zolderkamertje zaten om de systemen binnen te dringen. Het kon door simpel voor een paar euro een domeinnaam op te kopen. Gelukkig zijn zowel de klokkenluiders als RTL zorgvuldig omgegaan met de dossiers. Maar stel je toch eens voor dat dit anders was afgelopen.

Daarom de volgende vragen. Hoe kon dit gebeuren? Belangrijker: hoe kunnen we in de toekomst voorkomen dat dit bij andere instellingen gebeurt? Zijn er andere instellingen die melding hebben gemaakt van een soortgelijk datalek? Kan de minister uitsluiten dat er jeugdzorgdossiers in de verkeerde handen zijn beland? Is het preventief opkopen van andere oude domeinnamen de oplossing? Is dit gedaan met alle domeinnamen van oud-zorginstellingen, of alleen met domeinnamen van instellingen die bij Z-CERT zijn aangesloten? Kortom, is de privacy van alle jongeren in de jeugdzorg nu gewaarborgd? Kan de minister garanderen dat dit niet nog eens gebeurt?

Voorzitter. Instellingen moeten natuurlijk zelf hun ICT op orde hebben, maar de minister kan ze wel ondersteunen. Dit gebeurt ook, via Z-CERT, expertisecentrum op het gebied van cybersecurity in de zorg. De minister vraagt nu instellingen voor jeugdhulp en jeugdbescherming om zich hierbij aan te sluiten. Maar op de website zien we dat deze diensten alleen beschikbaar zijn voor ziekenhuizen en ggz-instellingen. Dus hoe zit dit? Mijn collega Ellemeet verzocht een aantal maanden geleden te verkennen of deelname aan Z-CERT verplicht kan worden gesteld. Is deze casus aanleiding om haar motie versneld uit te voeren of om over te gaan tot een verplichting?

Voorzitter. Niet alleen ging het hier mis, vanwege slordigheid met een domeinnaam, ook blijkt dat persoonsgegevens en soms hele dossiers onbeschermd per e-mail werden verstuurd. Hoe gaat de minister ervoor zorgen dat de mensen op de werkvloer weten hoe ze met deze gegevens moeten omgaan? Ik kan me namelijk goed voorstellen dat hoge werkdruk er soms toe leidt dat snelheid boven privacybewust handelen gaat.

Voorzitter. Eén gebruiksvriendelijk en eenduidig systeem waarmee medewerkers dossiers kunnen inzien, bijwerken en versturen, kan helpen. Dat verlaagt de werkdruk en verkleint de kans op het schaden van privacy. Niet elke instelling hoeft dan zelf het wiel uit te vinden. Graag een reactie van de minister. Hoe denkt hij hierover?

Waar nu onbevoegden toegang hadden tot dossiers van duizenden jongeren, krijgen jongeren zelf paradoxaal genoeg niet altijd toegang tot hun eigen gegevens. Ik hoor verhalen van jongeren die maanden bezig zijn om hun dossiers op te vragen en van gevallen waarin inzage simpelweg wordt geweigerd. Wat vindt de minister daarvan? Is hij het met ons eens dat dit heel raar en ook heel ongewenst is? Weet hij hoe vaak jongeren geen inzage krijgen in hun dossier? Wil hij jongeren helpen die hiertegen aanlopen?

Voorzitter, ik sluit af. Ik hoop dat er twee dingen uit dit debat komen. Ik hoop aan de ene kant dat het ervoor zorgt dat dossiers van jongeren beter worden beschermd en aan de andere kant dat jongeren zelf juist meer toegang krijgen tot hun eigen gegevens.

De **voorzitter**:
Dank u wel. Zoals reeds aangekondigd: de heer Edgar Mulder van de fractie van de Partij voor de Vrijheid.

De heer **Edgar Mulder** (PVV):
Rampzalig; de PVV kan het niet anders noemen. Ruim 3.000 dossiers van kwetsbare kinderen liggen in principe op straat, met details over misbruik, mishandeling, verwaarlozing en ga zo maar door. Een kwart van de kinderen is jongeren dan 12 jaar. Wat als deze gegevens in kwaadwillende handen waren gevallen of nog komen? Wat als dit op social media terechtkomt? Denk eens aan de gevolgen als afpersing, chantage en bedreiging en überhaupt de wanhoop bij deze kinderen! Een horrorscenario. Het gaat niet alleen om medische dossiers, maar ook om interne e-mails en voicemailberichten, audiobestanden waarin zorgverleners problemen bespreken, alles zonder beveiliging, zonder versleuteling of zelfs maar een wachtwoord om de toegang tot de dossiers op slot te zetten. Helemaal niets. Kleuterklasniveau. Er is sprake van falen op het gebied van ICT, maar ook natuurlijk menselijk falen.

Voorzitter. Uit alle gegevens blijkt dat deze organisatie, die zich Samen Veilig Midden-Nederland noemt, een totaal verkeerde omgang heeft met medische gegevens. Er is geen enkel besef van privacy, geen enkel besef van veiligheid, en blijkbaar geen besef wat de gevolgen kunnen zijn voor kwetsbare jongeren. Al sinds 2016 is de AVG in werking, de Algemene verordening gegevensbescherming, en moet een instelling dus ook verplicht een functionaris hebben voor gegevensbescherming. Hoe ziet de minister toe op deze verordening? Heeft Samen Veilig Midden-Nederland een dergelijke functionaris? En hoe zit het met de andere jeugdzorgbureaus in Nederland? Is de minister bereid om alle jeugdzorgbureaus door te lichten op hun ICT- en communicatieveiligheidsbeleid? Zo nee, dan wil ik ook graag weten waarom niet.

Voorzitter. Het is toch eigenlijk vreemd en ongelofelijk dat we dit debat nu hebben, in 2019. We kunnen naar Mars en doen dat ook, maar een dossier beveiligen lukt niet. Juist in de zorg zou ICT-beveiliging optimaal moeten zijn, niet alleen omdat data de nieuwe olie is, maar vooral omdat patiëntgegevens niet op straat mogen komen te liggen. De PVV snapt daarom ook niets van de reactie van minister De Jonge, die in zijn brief van 15 april schrijft dat het allemaal wel heel erg is, maar dat de oplossing zou liggen in een abonnement bij Z-CERT. Iedereen moet zich abonneren bij Z-CERT. In de hele brief van de minister komt Z-CERT zesmaal voor. De PVV vindt dit vreemd, want ICT hoort toch preventief te werken? Maar Z-CERT is een brandweer. We moeten toch voorkomen dat het gaat branden, in plaats van iets te regelen zodat we snel kunnen blussen? Graag een uitgebreide reactie hierop van de minister.

Voorzitter. Wat de PVV betreft stelt de minister deze instelling daarom onder verscherpt toezicht totdat is aangetoond dat de privacy van de kinderen gewaarborgd is.

De **voorzitter**:
Dank u wel. Dan de heer Hijink van de fractie van de SP.

De heer **Hijink** (SP):
Voorzitter. Door een fout bij Bureau Jeugdzorg zijn medische dossiers van duizenden kwetsbare kinderen gelekt. Dat is extreem gevaarlijk. Ik dacht net dat het ook wel bijzonder cynisch is dat dit juist bij Bureau Jeugdzorg is gebeurd, nu hun nieuwe naam SAVE is. Als deze data daadwerkelijk in verkeerde handen waren beland, dan waren de gevolgen niet te overzien geweest. Kinderen die verschrikkelijke dingen als mishandeling of seksueel misbruik hebben meegemaakt, moeten altijd in vertrouwen hun verhaal kunnen vertellen. Maar zij moeten er ook op kunnen vertrouwen dat hun verhaal veilig wordt bewaard. Het gaat om het leven van heel kwetsbare jongeren. Hun gegevens moeten tot op het hoogste niveau beveiligd en beschermd worden.

Voorzitter. Het is echt ernstig als een oude website die wordt afgesloten, zomaar wordt vrijgegeven en hierdoor zo veel data toegankelijk wordt, maar blijkbaar was het bij Bureau Jeugdzorg in Utrecht ook heel gebruikelijk om dossiers van kinderen in platte tekst per mail rond te sturen. Hoe kan de minister dat verklaren? Hoe kan zoiets basaals misgaan bij een dergelijke organisatie? Het wemelt in de zorg van datalekken: in de jeugdzorg, de ziekenhuiszorg en de ggz. Maar ook andere sectoren mogen eraan geloven. Kijk naar het nieuws van vandaag. Bij het CBR worden medische gegevens opgeslagen in een compleet achterhaald systeem met Windows XP. Medische gegevens worden daar bewaard in een systeem waar al jaren geen updates meer voor worden uitgevoerd.

Zorgorganisaties zijn verplicht om eventuele datalekken te melden bij de Autoriteit Persoonsgegevens, maar als zij knullig met hun dataverkeer zijn omgegaan, wordt dat natuurlijk niet gezien, totdat het misgaat. Dan wordt het gemeld. Is de Autoriteit Persoonsgegevens wel in staat om haar taken in de zorg naar behoren uit te voeren? Dat is ook mijn vraag aan de minister: is de autoriteit niet veel te afhankelijk van meldingen vanuit de sector zelf? Zou het niet goed zijn als de Autoriteit Persoonsgegevens en de Inspectie Gezondheidszorg en Jeugd opties gaan verkennen om het toezicht op en de controle van de bescherming van gegevens in de zorg te versterken, zodat wij datalekken juist kunnen voorkomen in plaats van altijd achter de feiten aan te lopen? Ik krijg op dit voorstel graag een reactie van de minister.

Voorzitter. Kunnen wij er eigenlijk wel op vertrouwen dat al die organisaties in de zorg, groot en klein, hun data op een goede manier beschermen? Moeten de toezichthouders en de minister daar niet veel meer op toezien? Het feit dat wij hier vanavond staan met minister De Jonge en niet met zijn collega Bruins laat ook zien hoe versnipperd ICT bij de overheid is. Tussen ministeries ... bínnen een ministerie is het al ingewikkeld. Laat staan tussen duizenden organisaties en zorgverleners in de zorg. Welke stappen heeft de minister inmiddels gezet richting andere aanbieders in de jeugdzorg? Wie rapporteert straks of alles op orde is? Of komen wij daar pas achter als het opnieuw is misgegaan? En geldt zijn oproep om de eigen dataveiligheid te onderzoeken ook voor andere sectoren in de zorg? Hoe gaat hij daar vervolgens op toezien? Wie gaat zorgen dat dit ook echt gaat gebeuren?

Wat vindt de minister van de optie om in samenwerking met brancheorganisaties, cybersecurityexperts en ethische hackers steeksproefsgewijs en breed hacktesten te gaan uitvoeren bij zorgorganisaties, dan weer eens bij een grote instelling, dan bij een kleine zelfstandige? Ga het maar eens proberen, uiteraard zonder de medische gegevens te verspreiden en door zo weinig mogelijk in te zien. Ga maar

eens testen hoe we ervoor staan. Graag een reactie van de minister op dit voorstel.

Tot slot. Als zorgorganisaties aangeven dat het beveiligen van gegevens prioriteit heeft, dan zien we dat nog onvoldoende terug. Van een incident is helaas niet meer te spreken als je ziet op hoeveel plekken in de zorg het op dit moment misgaat. Het is dan ook raar dat ziekenhuizen en andere zorgaanbieders in de Cybersecuritywet niet worden aangewezen als aanbieders van essentiële diensten. Daarmee krijgen zorgverleners en patiënten niet de veiligheid en zekerheid die zij nodig hebben. Is de minister bereid om te onderzoeken of deze zorgaanbieders alsnog aangewezen kunnen worden als een aanbieder van een essentiële dienst? Want als onze gezondheidszorg al niet meer een essentiële dienst is, dan vraag ik mij af wat het dan allemaal wel is.

Voorzitter. Het lekken van medische dossiers kan levens verwoesten. Deze situatie is buitengewoon ernstig. Welke maatregelen gaat de minister nemen om te zorgen dat dataverkeer in de zorg op het hoogst mogelijke niveau wordt beveiligd en wordt getoetst?

Dank u wel.

De **voorzitter**:
Dank u wel. Dan mevrouw Kooten-Arissen van de Partij voor de Dieren.

Mevrouw **Van Kooten-Arissen** (PvdD):
Voorzitter, dank u wel. Wat zou het prettig zijn als wij het vandaag konden hebben over een incident, dat iemand vergeten was de domeinnaam te registreren, dat de data uiteindelijk niet echt op straat was gekomen of dat het foutje was gecorrigeerd; eind goed, al goed. Maar de realiteit is anders: we moeten het hebben over structurele fouten in de omgang met privacy en data in de zorg. De zorg is de sector met de meeste datalekken. De voorbeelden van misstanden zijn legio: onterechte inzage in patiëntendossiers in het ziekenhuis, hackers die jongeren afpersen met informatie die die jongeren dachten online in vertrouwen met professionele hulpverleners gedeeld te hebben, honderdduizenden medische dossiers die in handen van Google belanden en nu dus de zeer gevoelige informatie van bijna 3.000 kwetsbare jongeren, die vrijelijk beschikbaar was. Dit alles in het afgelopen halfjaar.

Vandaag nog werd bekend dat er bij het CBR 1 miljoen medische dossiers zijn opgeslagen in een database die al negen jaar geen veiligheidsupdates heeft gehad. Het gaat dus structureel mis met de gegevens die de allerhoogste bescherming en zorgvuldigheid vereisen en verdienen. Met een beetje publiek beschikbare informatie kan al een individu worden achterhaald. Gezien de gevoeligheid van deze informatie mag dat niet gebeuren. Punt. Maar het gebeurt toch, want de infrastructuur waarop vertrouwd wordt is structureel gebrekkig. Als de infrastructuur zo in elkaar zit dat medische gegevens via onbeveiligde e-mail in plain text gedeeld worden, als studenten met een bijbaantje haast onbeperkte toegang tot de medische dossiers hebben of als de gegevens openstaan voor hackers, dan is er sprake van een gebrekkige infrastructuur en gegevensbescherming. Wat ons betreft bespreken we dit vandaag dan ook, met alle respect voor de vicepremier, met de verkeerde minister. Het is namelijk zijn collega, de minister voor Medische Zorg, die deze Kamer recent een brief stuurde waarin hij uiteenzette hoe hij de gehele zorgsector verplicht wil digitaliseren. De lijn die daarin geschetst wordt, is er niet een die doet geloven dat dit soort incidenten in het vervolg niet meer meegemaakt hoeven worden.

Omdat we altijd met menselijke fouten te maken zullen hebben, is het van belang om voor infrastructuur te kiezen die zo min mogelijk fouten, lekken en misstanden toelaat. Daarom is het onverstandig dat er nog altijd vertrouwd wordt op bijvoorbeeld het Landelijk Schakelpunt. De infrastructuur, die in 2011 ongekend hard afgewezen werd, stelt de gegevens van miljoenen mensen open voor veel meer mensen dan nodig: huisartsen, apothekers, zorgverleners en hun medewerkers in ziekenhuizen kunnen straks bij die data. Acht jaar later blijkt dit systeem dus nog altijd even onverenigbaar met privacybelangen, maar is het nog altijd niet ten grave gedragen. Het is zelfs door de sector benoemd tot "onomstreden bouwsteen".

Een privacywebsite schreef recentelijk naar aanleiding van de impasse waarin de minister is beland rondom de toestemmingsverlening — het is nu namelijk of te algemeen of niet uitvoerbaar — dat het tijd werd om na te denken over een wereld zonder het LSP; die stelling onderschrijf ik. Zoals het onveilig is om dossiers via onbeveiligde mail te versturen, zo is het ook onveilig om de gehele zorg te digitaliseren op basis van een systeem dat gegevens niet van verzender tot ontvanger versleutelt, dat geen specificering kent voor de toestemmingsverlening om ervoor te zorgen dat jouw dossier alleen openstaat voor diegenen die daar recht op hebben en dat wordt beheerd door een Amerikaans bedrijf dat door de nationale veiligheidswetgeving aldaar op elk moment gedwongen kan worden om alle data te overleggen zonder enige Nederlandse partij daar kennis van te geven.

Voorzitter. De Raad van State had recent kritiek op de wijze waarop de Nederlandse regering haar beleid vormgeeft. Belanghebbenden zouden te veel invloed hebben op de wijze waarop wetgeving tot stand komt. De minister komt nu met een voorstel om de gehele zorg verplicht te digitaliseren en gaat daarbij uit van de infrastructuur die door de senaat unaniem is weggestemd en door privacyorganisaties, die hierbij geen eigen belang hebben, onverenigbaar wordt geacht met de privacywetgeving. Ook lezen we dat het voornemen van de minister is om in een rap tempo te digitaliseren en om daarbij niet klein, met een proef, te willen beginnen maar meteen zo groot mogelijk in te willen zetten. Ik vraag de Kamer en de minister daarom om stevig te herbezinnen.

Voorzitter. Digitalisering kan helpen in de zorg, maar als we digitaliseren dan moet dat op vrijwillige basis; het mag geen verplichting zijn. En als men vrijwillig besluit deel te nemen, dan moet dat door middel van een infrastructuur die de allerhoogste privacy- en gegevensbescherming garandeert.

Voorzitter, tot slot. Kan de minister aangeven hoe het staat met het onderzoek naar de end-to-endencryptie in de zorg, zoals gevraagd in mijn aangenomen motie?

Dank u wel.

De **voorzitter**:
Dank u wel. Dan mevrouw Tielen van de VVD.

Mevrouw **Tielen** (VVD):
Voorzitter. Het is een nachtmerrie, een nachtmerrie waar sommige jongeren en hun ouders de afgelopen week van wakker hebben gelegen. Want stel je voor dat vreemde mensen zomaar het persoonlijke verhaal, de geheimen en de privésituatie van deze jongeren kunnen lezen, omdat mensen aan wie ze die toevertrouwden slordig zijn omgegaan met dat verhaal en de veiligheidsregels niet hebben toegepast. Het gaat om gevoelige verhalen, die nu dus ergens kunnen rondzwerven. Computers en ICT kunnen veel gemak brengen, maar dat betekent niet dat professionals kunnen stoppen met denken en hun gezonde verstand niet meer hoeven te gebruiken. Je laat een dagboek niet opengeslagen op de balie liggen. Je kopieert geen privéverhalen om ze vervolgens uit te delen. Je bent dus ook heel voorzichtig met de informatie die je van jongeren en hun ouders te horen krijgt.

Voorzitter. Volgens mij is er niemand in deze Kamer die er niet van is geschrokken. We hebben al een aantal bijdragen gehoord. Daarom is het goed dat we dit debat nu hebben. Er zijn drie dingen die ik vandaag van deze minister wil weten. Allereerst gaat het om de zekerheid over de veiligheid van de dossiers bij soortgelijke jeugdhulporganisaties. Ik wil ook weten wat de reden is dat de huidige wet- en regelgeving kennelijk niet in de praktijk wordt gebracht. Ten slotte heb ik vragen over de verantwoordelijkheden en het toezicht op de veiligheid van die gegevens.

Allereerst vraag ik deze minister wat er klopt van de berichten van SAVE Midden-Nederland. In de brief die we gisteren van de minister kregen, staat dat SAVE zelf een onderzoek doet naar de omvang van het lek. Wanneer zijn de resultaten van dit onderzoek beschikbaar? En kan dat niet sneller, zou ik nu alvast willen zeggen. Wat heeft SAVE nu laten weten aan die kinderen, jongeren en ouders die potentieel slachtoffer zijn van dit datalek? Wat doet deze minister om jongeren in het land de zekerheid te geven dat hun dossiers en verhalen veilig zijn? Ik ga er ook van uit dat deze minister zich vorige week meteen heeft laten informeren over de dataveiligheid bij soortgelijke jeugdhulpinstellingen. Ik wil graag horen wat hij heeft gedaan en doet om te zorgen dat jongeren in Nederland er vertrouwen in kunnen hebben dat hun verhalen veilig zijn én blijven in de handen en de dossiers van die hulpverleners. Graag een reactie.

Voorzitter. Als tweede wil ik mijn ongeloof uiten over al die wetten en regels die we hier hebben vastgesteld en het feit dat het kennelijk niet lukt om die altijd in de praktijk te brengen. Ik geloof dat eigenlijk echt niet. Toch zie je het gebeuren. Wat gaat deze minister doen om ervoor te zorgen dat professionals die in de jeugdhulp werken ook daadwerkelijk wat kunnen doen met de regels die we hebben, elke dag, met elk dossier, met elk verhaal en in contact met elke collega, gewoon altijd en overal? De minister schreef in zijn brief over de Z-CERT-aansluiting. Ik vind het ook een moeilijke naam, moet ik zeggen. Hij onderzoekt of die rond de zomer wellicht verplicht kan worden, op initiatief van de aangenomen motie-Ellemeet. Ik verwacht van de minister iets meer daadkracht en actie in plaats van onderzoek. Graag een reactie.

Tot slot de eenvoud van de verantwoordelijkheden en het toezicht daarop. Ik vind het niet eenvoudig. Wie is er nu verantwoordelijk voor die dataveiligheid, en wie kan de verantwoordelijke mensen en instanties op de vingers tikken als dat nodig is en tot verbetering dwingen? Dat het bestuur van een organisatie er verantwoordelijk voor is om wetten en regels met betrekking tot privacy uit te voeren, lijkt me duidelijk. Dat het bestuur moet zorgen dat zijn medewerkers weten hoe ze goed, veilig en vertrouwd werken, lijkt me ook duidelijk. Maar wat als dat kennelijk niet goed genoeg lukt? Wat dan? Ligt dat dan bij de raad van toezicht, het college van burgemeester en wethouders dat erbij betrokken is, de inspectie, de minister of de Autoriteit Persoonsgegevens? En als ik het al niet goed snap, hoe moeten al die jongeren en hun ouders het dan begrijpen? Wie is aanspreekbaar als er dingen fout gaan? Kan de minister toezeggen dat hij het toezicht verheldert? Bij wie moeten ze zich melden, de jongeren die bang zijn dat hun verhalen niet meer veilig zijn?

Voorzitter. Dit debat moet helpen om de medewerkers in de jeugdzorg bewust te maken van de veiligheid en het vertrouwen dat zij moeten bieden en waar nu twijfel over is. Dit debat moet er vooral voor zorgen dat kinderen en jongeren in vertrouwen hun verhalen kunnen vertellen, zodat ze passende hulp kunnen krijgen. Dat vertrouwen mag niet geschaad worden, maar dat is vorige week wel gebeurd. Graag hoor ik van deze minister wat deze kinderen en jongeren van hem mogen verwachten om dat vertrouwen terug te krijgen.

Dank u wel.

De **voorzitter**:
Er is een vraag van de heer Hijink.

De heer **Hijink** (SP):
Ik heb daarstraks het punt gemaakt dat het probleem met het lekken van data natuurlijk is dat we er altijd pas achteraf achter komen dat er een probleem is. Als een zorginstelling data lekt, dan moet zij daarvan melding maken bij de Autoriteit Persoonsgegevens en vervolgens vinden we dat allemaal verschrikkelijk. Maar daar schieten we natuurlijk niet zo gruwelijk veel mee op. Mijn vraag is dus: vindt mevrouw Tielen, vindt de VVD nou ook niet, net als de SP, dat er vooraf veel meer toezicht zou moeten zijn op de veiligheid van data bij zorginstellingen en dat de inspectie of de Autoriteit Persoonsgegevens steekproefsgewijs of op een andere manier veel vaker bij instellingen moet controleren of ze de boel wel op orde hebben?

Mevrouw **Tielen** (VVD):
Meneer Hijink haalt een goed punt aan. Dat heeft ook te maken met de vragen die ik stel: hoe zit dat toezicht in elkaar en waar moet je zijn? Het doorlichten van het hele systeem klinkt als iets wat we allemaal graag zouden willen, maar ik weet niet wat we daarmee over ons heen trekken. In essentie ben ik het dus eens met wat meneer Hijink zegt. Ik hoor graag hoe de minister daarnaar kijkt. Maar wat u zegt, namelijk "liever voorkomen dan genezen" of — hoe heet het ook alweer officieel? — "de put dempen voor het

kalf verdrinkt", daar ben ik zeker ook van. Als dat nodig is, dan graag.

De heer **Hijink** (SP):
De inspectie controleert ook niet iedere dag iedere instelling. Dat stellen wij ook niet voor. Ik stel voor dat er veel vaker naar een instelling wordt toegestapt — de ene keer kan dat een groot ziekenhuis zijn en de andere keer een zelfstandige psychiater — en dat dan heel gericht wordt gekeken, ook in samenwerking met ethische hackers, die dat op een goede manier kunnen doen, of dat ziekenhuis dan wel die meneer of mevrouw de veiligheid wel op orde heeft, en dat daar dan publiekelijk over wordt gerapporteerd, zodat als het fout gaat daar een waarschuwing van uitgaat naar andere zorgverleners: let op, jullie liggen onder het vergrootglas en als je het niet goed voor elkaar hebt, dan gaan we dat melden en dan komt het in de krant.

Mevrouw **Tielen** (VVD):
Vanmiddag hebben we het, overigens in een ander debat, uitgebreid over de inspectie gehad: waar kun je met je risico's en signalen terecht, en gebeurt er dan iets mee? Wat mij betreft heeft u heel erg gelijk. De vraag is ook: als je het gevoel hebt dat de veiligheid, het vertrouwen wat betreft informatie en gegevens over jou niet goed geborgd wordt, kun je dan ergens aankloppen en kijkt dan iemand met je mee? Ik denk heel eerlijk dat — het komt niet vaak voor volgens mij — we het met elkaar eens zijn, meneer Hijink.

De **voorzitter**:
Dank u wel. We gaan luisteren naar de heer Raemakers van de fractie van D66.

□

De heer **Raemakers** (D66):
Voorzitter. "Boos en bang." "Geweld en misbruik." "Geschopt en geslagen." Dit zijn woorden die veel terugkomen in dossiers van duizenden vaak kwetsbare kinderen, dossiers die zomaar op straat hadden kunnen liggen. Het gaat om uiterst gevoelige informatie, over een eetstoornis, anorexia, over een depressie, over seksueel misbruik of over zelfmoordpogingen. D66 kan er niet bij dat gegevens van kwetsbare kinderen zo makkelijk kunnen lekken. Hoeveel kinderen zijn nu bang dat hun verhaal op straat komt te liggen? Hoeveel kinderen durven hun verhaal straks niet meer te delen? En hoeveel kinderen hebben nu minder vertrouwen in de zorg? Voor D66 zijn dit vragen die vandaag centraal staan. Hoe zorgt de minister ervoor dat alle kinderen weer vertrouwen in de zorg krijgen?

Voorzitter. Allereerst wil ik mijn waardering uitspreken voor de wijze waarop de klokkenluiders en journalisten met het datalek zijn omgegaan. Ze hebben het lek ontdekt en duidelijk gewaarschuwd voor de kwetsbaarheden van soortgelijke organisaties. Tegelijkertijd houden deze ethische hackers rekening met de mogelijke gevolgen voor de slachtoffers. Maar wat als kwaadwillenden gebruik hadden gemaakt van dit lek of in de toekomst hiervan gebruik gaan maken? Vorig jaar nog waarschuwde de Autoriteit Persoonsgegevens ons heel duidelijk. Toen maakte de AP bekend dat er meer dan 3.000 datalekken in de zorg zijn. En van het totale aantal lekken bij de overheid is een derde een lek in de zorg. Daarmee is de zorg de twijfelachtige koploper. IT-experts vertellen ons dat het droevig is gesteld met de dataveiligheid in de zorg en dat die sector achterloopt. Dat werd nog maar eens duidelijk door de basale fouten die zijn gemaakt bij de Utrechtse jeugdzorginstelling: zeer gevoelige gegevens over jongeren werden rondgemaild zonder enige vorm van versleuteling en verouderde domeinnamen werden niet veiliggesteld om misbruik te voorkomen. En nu waarschuwen de klokkenluiders bovendien dat er tientallen organisaties zijn waar de dataveiligheid ook niet op orde is. Kortom, dit is geen incident maar een structureel probleem. Ik kan niet anders dan constateren dat deze minister dit probleem heeft genegeerd. De minister lijkt het niet onder controle te hebben, hij schuift alle verantwoordelijkheid van zich af. De minister wijst in zijn brief vooral op de verantwoordelijkheden van anderen: Z-CERT, SAVE Midden-Nederland en Jeugdzorg Nederland. Maar ik wil weten: wat gaat de minister zelf doen? Wat heeft hij het afgelopen jaar gedaan? Ik word niet echt wijs uit het feitenrelaas dat ik voor vandaag heb opgevraagd. Als het gaat over jeugdzorg, lees ik al helemaal niets. Het woord "jeugdzorg" komt er niet eens in voor. Wil de minister dit helemaal overlaten aan de gemeenten?

Vorige week nog stuurde het kabinet een brief naar de Kamer over digitalisering van patiëntengegevens, een heel belangrijk onderwerp. Maar hoe kunnen mensen erop vertrouwen als er zo met de gegevens wordt omgegaan? Wat D66 betreft gaat de minister nu eerst snel aan de slag met de cyberveiligheid in de hele zorg. Die moet op orde voordat we verder gaan met digitalisering van gegevensuitwisseling. Veiligheid voorop. Graag een reactie.

Is de minister in dat kader bereid om in samenwerking met cybersecurity-experts en ethische hackers hacktesten te laten uitvoeren in alle zorgsectoren, zoals de SP zonet al vroeg? Is deze minister, gezien de grote risico's van meer datalekken en het feit dat het om zeer kwetsbare jongeren gaat, bereid om op zeer korte termijn alle jeugdzorginstellingen door te lichten op het gebied van gegevensbescherming?

Tot slot nog een aantal specifieke vragen. Eerst over Z-CERT, het Zorg-CERT. Wat heeft de minister gedaan om Z-CERT te versterken? Is de minister bereid nog voor de zomer het onderzoek over het verplicht stellen van deelname van de Z-CERT af te ronden? De minister heeft Z-CERT gevraagd zelf alle domeinnamen te gaan registreren. Hoeveel oude domeinnamen zijn er gekocht door anderen? Is het nodig om oude domeinen op te gaan kopen?

En over specifiek de jeugdzorg. Weet de minister hoeveel jeugdzorginstellingen hun informatie, e-mails en voicemails niet versleutelen? En wat doet hij daartegen? Hoeveel jeugdzorginstellingen hebben überhaupt beleid ten aanzien van dataveiligheid? Wat gebeurt er als er ergens in Nederland dossiers op straat komen te liggen? En als die dadelijk echt op straat komen te liggen, hoe worden de slachtoffers van zo'n lek dan geholpen? Worden medewerkers van jeugdzorginstellingen überhaupt wel getraind op cyberveiligheid, op cyberhygiëne? Wat is de rol van de inspectie hierin?

Al met al verwacht ik vandaag echt concrete stappen te vernemen van deze minister. Voor een man die houdt van actieplannen is het op dit moment nog angstvallig stil.

Dank u wel.

De heer **Hijink** (SP):
Hoorde ik de heer Raemakers nou net zeggen dat, voordat de cyberveiligheid van data in de zorg op orde is, de minister zijn plannen on hold moet zetten? Ik denk bijvoorbeeld aan de PGO's, de patiënten gezondheidsomgeving waarbij iedereen in een app zijn eigen dossier kan inzien, of aan de discussies die we hebben over de communicatie tussen zorginstellingen waar een hoop gebeurt, een landelijk schakelpunt zoals mijn buurvrouw dat net heeft genoemd. Zegt de heer Raemakers eigenlijk: dat moeten we allemaal bevriezen totdat de veiligheid op orde is? Dat zei hij volgens mij en dat is een vrij vergaande stap. Ik vraag mij af of hij dat serieus meent.

De heer **Raemakers** (D66):
Zeker. Wij vinden dat veiligheid vooropstaat. En wat we vorige week hebben gezien, beoordeelt mijn fractie als zeer ernstig. Natuurlijk delen wij — daar hebben wij vaker in deze Kamer een punt van gemaakt — dat gegevens in de zorg slimmer en beter kunnen worden uitgewisseld. We hebben ook situaties waarbij iemand in een ambulance terechtkomt en de cruciale informatie die nodig is dan met een fax moet worden aangeleverd. Dat kan anno 2019 niet meer, en dus moeten we dat systeem veranderen. Maar volgens mij moeten we bij deze verandering één ding vooropstellen, en dat is de veiligheid. Als we met elkaar verdergaande stappen gaan nemen in het kader van digitalisering, dan moet aan één randvoorwaarde absoluut altijd worden voldaan, en dat is de veiligheid. Medische gegevens horen niet in handen van mensen die er niks mee te maken hebben. Het antwoord op de vraag is eigenlijk heel helder. Voor D66 is het heel duidelijk: veiligheid voorop.

De heer **Hijink** (SP):
Ja, dat is mij inmiddels ook duidelijk, maar de vraag is altijd wat dat in de praktijk betekent. Betekent dat heel concreet dat D66 bij dezen zegt: de ontwikkeling van de PGO's die de minister en zijn collega Bruins graag willen, zetten wij nu on hold. De gesprekken die gaan over de samenwerking tussen zorginstellingen zetten wij on hold totdat dit probleem is opgelost. Is dat wat D66 zegt?

De heer **Raemakers** (D66):
Ik heb net een aantal concrete vragen gesteld aan de minister, waarvan ik echt vind dat deze minister die op korte termijn moet oppakken. Ik wil heel graag horen of de minister bereid is die stappen te zetten. Het is inderdaad waar dat deze minister misschien een aantal zaken samen met de minister voor Medische Zorg zal doen, maar vanavond spreken wij met de minister van VWS. Deze minister is stelselverantwoordelijk en verantwoordelijk voor het ministerie. Ik wil van deze minister horen hoe hij dat ziet.

De heer **Hijink** (SP):
Dat is geen antwoord op de vraag. Ik vroeg hem: vindt D66 dus nu dat de ontwikkeling van de PGO's, de patiënten gezondheidsomgevingen, als voorbeeld en de andere ontwikkelingen die er op ICT-gebied aan de gang zijn, gestopt moeten worden, gestaakt moeten worden, tot het moment dat deze minister kan garanderen dat de beveiliging van medische gegevens helemaal op orde is? Is dat wat hij zegt?

De heer **Raemakers** (D66):
Volgens mij is het duidelijk. Veiligheid is onze randvoorwaarde. Dus wij willen alleen verder met dat soort zaken als de minister ons vanavond kan garanderen dat de veiligheid vooropstaat en dat de regering er alles aan zal doen om allereerst de veiligheid te borgen.

Mevrouw **Van Kooten-Arissen** (PvdD):
Dit is een prachtige draai van D66, zou ik bijna zeggen. Ik vond het bij het referendum een beetje pijnlijk, maar nu ben ik heel blij dat D66 hierop blijkbaar gedraaid is. Dit staat in schril contrast met de motie die D66 samen met de VVD en het CDA heeft ingediend op 7 juni vorig jaar en waarin zij de minister verzochten om juist heel veel haast te maken met het verplicht stellen van het delen van medische dossiers op een elektronische manier en dan ook via het LSP. Hoe verhoudt dit zich daartoe?

De heer **Raemakers** (D66):
Dat is een goede vraag. Gegevensuitwisseling heeft een positieve kant en een negatieve kant. Op dit moment wordt in de zorg nog heel veel informatie met een fax vervoerd. Hierdoor worden in de eerste plaats patiënten niet op tijd geholpen, wat gezondheidsrisico of gezondheidsschade voor de patiënt kan betekenen. In de tweede plaats zie je dat er bij medewerkers in de zorg, omdat informatie via een fax wordt gedeeld of via andere, bijna middeleeuwse methoden, meer risico ontstaat op medische fouten. Dus ja, dat moeten we aanpakken. Ik blijf natuurlijk achter die motie staan dat de regering ook op dat gebied niet kan zeggen: dat laten we aan het zorgveld over en wij gaan verder niets doen om dat aan te jagen. Ik heb afgelopen jaar tegen minister Bruins gezegd dat ook daarin de minister een rol heeft om te zorgen dat het beter gaat. Maar ook bij de negatieve zijde van gegevensuitwisseling en de risico's die er zijn, vind ik dat deze regering daar meer aan moet doen. Deze regering moet meer doen aan de positieve kant van gegevensbescherming, maar ook aan de risico's. De Autoriteit Persoonsgegevens heeft het afgelopen jaar al meerdere malen gewaarschuwd voor de risico's die er zijn. Van de minister wil ik weten wat hij eraan gedaan heeft en of we er wel genoeg aan doen. Ik heb ook een aantal vragen gesteld waarmee ik wil zeggen dat ook dat echt een tandje sterker mag.

Mevrouw **Van Kooten-Arissen** (PvdD):
Dat zijn heel veel woorden, maar het is geen antwoord op mijn vraag. Het gaat mij erom dat D66 ook nu zegt: hoe kunnen mensen nu vertrouwen hebben dat hun medische gegevens veilig zijn? Als D66 zegt dat veiligheid en vertrouwen eerst komen, absolute veiligheid dus, hoe kan D66 dan willen dat het delen van medische gegevens op een elektronische manier via het LSP, wat volgens experts niet in overeenstemming te krijgen is met het medische beroepsgeheim en de privacywetgeving, verplicht wordt gesteld?

De heer **Raemakers** (D66):
Twee dingen. In de eerste plaats geldt veiligheid als absolute randvoorwaarde voor iedere stap die we hier nemen. Ik bedoel met veiligheid dat gegevens niet in verkeerde handen kunnen vallen. Maar veiligheid heeft ook betrekking op patiëntveiligheid. Daar waar er nu situaties zijn dat verouderde technieken zorgen voor een onveilige situatie, vinden wij dat ook niet goed.

Dan het tweede deel van mijn beantwoording. D66 vindt eigen keuzevrijheid heel belangrijk. Wij willen dat patiënten zelf kunnen aangeven waarvoor zij wel en geen toestemming geven. Daarvoor is een systeem van gespecificeerde toestemming voorgesteld. Dat dreigde te verzanden in een systeem van 160 hokjes. Daarvan hebben wij gezegd dat dit simpeler moet kunnen. Ook daar zien wij voor de regering een taak om ervoor te zorgen dat iedere burger in Nederland zelf kan kiezen of hij überhaupt patiëntgegevens wil delen en als hij dat wil, welke dan. Wij vinden dat de regering hier meer stappen in moet zetten.

De **voorzitter**:
Dank u wel. We gaan luisteren naar mevrouw Kuiken van de fractie van de Partij van de Arbeid.

Mevrouw **Kuiken** (PvdA):
Voorzitter. Het gaat hier om hele kwetsbare, hele jonge kinderen, waarvan hele intieme, hele persoonlijke en hele nare gegevens op straat hebben gelegen. Dat is natuurlijk schandalig. Daarover zijn we het met de hele Tweede Kamer denk ik eens. Het lek is nu gedicht, maar we weten niet of er schade is ontstaan, omdat we simpelweg niet weten wie op welk moment over deze data heeft kunnen beschikken. Het is wel heel goed dat er onderzoek is gedaan. Ik ben de klokkenluiders en RTL dan ook dankbaar dat ze dit onderzoek hebben gedaan en ook voor de wijze waarop ze vervolgens de gegevens hebben beschermd. Want keer op keer blijkt dat we dit soort onderzoeken nodig hebben om dit soort lekken boven water te krijgen. Terwijl er eigenlijk geen raketgeleerdheid voor nodig is om te beseffen hoe je gegevens veilig houdt, is het heel ingewikkeld. We hebben allemaal heel ingewikkelde wetsvoorstellen. We hebben allemaal heel ingewikkelde regelgeving en uiteindelijk gaat het om zoiets simpels als het niet laten verlopen van een domeinnaam, of het niet via WhatsApp delen van gegevens of het niet open laten liggen van de gegevens. Uiteindelijk komt het allemaal weer neer op het boerenverstand gebruiken, ook als het gaat over informatiedeling.

Ik heb daarom een paar simpele vragen. Toen dit nieuws naar buiten kwam, was mijn eerste gedachte: ik hoop dat er een heel belteam op het ministerie 24 uur bezig is om alle zorginstellingen in Nederland te bellen. Ik hoopte dat ze zouden vragen: wat heb je de afgelopen tijd verkocht, heb je een veiligheidsfunctionaris, heb je gecheckt of je zo'n zelfde lek hebt? Dat is de urgentie die ik nu mis. Er worden wel een aantal onderzoeken aangekondigd, maar ik heb geen enkele garantie dat wat er nu boven tafel is gehaald, in de tussentijd niet ergens anders ook is gebeurd.

Ik zag Amsterdam een melding doen op de eigen site "wij voldoen aan alle regels rondom privacy". Maar welke garanties heb ik daarvoor? Welke garanties heeft de minister daarvoor? Geen enkele volgens mij, omdat we het simpelweg niet weten. Dat was mijn eerste vraag, voorzitter.

Mijn tweede vraag is: wie is er verantwoordelijk op het moment dat het misgaat met diezelfde veiligheid? Is dat de bestuurder van een zorginstelling? Welke rol speelt de raad van toezicht daarin? Op welk niveau ben je als individu aansprakelijk en op welke wijze vindt dat plaats?

Mijn laatste vraag hebben alle andere partijen ook gesteld. Waarom gunnen we zorginstellingen nog zoveel vrijblijvendheid als het over zulke gevoelige informatie gaat? Waarom wordt men niet verplicht om via een aantal informatieprotocollen te werken? Of dat nu via systeem A of systeem B is, of via systeem Z, dat vind ik niet zo relevant. Maar die vrijblijvendheid zou er toch eigenlijk niet meer mogen zijn. Om welke informatie het ook gaat, of het gaat over de medische dossiers of over de mentale dossiers: het zou altijd op orde moeten zijn.

Daarmee rond ik af. Het ging hier om hele kwetsbare kinderen, die heel erg afhankelijk zijn van ons en van het systeem en die zich vaak een nummer voelen in het systeem. Het zijn kinderen die van zorgverlener naar zorgverlener gaan, van hulpverlener naar hulpverlener en nu blijken ze weer een nummer, omdat hun dossiers niet veilig zijn en omdat ze doorgeschoven worden zonder dat iemand checkt of dat wel op een goede manier gebeurt. Dat vind ik zorgwekkend, teleurstellend en heel schandelijk, voorzitter.

Dank u wel.

De **voorzitter**:
Dank u wel. De laatste spreker van de zijde van de Kamer is de heer Peters van de fractie van het CDA.

De heer **Peters** (CDA):
Dank u wel, voorzitter. Een datalek bij het voormalige Bureau Jeugdzorg in Utrecht. De meest gevoelige informatie van de meest kwetsbare kinderen is in handen gekomen van derden. Misschien heeft dat nu direct niet de allergrootste gevolgen, maar dat ligt aan de manier waarop de klokkenluiders en in dit geval RTL4 met de informatie zijn omgegaan. Maar toch: het is erg. Het is heel erg en ik kan mij voorstellen hoe cliënten van jeugdzorg en hun ouders en familie hiervan geschrokken zijn. Maar ook de verantwoordelijke instellingen zelf. Dit is natuurlijk het laatste wat je als organisatie wilt. Ik heb dan ook direct schriftelijke vragen gesteld. Ik dank de minister voor de beantwoording daarvan. Toch heb ik een aantal voor de hand liggende vragen.

Ten eerste. Kan de minister bevestigen dat die gevoelige informatie van kinderen echt niet op straat is komen te liggen? Heeft echt niemand inzicht gehad in die dossiers? Twee. Kan de minister bevestigen dat ouders en kinderen hiervan op de hoogte zijn gesteld en dat hun eventuele zorgen op dat vlak zijn weggenomen? En kan de minister bevestigen — mevrouw Kuiken van de Partij van de Arbeid vroeg dat ook — dat de oorzaak van het datalek duidelijk is en dat verdere lekken niet meer mogelijk zijn? Niet hier en op deze manier ook niet bij andere organisaties?

Voorzitter. Niemand wil datalekken, zeker niet van zulke gevoelige informatie en zeker niet van informatie die beschadigend zou kunnen zijn voor kwetsbare kinderen en hun familie. Wij willen dat voorkomen, al kan dat nooit voor 100%. Het liefste willen we de verantwoordelijken daarvoor vinden en aanpakken. De PVV wil de hele instelling onder verscherpt toezicht stellen. Die neiging is natuurlijk menselijk, maar misschien niet per se de juiste. Het is verleidelijk vanuit emotie en betrokkenheid vanuit deze Kamer op te roepen tot het maken van nieuwe regels om nieuwe lekken uit te sluiten, en om 100% garantie te vragen. Maar de vraag is of dat kan. De vraag is ook of nieuwe regels wel helpen en of die niet gewoon nieuwe, extra bureaucratie met zich meebrengen. Wij noemen dat ook wel de zogenaamde risicoregelreflex. Daarom de volgende drie vragen aan de minister. Ten eerste: zijn er nieuwe regels nodig om lekken zo veel mogelijk te voorkomen? Of, vraag twee, zijn de huidige regels en richtlijnen eigenlijk wel voldoende maar moeten ze gewoon worden nageleefd? Het gezond verstand. Waarom sturen we platte mails met teksten? Daar hoef je geen regels voor te hebben; dat moet je gewoon niet doen. Of hebben we in dit geval te maken met een mogelijkheid waar gewoon niet aan gedacht is, is het lek dichten voldoende en is er sprake van een incident? Dat geloof ik niet, maar dat vraag ik toch.

Voorzitter. Ook de roep om verantwoordelijken of schuldigen te zoeken, is menselijk maar niet per se constructief. Niemand wil deze lekken, en al helemaal niet de mensen die zijn aangesteld om de veiligheid van kinderen te waarborgen. Extra regels, in combinatie met extra drukke professionals, zorgden in het verleden — zie bijvoorbeeld het Maasmeisje — tot risicomijdend gedrag, het nemen van extra maatregelen, meer ots en een toename van bureaucratie, omdat professionals in ieder geval wilden aantonen dat ze in juridische zin geen fouten maakten. Het heeft gewoon niet geleid tot betere zorg. Het CDA pleit voor het oplossen van het probleem, voor rust en het gebruik van het gezond verstand, en voor leren in plaats van afstraffen.

Voorzitter. Dan het element van de privacy. Even los van deze casus kan het belang van goed omgaan met informatie nauwelijks worden overschat. Al moet een al te grote nadruk op privacy, zeker in de zorg, geen excuus worden om helemaal niet meer samen te werken. Hier en daar is dat wel het geval. We sturen met z'n allen — dat zeggen we tenminste- al sinds de jaren zeventig op één gezin en één plan. Maar door een ongezonde fetisj op rechtmatigheid is dat inmiddels al onmogelijk geworden. U krijgt de best mogelijke hulp voor ieder deelprobleem en helemaal niet de best mogelijke totaaloplossing. Een diepgekoesterde wens sinds de jaren zeventig is op deze manier gewoon niet mogelijk, ook al roepen we hier van wel. Het is gewoon niet mogelijk. Maar als door een nog grotere nadruk op verkeerd begrepen privacy alle hulpverleners ook nog eens stoppen met elkaar te communiceren, dan hebben we echt het slechtste van alle werelden georganiseerd.

Voorzitter. Voor mij is het helder. Privacy, en dan bedoel ik dus het zorgvuldig omgaan met data en informatie, is van het grootste belang. Maar het CDA wil niet op voorhand nieuwe regels. Het CDA wil geen heksenjacht op verantwoordelijken. Het CDA wil dat fouten worden hersteld, dat ervan wordt geleerd en dat mensen hun verantwoordelijkheid nemen. Voor het CDA gaan een zorgvuldige omgang met data en samenwerking tussen professionals hand in hand. Tot zover mijn eerste termijn.

De **voorzitter**:
Dank u wel. Een vraag nog van mevrouw Westerveld.

Mevrouw **Westerveld** (GroenLinks):
Het CDA lijkt het probleem te bagatelliseren. Ik hoor hier helemaal niet allemaal collega's pleiten voor extra regels. Ik hoor wel collega's zeggen dat we dit serieus moeten nemen. Ik hoor collega's zeggen: wij willen van de minister horen of hij de privacy van andere jeugdigen wel kan waarborgen. Ik zou de heer Peters willen vragen of hij het met mij eens is dat collega's dat vragen aan de minister en niet oproepen tot allerlei extra regels. Want die suggestie wordt hier wel gewekt.

De heer **Peters** (CDA):
Ik leer, voorzitter, ik wacht nu op u. De vorige keer deed ik dat niet, maar nu doe ik het wel.

De **voorzitter**:
Dan kunt u uren wachten.

De heer **Peters** (CDA):
Oké, laten we dat niet doen. Dat ben ik maar gedeeltelijk met u, mevrouw Westerveld moet ik zeggen, eens. Sowieso kan een garantie van de minister vragen dat dingen niet fout kunnen gaan — dat heb ik verschillende keren gehoord — gewoon niet. Kan de minister garanderen dat het niet nog een keer fout gaat? Nou, ik ben de minister niet, maar dat kan hij gewoon niet. Ik heb verschillende mensen horen vragen: hoe kunnen we testen doen om te controleren? Mensen in de krant zetten als ze zich niet aan de regels houden? Ik heb zelfs iemand horen vragen of we de hele instelling niet onder curatele kunnen stellen. Dus ik ben het maar gedeeltelijk met u eens. Ik bagatelliseer het probleem helemaal niet, want privacy is belangrijk en er moet zorgvuldig worden omgegaan met data. Volgens mij is mijn enige stelling dat we heel erg voorzichtig moeten zijn met te concluderen dat er allerlei nieuwe regels voor nodig zouden zijn. Dat is de vraag. Ik denk ook dat we erg voorzichtig moeten zijn met het vragen om garanties, maar dat we gewoon ons gezonde verstand moeten gebruiken, een lerende organisatie moeten kweken en niet mensen achter de vodden zitten die dan straks alleen in juridische zin geen fouten meer gaan maken. Dat hebben we in het verleden vaak genoeg geprobeerd, maar dat werkt niet.

Mevrouw **Westerveld** (GroenLinks):
Het is niet niets wat er is gebeurd. De gegevens van duizenden kinderen liggen op straat. Privacygevoelige gegevens. Zaken als seksueel misbruik, mishandeling en verslaving konden zomaar op straat liggen. Dankzij het handelen van een paar oplettende klokkenluiders en RTL Nieuws is dat niet gebeurd. Dat zou toch reden genoeg moeten zijn om in ieder geval hier als Kamer kritische vragen aan de minister te stellen en niet bij voorbaat te zeggen dat er helemaal geen nieuwe regels moeten zijn?

De heer **Peters** (CDA):
Nee, dat klopt, mevrouw Westerveld. Daarom heb ik de minister ook gevraagd of er nieuwe regels nodig zijn. Maar dat is wel een vraag en geen stelling.

De heer **Edgar Mulder** (PVV):
Er wordt terecht gesteld dat mensen nu eenmaal fouten maken. Dat doet mijn CDA-collega ook. We hebben niet opgeroepen om een instelling onder curatele te stellen, maar we hebben wel opgeroepen tot verscherpt toezicht. Dat lijkt me niet meer dan logisch, tot het moment dat bewezen is dat men daar op een ordentelijke wijze met de privacy van cliënten omspringt.

U hebt het over het gezond verstand. Het lijkt me niet meer dan je gezonde verstand gebruiken om deze organisatie pas weer volledig zelfstandig te laten handelen als die ordentelijke omgang met de privacy gegarandeerd is. Je kunt niet garanderen dat er geen fouten worden gemaakt, maar je kunt wel de huidige fouten eerst oplossen en zorgen dat die geborgd zijn. Dat lijkt me niet meer dan logisch.

De heer **Peters** (CDA):
Daarom heb ik de minister ook gevraagd om te bevestigen dat het lek gedicht is, zoals ik in de brief ook heb zien staan.

De **voorzitter**:
Prima. Ik schors tot 21.00 uur. O nee, toch niet. Meneer Raemakers komt toch nog even uit de bankjes. Dan is er echt iets aan de hand.

De heer **Raemakers** (D66):
De heer Peters zegt: ik vraag de minister of het lek gedicht is. En dat is het dan. De heer Peters is het toch wel met mij eens dat deze minister ook wel een aantal dingen zal moeten doen om dit in de toekomst te voorkomen? Erkent het CDA dat ook?

De heer **Peters** (CDA):
Jazeker. Iedereen moet zich altijd bewust zijn hoe we met die data omgaan, en we moeten allemaal ons gezond verstand gebruiken. Daarom word ik al kriegel van mensen die op hun website zetten dat zij voldoen aan alle privacyregels. Het is allemaal prachtig als je aan die regels voldoet, maar ik wil dat je concreet waarneembaar gedrag vertoont dat erop wijst dat je het serieus neemt. Het antwoord is dus: natuurlijk. Dat vraag ik van de minister, van mijzelf en van iedere instelling. Je moet je niet alleen aan de regels houden maar ook gewoon je gezonde verstand gebruiken, zodat je fatsoenlijk met gevoelige informatie omgaat.

De **voorzitter**:
Afrondend.

De heer **Raemakers** (D66):
Dus de conclusie van het debat van vandaag mag ook wat betreft de heer Peters niet zijn dat het lek gedicht is en dat we dus klaar zijn? Dat begrijp ik goed?

De heer **Peters** (CDA):
Ja, natuurlijk. Dat zou wel heel simpel zijn. Als het lek gedicht is, is dat prima en heel mooi: dan is het urgente probleem opgelost. Maar het belangrijke probleem blijft altijd bestaan.

Wij zullen altijd netjes moeten omgaan met die data, of je nu systeem A, B of C gebruikt. Welk systeem je gebruikt, kan mij niet schelen, zoals mevrouw Kuiken ook zei. Je kunt ze allemaal gebruiken, maar je zult ze niet alleen moeten implementeren, je moet ze gebruiken, je moet het opvolgen. Je moet privacy tot een onderdeel van je hele wezen maken. Dan heb ik het natuurlijk over de veiligheid. Het is geen incident in de zin van: "lek dicht, case closed".

Mevrouw **Tielen** (VVD):
Ik vind het wel interessant dat de heer Peters de vinger precies op de juiste plek legt. Dat zie je aan de reacties uit de zaal en ook aan de mijne. Volgens mij heeft niemand geroepen om extra regels, maar wel om een serieuze omgang met wat er ligt.

Ik heb dus een vraag aan de heer Peters, over twee dingen. Het kan zijn dat het lek gedicht is en dat de minister dat ook kan bevestigen. Ik vind het dan nog steeds belangrijk dat de mensen in het land, die nu toch enigszins ongerust zijn over de veiligheid van hun gegevens, van deze minister wel uitspraken horen die hun ongerustheid weg kunnen nemen. Ook al zijn dat misschien geen garanties. Is de heer Peters dat met mij eens? Dat is het eerste.

Is de heer Peters het ook met mij eens — en dat is het tweede — dat er toch ergens wel een plek moet zijn waar je aan de bel kunt trekken, als je inderdaad denkt dat een organisatie ondanks bijvoorbeeld teksten op de website toch slordig omgaat met persoonsgegevens?

De heer **Peters** (CDA):
Dat ben ik allebei met mevrouw Tielen eens.

De **voorzitter**:
Nou, dan zijn we er toch?

Ik schors tot negen uur en dan gaan we luisteren naar de antwoorden van de minister.

De vergadering wordt van 20.47 uur tot 21.05 uur geschorst.

De **voorzitter**:
Het zou mijn voorstel zijn om er geen nachtwerk van te maken vandaag, maar dat ligt allemaal in uw handen. Het woord is aan de minister.

Minister **De Jonge**:
Voorzitter, dank u wel. Dank voor de inbreng van de Kamer in de eerste termijn. Dank ook voor de vele vragen die, terecht ook, zijn gesteld. Het datalek dat vorige week is ontdekt bij SAVE Midden-Nederland is een ernstige kwestie. Zorgorganisaties moeten zorgvuldig omgaan met persoonlijke gegevens. Zeker kwetsbare kinderen en hun ouders

moeten daarop kunnen vertrouwen. De verhalen die je vertelt en de zorgen die je deelt met medewerkers in de zorg moeten veilig zijn.

Ik denk dat het goed is om de vragen als volgt te beantwoorden. In het eerste blok wil ik ingaan op deze specifieke casus. Wat is daar gebeurd en hoe is er geacteerd in deze specifieke casus bij Samen Veilig Midden-Nederland? In het tweede blok wil ik ingaan op de vraag wat we kunnen doen om de gegevensbescherming in de zorg als geheel te versterken. In het derde blok ga ik in op de overige vragen.

Voorzitter. Eerst de casus, het datalek bij Samen Veilig Midden-Nederland. Een aantal fracties heeft gevraagd naar de feiten als het gaat om wat vorige week is ontdekt en naar de maatregelen die vervolgens zijn getroffen. Eerst de feiten. Op voorhand moet ik zeggen dat het gaat om de feiten zoals die ons nu bekend zijn. Ze worden op dit moment niet voor niets onderzocht door zowel SAVE Midden-Nederland, dat de feiten intern en extern laat onderzoeken, alsook de samenwerkende gemeenten in Utrecht, die een extern onderzoek laten uitvoeren.

Laat ik vooruitlopend op de uitkomsten van die onderzoeken meedelen wat wij op dit moment weten uit navraag bij de gemeente Utrecht en bij SAVE Midden-Nederland. Bij de decentralisatie van de jeugdzorg is Bureau Jeugdzorg Utrecht omgevormd tot SAVE Midden-Nederland. De oude domeinnaam van het voormalige Bureau Jeugdzorg Utrecht is in december 2017 verlopen. In oktober 2018 is die domeinnaam door de melders opgekocht. Door de registratie van deze domeinnaam was er toegang tot dossiers die zijn gemaild, tot interne e-mails met informatie over cliënten en tot voicemailberichten. De partij die de domeinnaam heeft opgekocht, heeft zichzelf gemeld bij RTL Nieuws en via RTL aan de bel getrokken. RTL meldt dat het gaat om dossiers van in totaal 2.700 kinderen.

Het is belangrijk om te onderstrepen dat ik op dit moment geen aanwijzingen heb dat die data terecht zijn gekomen bij andere, onbevoegde personen dan de klokkenluiders en RTL Nieuws. Woordvoerders van een aantal fracties vroegen daarnaar: de heer Mulder, de heer Peters en mevrouw Westerveld. Op dit moment heb ik dus geen aanwijzingen dat die gegevens door anderen zouden zijn ingezien dan door RTL en deze klokkenluiders. Door SAVE Midden-Nederland is nog niet zelf vastgesteld om hoeveel zaken het gaat en welke gegevens men heeft kunnen raadplegen. Daar zijn die onderzoeken voor bedoeld. Zoals gezegd gaat het over een intern onderzoek en een extern onderzoek. Ik zeg daar zo meteen nog wat meer over.

Er is gevraagd wat er de oorzaak van zou kunnen zijn dat door die domeinnaam anderen toegang hebben kunnen krijgen tot wat in die mails beschikbaar was. In antwoord daarop kan ik zeggen dat drie mogelijkheden mogelijk ten grondslag lagen aan het datalek. De eerste mogelijkheid is dat er een tool werd gebruikt, die extern gehost werd, waarmee medewerkers op de hoogte werden gebracht als er iets verandert in een dossier. Daarbij is mogelijk gebruikgemaakt van oude adreslijsten en zijn er dus mails gestuurd naar oude mailadressen. De tweede mogelijkheid is dat accounts in de telefooncentrale van SAVE Midden-Nederland voicemailberichten naar oude mailadressen hebben gestuurd. En een derde mogelijkheid is dat externe partijen cliëntinformatie naar oude e-mailadressen hebben gestuurd. Als je zo'n domeinnaam vervolgens machtigt en een soort catch-allfunctie instelt, betekent dat dat je jezelf vervolgens inderdaad toegang zou kunnen verschaffen tot mails.

Sowieso is er een intern onderzoek gestart naar de oorzaken van het datalek, naar hoe het kan dat de dossiers van cliënten onbeveiligd doorgestuurd konden worden via de mail en naar hoe het kan dat die mailadressen van de oude domeinnaam nog in omloop waren. Waren er nog adreskaartjes? Was er nog ergens foldermateriaal, briefpapier of wat dan ook met oude adressen erop? Of waren er ondertekeningen van e-mails met oude adressen erop? Dat is het interne deel van het onderzoek.

Welke maatregelen zijn er getroffen, zowel door Samen Veilig Midden-Nederland als door de gemeente Utrecht en de Autoriteit Persoonsgegevens, en wat heeft het departement gedaan? Ten eerste is Samen Veilig Midden-Nederland als instelling zelf verantwoordelijk om zich aan de wet te houden en om te zorgen voor een veilige omgang met persoonsgegevens. Die instelling heeft, onmiddellijk nadat zij was ingelicht, een aantal dingen gedaan. Men heeft de domeinnaam teruggekocht en het lek gedicht. Alle mail die naar oude adressen wordt verstuurd, wordt daardoor weer opgevangen door de organisatie Samen Veilig Midden-Nederland zelf. Een aantal Kamerleden heeft daarnaar gevraagd. Twee. De opdrachtgever, de gemeente Utrecht, is, zoals dat hoort, geïnformeerd. Drie. Bij de Autoriteit Persoonsgegevens is, zoals dat hoort en zoals dat ook wettelijk verplicht is, melding gedaan van het datalek. Vier. Er is een intern en een extern onderzoek naar het datalek gestart. Ik noemde net al dat interne onderzoek, maar dat externe onderzoek gaat over de vraag hoe het mogelijk was dat op het oude domein nog mails in te lezen waren. Hoe is dat technisch gegaan? Kan achterhaald worden welke dossiers daardoor daadwerkelijk inzichtelijk zijn geworden? Dat zijn de dossiers die daadwerkelijk als lek moeten worden beschouwd. En kan worden achterhaald — dat is ook belangrijk voor de reactie op de vragen die u heeft gesteld — wie zich toegang heeft verschaft tot deze dossiers? Dat is het externe onderzoek dat zal worden uitgevoerd door Fox-IT.

Dan de cliënten. Daarover is ook een aantal vragen gesteld. Hoe zijn die geïnformeerd? Eén. Op de eigen website is een bericht geplaatst dat regelmatig van updates over deze kwestie wordt voorzien. Twee. Er is een apart e-mailadres en een telefoonnummer geopend waar mensen met vragen en informatie terechtkunnen. Drie. Kinderen en gezinnen worden via dagelijks contact door de organisatie geïnformeerd. De organisatie stuurt informatiebrieven mee met de officiële correspondentie en houdt per cliënt bij of deze brieven ook daadwerkelijk zijn ontvangen. Daarnaast heb ik van de gemeente Utrecht begrepen dat men gezinswerkers van het lokale buurtteam heeft geïnstrueerd om alert te zijn op vragen en zorgen van kinderen en ouders, die zelf te maken hebben gehad met Samen Veilig Midden-Nederland en zorgen hebben over de veiligheid van hun gegevens. Die kunnen eventueel ook ondersteuning bieden bij gesprekken daarover.

Mevrouw **Westerveld** (GroenLinks):
De minister vertelde dat oude domeinnamen zijn opgekocht. Ik vroeg in mijn bijdrage welke domeinnamen er allemaal zijn opgekocht. Is dat breder? Geldt dat voor meer zorgin-

stellingen die van naam veranderd zijn en waarvan de oude domeinnaam is opgekocht? Ik kan me voorstellen dat dit probleem ook breder speelt. Toevallig speelt het nu bij deze jeugdzorginstelling, maar het kan ook breder bij meer zorginstellingen spelen.

Minister **De Jonge**:
Ik heb dat nog niet gezegd, maar ik ga straks wel zeggen dat er ook andere domeinnamen zijn opgekocht. Ik zal dan even toelichten hoe vaak dat is gebeurd. Maar hier had ik het over de domeinnaam die door de klokkenluiders was gekocht. Die is dus onmiddellijk teruggekocht door SAVE Midden-Nederland en zodoende konden ze weer zelf beschikken over de mails die eventueel naar een oud adres zouden zijn gestuurd. Dit is dus de achtergrond en dit zijn de maatregelen die SAVE Midden-Nederland zelf heeft genomen.

Dit raakt allemaal aan de verantwoordelijkheidsvraag die mevrouw Tielen indringend heeft gesteld, en terecht ook. De eerste verantwoordelijkheid ligt natuurlijk bij de instellingen zelf. De tweede verantwoordelijkheid ligt in dit geval bij de gemeenten. Je zou kunnen zeggen: de tweede verantwoordelijkheid ligt bij opdrachtgevers, namelijk om erop toe te zien dat hun opdrachtnemers zich verhouden tot alle wettelijke bepalingen; ik kom daar zo op terug. In dit geval is de gemeente Utrecht, of zijn de gezamenlijke Utrechtse gemeenten, opdrachtgever van SAVE Midden-Nederland. De Utrechtse gemeenten hebben zeer alert gereageerd. Zij hebben het bestuur en de raad van toezicht van Samen Veilig Midden-Nederland meteen ter verantwoording geroepen. Naast het onderzoek dat SAVE uitvoert en het onderzoek dat in opdracht van SAVE extern wordt uitgevoerd door Fox-IT, gaan de betrokken 26 Utrechtse gemeenten ook zelf een onafhankelijk onderzoek laten uitvoeren naar hoe het er met de persoonsgegevens en de privacy aan toegaat bij SAVE, en of daar nog meer noodzaak tot ingrijpen is. Ook heeft de gemeente Utrecht aan al haar gecontracteerde zorgaanbieders, zowel jeugd als Wmo, opdracht gegeven om aan te tonen hoe zij ervoor zorgen dat privacygevoelige informatie van hun cliënten voldoende beschermd is. Dus niet alleen uw Kamer maar ook gemeentebesturen, gemeenteraden, zitten erbovenop. Het debat dat wij hier vanavond voeren, wordt morgen in de gemeenteraad in Utrecht gevoerd. Daartoe is vandaag een brief gestuurd door de gemeente Utrecht aan de raad van Utrecht.

De heer **Hijink** (SP):
Ik hoor de minister zeggen dat na de organisatie zelf de gemeente, als opdrachtgever voor de jeugdzorg, eigenlijk de eerstverantwoordelijke is voor goede databeveiliging. Nu vraag ik me het volgende af. We hebben vanmiddag een debat gehad over misstanden in de jeugdzorg, over hoe de kwaliteit vaak nog achterblijft en de gemeente eigenlijk te weinig toezicht houdt en daar soms ook echt niet goed toe in staat is. Denkt de minister nu echt dat gemeenten in staat zijn om toezicht te houden op de manier waarop zorginstellingen, jeugdzorginstellingen in dit geval, hun data beveiligen? Ik acht gemeenten hoog, maar ik vraag me toch echt af of zij daartoe in staat zijn.

Minister **De Jonge**:
Ik denk dat dit een eerste verantwoordelijkheid is van instellingen zelf, een tweede verantwoordelijkheid van de opdrachtgevers, een derde verantwoordelijkheid van de toezichthouders en een vierde verantwoordelijkheid van de stelselverantwoordelijke. Ik wil eigenlijk alle verantwoordelijkheden nalopen in deze casus. Daarna, in het tweede blok, wil ik alle verantwoordelijkheden nalopen voor wat we in den brede richting de zorg kunnen doen. Ik denk dat je als opdrachtgever weliswaar allicht niet op alles kunt sturen, maar bijvoorbeeld via contractuele bepalingen behoorlijk goed kunt sturen op het naleven van veiligheidsvereisten. Dat klopt. Ik denk dat. Tegelijkertijd is het inderdaad zo dat een gemeente, of een opdrachtgever — in een ander stelsel is dat een zorgkantoor of een zorgverzekeraar — er niet bij is; je staat niet naast alle zorgverleners op het moment dat daar informatie wordt uitgewisseld. In je opdrachtgeversrol kun je inderdaad de uitvoeringspraktijk versterken, maar daarmee kun je in je eentje die toezichtsverantwoordelijkheid niet waarmaken. Daarom zeg ik ook: het is een eerste verantwoordelijkheid voor instellingen, het is een verantwoordelijkheid voor opdrachtgevers, het is een verantwoordelijkheid voor toezichthouders, de AP in eerste instantie en daarnaast ook een verantwoordelijkheid bij de IGJ — ik kom daar allemaal zo op — en het is ook een verantwoordelijkheid voor het Rijk als stelselverantwoordelijke. Als je die stappen wilt zetten in de uitvoeringspraktijk richting veiligheid, kun je de verantwoordelijkheid pas daadwerkelijk waarmaken als alle vier die verantwoordelijkheidslagen, zo zou je kunnen zeggen, doen wat er van ze mag worden verwacht.

De heer **Hijink** (SP):
Volgens mij raakt dit precies de kern van het probleem: er zijn zo veel lagen verantwoordelijk dat uiteindelijk niemand zich verantwoordelijk voelt. Ik vermoed dat dat voor de rest van de zorgsector ook geldt.

Minister **De Jonge**:
Dat is niet waar.

De heer **Hijink** (SP):
Wat er dan dus gebeurt, is dit. Als zich dan een incident voordoet, en als er een datalek is, komen wij er altijd pas nadien achter. Er komt dus nooit — ik heb dat niet eerder gehoord — vanuit een inspectie, vanuit de Autoriteit Persoonsgegevens, vanuit een gemeente of van wie dan ook, naar buiten: wij hebben deze organisatie op de vingers getikt omdat daar risico's waren. Dus wat gebeurt er in de zorg, altijd? Een datalek wordt gemeld, en dan schreeuwt iedereen moord en brand. Dat is natuurlijk precies het probleem. Vooraf houden wij, in mijn ogen, veel te weinig toezicht. We doen steekproefsgewijs veel te weinig onderzoek bij zorginstellingen: hebben zij die beveiliging wel op orde? Dat is bij deze instelling ook niet gebeurd.

Minister **De Jonge**:
Ik ben minder somber. Maar ik kom zo toe aan de verschillende verantwoordelijkheden en wat er mag worden verwacht per verantwoordelijke. Ik heb in mijn eigen wethouderspraktijk gezien hoe je inderdaad tegen informatiebeveiligingskwesties kunt aanlopen en hoe je als opdrachtgever

wel degelijk daarin kun sturen. Ik kom er zo nog uitgebreider op terug, maar een voorbeeld is de mail. Wij hebben daar een landelijke stelselverantwoordelijkheid in. Maar een heel directe verantwoordelijkheid ligt bij de opdrachtgever. Je kunt namelijk gewoon contractueel afspreken met alle instellingen die een contract hebben met de gemeente dat men gebruikmaakt van beveiligde mailverbindingen.

Kijk hoe de gemeente heeft geacteerd in dit concrete geval. De gemeente heeft niet alleen SAVE Midden-Nederland aangesproken, maar heeft vervolgens al haar gecontracteerde Wmo- en jeugdhulpaanbieders aangesproken om iets te doen met de lessen die hier geleerd kunnen worden, om zichzelf te evalueren, om maatregelen te treffen. Zo zie je dus, denk ik, dat het juist nodig is dat alle partijen op hun eigen speelveld en met hun eigen invloedsfeer doen wat er van ze mag worden verwacht.

Werkgevers hebben daarin een taak in de richting van hun eigen mensen. Dat is de eerste taak. Je zou ook kunnen zeggen dat dat de makkelijkste taak is, want die ligt het dichtst bij de echte uitvoeringspraktijk. Opdrachtgevers hebben daarin een taak in de richting van die werkgevers. Toezichthouders hebben daarin een taak, maar het is ook onmogelijk, met 1,3 miljoen mensen in de zorg, om naast iedere medewerker een toezichthouder te zetten. Maar een toezichthouder is wel heel erg belangrijk, zeker ook een toezichthouder die consequenties verbindt aan het toezicht dat wordt gehouden. En het Rijk heeft een stelselverantwoordelijkheid. Ook daarin hebben we ondersteunend te zijn. Dat doen we ook. Er is nog meer te doen en daar kom ik zo meteen op terug.

De **voorzitter**:
Zullen we even doorgaan, meneer Raemakers?

De heer **Raemakers** (D66):
Nee, dit gaat echt over een principiële vraag. De minister schetst het systeem. Hij zegt dat je opdrachtgevers, instellingen en toezichthouders hebt en het ministerie als stelselverantwoordelijke. Dit is een heel belangrijke vraag. Ik heb natuurlijk de summiere Kamerbrief van maandag heel goed gelezen. Daarin stoort het mij dat de minister heel erg de verantwoordelijkheid neerlegt bij Jeugdzorg Nederland. De minister schrijft dat hij Jeugdzorg Nederland heeft gevraagd om dringend het belang bij de leden aan te stippen en om aanvullende maatregelen te nemen en dat hij Jeugdzorg Nederland gevraagd heeft om hem rond de zomer te informeren. Ik hoor "Jeugdzorg Nederland" nu niet meer in het rijtje. Volgens mij is dat ook terecht. Begrijp ik dus goed dat de minister nu terugkomt op zijn Kamerbrief van maandag waarin hij Jeugdzorg Nederland een wel heel grote rol toedicht?

Minister **De Jonge**:
Nee, dat begrijpt de heer Raemakers niet goed. Ik ben begonnen met het uitdiepen van de casus: wat zou hier gebeurd kunnen zijn; wat weten we op dit moment? Vervolgens heb ik toegelicht wat de rol is geweest van SAVE Midden-Nederland nadat die casus naar boven kwam en welke acties zij hebben ondernomen. Het tweede blokje betrof de rol van de samenwerkende Utrechtse gemeenten en de acties die zij hebben ondernomen. Ik zou nu aankomen bij de Autoriteit Persoonsgegevens als toezichthouder en daarna toekomen aan wat ik als minister heb gedaan, als stelselverantwoordelijke. Daarbij heeft inderdaad Jeugdzorg Nederland een rol, maar niet als enige. Het is dus niet een kwestie van de taak op het bord van een ander leggen, maar het is wel een kwestie van ieders rol daadwerkelijk gebruiken. Want ik denk dat we ieders rol kunnen benutten om te zorgen voor een betere gegevensbescherming.

Ik kom er dus zo op. Als u het goedvindt, behandel ik eerst de Autoriteit Persoonsgegevens en kom ik zo te spreken over de rol die wij als ministerie te spelen hebben.

De heer **Raemakers** (D66):
Het is wel een principieel puntje. Want als er een Kamerbrief uitgaat, wordt die in het hele land meegelezen. Het kan een verkeerd beeld bij de sector wekken als er in een Kamerbrief helemaal niets wordt vermeld over de stelselverantwoordelijkheid van het ministerie, terwijl wij daar wel naar vroegen, en als de regering schrijft "we hebben Z-CERT, we hebben de inspectie, we hebben de Autoriteit Persoonsgegevens, en, oh ja, heel veel dingen gaan we bij Jeugdzorg Nederland neerleggen". Is de minister dat met mij eens? De sector wil natuurlijk graag gesteund worden door het ministerie. Maar met een Kamerbrief als die van afgelopen maandag voelt de sector zich absoluut niet gesteund.

Minister **De Jonge**:
Nee, dat ben ik niet met u eens. Dat vind ik ook een vreemde voorstelling van zaken. Jeugdzorg Nederland is een brancheorganisatie. Bij de totstandkoming van bijvoorbeeld Z-CERT hebben brancheorganisaties een heel belangrijke initiërende rol gespeeld. Ik kom zo nog terug op Z-CERT en wat de daar de rol voor de toekomst zou kunnen zijn. Maar Z-CERT is juist geboren uit de actie van een aantal brancheorganisaties, in samenwerking met het ministerie.

Daarin trek je samen op en dat is ook logisch. Alle werkgeverstaken die een zorgsector aangaan, zijn per definitie ook de taken die een brancheorganisatie op zich heeft te nemen. En het is dus logisch dat ik Jeugdzorg Nederland aanspreek op het aanspreken van haar leden. Daarmee zeg ik niet: nu is de klus voor jullie en blijf ik langs de kant staan. Integendeel! Als u dat eruit heeft begrepen, is dat geenszins mijn bedoeling geweest. Nee, we hebben juist heel veel te doen, zoals ik zo ook zal schetsen, niet alleen in deze casus, maar juist ook in de zorgsector als geheel.

Ik was bij de Autoriteit Persoonsgegevens gebleven, de derde laag, de laag van de toezichthouders. Bij misstanden in de verwerking van persoonsgegevens is de Autoriteit Persoonsgegevens, de AP, de aangewezen toezichthouder, wettelijk bepaald. De AP houdt toezicht op naleving van de Algemene verordening gegevensbescherming, de AVG. De AP is op dit moment bezig met het verzamelen van feiten rond de inbreuk en staat in contact met Samen Veilig Midden-Nederland. Van Samen Veilig Midden-Nederland en de AP begrijp ik dat gedurende het onderzoek de eerste resultaten alvast worden gedeeld. Dat betekent ook dat de AP zich een beeld kan vormen van wat zich hier heeft voorgedaan. Dan is het aan de onafhankelijke toezichthouder welke vervolgstappen men hierin neemt. Daar kan ik niet op vooruitlopen.

Dan de rol van de minister, zeg ik in de richting van de heer Raemakers. Die is inderdaad stelselverantwoordelijke. Daar loop ik niet voor weg. Sterker nog, wij hebben onze stelselverantwoordelijkheid genomen in deze casus. We hebben die in het verleden ook breed genomen en we zullen die ook gaan nemen in de toekomst. Allereerst hebben we uiteraard navraag laten doen bij SAVE Midden-Nederland, dat in eerste instantie verantwoordelijk is. We hebben alle feiten zo goed mogelijk in beeld gebracht en onszelf de vraag gesteld of de actoren hier hebben gedaan wat er van de verschillende actoren verwacht mag worden. We hebben geconstateerd dat dat zo is. Er zijn allemaal onderzoeken uitgezet: bij SAVE Midden-Nederland intern, bij SAVE Midden-Nederland extern, bij de samenwerkende gemeenten in Utrecht, en daarnaast bij de toezichthouder op de AVG, de Autoriteit Persoonsgegevens. Daar wordt allemaal onderzoek gedaan.

Daarop vooruitlopend heb ik Jeugdzorg Nederland vorige week vrijdag het volgende gevraagd. Allereerst heb ik gevraagd om het belang van goede gegevensbescherming onder de aandacht te brengen van hun leden en om hun eigen gegevensbescherming te evalueren. Dat is noodzakelijk, want het begint ermee dat instellingen zich ervan bewust worden of wat in Utrecht is gebeurd, bij hen ook kan gebeuren. Dat is ook een beetje hoe wij hier dit Kamerdebat voeren, geschrokken van wat er gebeurd is. Je wilt nagaan of dit ook elders kan gebeuren. Het is toch een beetje een wake-upcall, ook voor ons. Voor hen zou het dat ook moeten zijn. Dat is het eerste. Ten tweede heb ik Jeugdzorg Nederland gevraagd om risico's in kaart te brengen en op basis van die geconstateerde risico's aanvullende maatregelen te nemen. Ten derde heb ik, vooruitlopend op de uitvoering van de motie-Ellemeet — ik kom zo terug op wat we in de breedte zouden moeten doen — gevraagd om te bevorderen dat hun leden zich aansluiten bij Zorg-CERT, het Zorg-Computer Emergency Response Team. Dat is hét cybersecuritycentrum voor de zorg, zou je kunnen zeggen. Het helpt bij ICT-incidenten, zowel bij het voorkomen als bij het blussen van de brand. Ik heb Jeugdzorg Nederland gevraagd om mij voor 1 juli te informeren over de uitkomsten van die acties. Men heeft vandaag een algemene ledenvergadering gehad waar dit ook besproken is. Ik ga de uitkomsten van die algemene ledenvergadering op korte termijn bespreken met Jeugdzorg Nederland. Dat doe ik ook met de VNG, om te kijken wat we in de jeugdzorgsector, nog voor alle onderzoeken zijn afgerond, al aan extra stappen zouden kunnen zetten om de jeugdzorgsector alerter en waakzamer te maken op gegevensbescherming.

Als laatste heb ik Zorg-CERT gevraagd om passende actie te ondernemen. Dat is de vraag die mevrouw Westerveld net herhaalde, en ik geloof dat ook Raemakers daarnaar gevraagd heeft in eerste termijn. We hebben Zorg-CERT vrijdag gevraagd of er nog meer domeinnamen zijn die ooit bij een instelling hoorden, terwijl de instelling inmiddels van naam is veranderd en een nieuwe domeinnaam heeft, waardoor die domeinnamen zijn vrijgekomen. Hebben we daar een beeld van? En als we daar een beeld van hebben, kunnen we dan alsjeblieft dat gat meteen dichten? Want nu dit nieuws naar buiten is gekomen, kan het ook voor een niet-goedbedoelende hacker een idee zijn om zo'n domeinnaam te registreren, met alle ellende van dien. We weten nu wat ervan kan komen. Op dat verzoek heeft Zorg-CERT alle domeinnamen geregistreerd van andere instellingen die bekend zijn en vrij zijn gekomen. Daarmee zijn ze dus niet meer beschikbaar voor anderen.

De heer **Edgar Mulder** (PVV):
Interessant wat de minister zegt. Zou hij kunnen toelichten hoe Z-CERT bijdraagt aan het voorkomen van problemen? Het blussen van de brand, snap ik, maar het voorkomen.

Minister **De Jonge**:
Zeker. Als je kijkt wat men doet, dan is dat een breed takenpakket. Daarbij kan men helpen bij het dichten van datalekken die kunnen ontstaan, maar men kan ook helpen met nadenken over manieren om een datalek te voorkomen. Een van de rollen die Zorg-CERT heeft gekregen en nu ook al echt speelt in de ziekenhuiswereld, die nog vatbaarder is voor cyberaanvallen dan welke andere zorginstelling dan ook, is werken met ervaringen met hackers, datalekken of cyberattacks op het internet. Als een aangesloten instelling die heeft, dan meldt die dat bij Zorg-CERT. Die zorgt dan niet alleen dat er wordt meegedacht met die instelling, maar ook dat andere aangesloten instellingen alert zijn op het voorkomen van die inbreuk. Kortom, een gebleken lek of cyberattack bij de ene instelling is tegelijkertijd weer een les voor andere instellingen. Zo zorgt Zorg-CERT voor continue waakzaamheid en alertheid, ook in het voorkomen ervan. Daarmee is de vergelijking met de brandweer eigenlijk heel erg goed: de brandweer blust niet alleen, maar leert ook van brandonveiligheid in het ene gebouw om daarmee de brandveiligheid in een ander gebouw te bevorderen. Dat is een beetje wat Zorg-CERT doet.

De heer **Edgar Mulder** (PVV):
Dat zijn een hoop woorden, maar als dit het dus is — een preventieve werking op mogelijke datalekken en cyberattacks — dan is een abonnement op Zorg-CERT even waardevol als een abonnement op Computer!Totaal. Want daarin staat ook voortdurend een opsomming van datalekken die er zijn geweest. Als het alleen een doorgeeffunctie is, dan snap ik niet waarom dat hoge bedrag betaald moet worden. Als u echt een oplossing zou willen zoeken, zeg ik via de voorzitter, dan vind ik dat iedere organisatie met een substantiële infrastructuur waarop een applicatielandschap draait, een eigen CERT zou moeten hebben. Dat zou dan toch veel beter zijn?

Minister **De Jonge**:
Laten we nou niet badinerend doen over dit type initiatieven. U mag aannemen dat grotere zorginstellingen en ziekenhuizen die te maken hebben met heel veel gevoelige gegevens, buitengewoon goed in staat zijn hun eigen ICT-infrastructuur op een veilige manier te doen te onderhouden, zich te wapenen tegen cyberattacks en wat dies meer zij. Daarnaast hebben de NVZ (Nederlandse Vereniging van Ziekenhuizen), GGZ Nederland en het departement gezamenlijk gekozen — en dat is juist iets heel moois — om per 1 januari 2018 een cybersecuritycentrum in het leven te roepen speciaal gericht op de zorg, waarin alle kennis wordt gebundeld van beveiliging, datalekken, gegevensbescherming en cyberattacks. Daar wordt kennis continu up-to-date gehouden en beveiligd gedeeld, omdat het type hacks en het type data-inbreuken ook veranderen. Dat zijn ook mensen met veiligheidsscreeningen natuurlijk. Dat type kennis

is uniek. Ik denk dat het goed is dat de zorgsector juist zichzelf in bescherming neemt en op deze manier voor zichzelf die brandweerfunctie heeft gecreëerd. De vraag die zich hierbij voordoet, is waarom de jeugdzorgsector daar eigenlijk niet allang op is aangesloten. De motie-Ellemeet is een zeer terechte motie geweest. Daar ga ik ook graag mee aan de slag. Collega Bruins is daarmee aan de slag. Ik zou eigenlijk denken dat de vraag was te onderzoeken of niet alle instellingen aangesloten zouden moeten zijn op Zorg-CERT. Eerlijk gezegd denk ik dat dat vooral een vraag is van "hoe" en niet zozeer van "of". Want dat we instellingen vragen zich aan te sluiten bij Zorg-CERT, zodat men ook telkens alert kan blijven, is volgens mij iets wat je moet willen. De vraag is hoe we dat op zo'n manier doen dat het niet leidt tot enorme kosten en dat het hanteerbaar te maken is. We hebben natuurlijk duizenden, tienduizenden zorginstellingen, dus het moet ook allemaal behapbaar blijven. Eerlijk gezegd denk ik dat we vooral de vraag van het hoe te onderzoeken hebben en niet zozeer de vraag van het of.

De heer **Edgar Mulder** (PVV):
De PVV stelde in haar bijdrage dat Z-CERT een brandweer is: blussen achteraf. De minister stelt: nee, er wordt ook iets gedaan "om te voorkomen". Op mijn vraag wat er wordt voorkomen, antwoordt de minister dat het alleen het doorgeven van datalekken betreft die ergens anders hebben plaatsgevonden. Dan zeg ik: dat kun je ook gewoon op het internet vinden of in een goed computertijdschrift. Wat dat betreft blijf ik erbij dat Z-CERT een brandweerfunctie heeft. Die moeten we niet onderschatten, maar het is geen oplossing voor de problemen die er zijn met het beschermen van data.

Minister **De Jonge**:
Ik deel niet wat de heer Mulder hier zegt.

De heer **Raemakers** (D66):
Ook ik heb een vraag over Z-CERT. Ik ben wel verbaasd dat het kabinet de motie-Ellemeet nodig heeft om dit een belangrijk thema te vinden. Je zou toch mogen verwachten dat men hier al langer mee bezig is. Dus ik zou ook de minister willen vragen hoeveel geld er vanuit het ministerie naar Z-CERT gaat. Hoeveel mensen werken er bij Z-CERT? Is dat in zijn ogen voldoende om de uitdagingen die nu allemaal op het bordje van Z-CERT worden gelegd, te kunnen dragen?

Minister **De Jonge**:
Ik heb aangegeven dat de motie-Ellemeet is ingediend in een ander debat, met collega Bruins. Die motie stelt een buitengewoon reële vraag, namelijk: zouden eigenlijk niet alle zorginstellingen aangesloten moeten zijn op Z-CERT? Zou dat ook geen verplichtende aansluiting moeten zijn? In deze tijd, waarin ICT-veiligheid en databescherming zo'n belangrijke en steeds grotere rol spelen, zou je eigenlijk moeten zeggen: dat is wel heel erg logisch. De vraag gaat vooral over het hoe. Hoe stel je die wettelijke verplichting dan? Wat zijn de implicaties van zo'n wettelijke verplichting? Geldt dat voor alle tienduizenden instellingen in de zorg? En als je dat doet, wat betekent dat dan vervolgens voor de organisatie? Het is nu natuurlijk een kleine organisatie, en dat zou dan heel veel groter moeten worden. Maar hoeveel groter dan? Kunnen we dat dan behappen? En welke taken kun je dan wel en niet van ze vragen? Mijn indruk is dat we van de motie van Corinne Ellemeet moeten zeggen dat niet zozeer de vraag is "of" maar vooral "hoe". Ik wil u — ik meen dat het een vraag van u of van mevrouw Tielen was — voorstellen om daar voor de zomer nog op terug te komen. Dan kan ik ook aangeven wat daarvan de implicaties zijn, ook voor de omvang.

De heer **Raemakers** (D66):
Dat is geen antwoord op de vraag. Ik heb gevraagd hoeveel budget ernaartoe gaat, hoeveel mensen daar werken en of dat lukt. Misschien kan de minister dat in tweede termijn beantwoorden. Ook wil ik even reageren op het blokje dat de minister nu heeft behandeld. Hij zegt: ik leg een aantal zaken neer bij Jeugdzorg Nederland en verwacht van hen op 1 juli een antwoord. Ik vind dat twijfelachtig; ik ben het daar niet helemaal mee eens. Maar oké, laat ik er even van uitgaan dat Jeugdzorg Nederland op 1 juli 2019 de minister een aantal zaken gaat aanleveren. Kunnen we dan in de zomer, na 1 juli, een aantal cyberexperts en ethische hackers op een aantal jeugdzorginstellingen in Nederland afsturen om te testen of het inderdaad overal veilig is? Wat denkt de minister ervan om dat na 1 juli direct te gaan uittesten?

Minister **De Jonge**:
U kijkt erbij alsof het niet gebeurt. Dat gebeurt namelijk wel. Dat gebeurt overigens niet bij alle instellingen, want het is aan de instelling zelf om de opdracht te geven voor een pentest. Dat heeft overigens niet alleen te maken met data en ICT. Dat heeft ook te maken met de vraag hoe we überhaupt omgaan met gegevensbescherming in ons pand. Dus ook papieren die ergens slingeren waar ze niet horen te slingeren, horen daarin meegenomen te worden. Ik weet dat heel veel gemeenten het doen. Ze worden daarin ondersteund door de VNG. Zorginstellingen doen het ook. Ik vind het eigenlijk een heel goede gedachte om te kijken of we niet een proactiever hulpaanbod moeten bieden in de richting van instellingen. Dat zou bijvoorbeeld een vraag kunnen zijn aan Zorg-CERT. Dat heb ik in die korte tijd tussen de eerste termijn van de kant van de Kamer en de eerste termijn van de kant van het kabinet niet kunnen uitzoeken. Maar het lijkt mij een hele zinvolle vraag, omdat ik denk dat het kan helpen. Ik kom zo bij wat we überhaupt te doen hebben. Dit ging allemaal nog over deze individuele casus en wat we hebben gedaan naar aanleiding van deze individuele casus. Als we straks het blok gegevensbescherming in de zorg überhaupt doornemen, denk ik dat het goed is als we kijken wat we vanaf hier zullen moeten doen. Deze vraag heb ik gesteld aan Jeugdzorg Nederland. Daar ga ik met de VNG en met Jeugdzorg Nederland over in gesprek. Uw vraag of we niet veel meer zouden moeten doen met pentesten en of dat niet heel behulpzaam is om instellingen continu waakzaam en alert te maken, zou ik daar heel graag in meenemen, omdat ik denk dat het een heel zinvolle suggestie is.

De heer **Raemakers** (D66):
Maar de minister doet nu weer precies hetzelfde. Hij zegt: instellingen kunnen zelf pentests doen en gemeenten kunnen dat zelf ook doen; ik zal het nog eens onder de aandacht brengen bij Z-CERT en ik zal het nog eens onder de aandacht brengen bij Jeugdzorg Nederland. Maar ik wil dat de

minister ook zelf een aantal zaken gaat testen. Want er kunnen misschien instellingen zijn die zeggen: we hebben helemaal geen behoefte aan die pentest. Er kunnen misschien gemeenten zijn die zeggen: dat speelt niet in onze gemeente. Dus waarom kan de minister niet zelf een aantal ethische hackers inhuren en zelf steekproefsgewijs bij die gemeenten en die instellingen testen of het systeem nou waterdicht is of niet? Daar is hij toch stelselverantwoordelijk voor?

Minister **De Jonge**:
Ja, maar het woord "stelselverantwoordelijkheid" duidt nou juist op stelselverantwoordelijkheid. Het betekent niet dat je ieders verantwoordelijkheid overneemt, en dat maakt u er nu toch een beetje van. Er geldt namelijk gewoon een verantwoordelijkheidsverdeling die ook in de wet is vastgelegd. Die houdt in dat instellingen eerst verantwoordelijk zijn voor gegevensbeheer — en gelukkig maar, want probeer eens uit te rekenen hoe groot het departement zou moeten zijn als we al die verantwoordelijkheid over zouden willen nemen. Dat wil niemand van ons, denk ik. Instellingen zijn dus eerst verantwoordelijk. Vervolgens zijn opdrachtgevers van die instellingen verantwoordelijk. In dit geval zijn dat de gemeenten. In sommige gevallen zijn dat de zorgverzekeraars en in sommige gevallen zijn dat de zorgkantoren. Dat zijn de opdrachtgevers van deze instellingen. Die kunnen via contractmanagement een hele hoop. Ook die pentesten kun je contractueel afspreken. Daarnaast hebben we toezichthouders. Die toezichthouders hebben toe te zien op datalekken in formele zin. Ik kom straks nog bij de rol van de inspectie. Daarnaast hebben we inderdaad die stelselverantwoordelijkheid. Vanuit die stelselverantwoordelijkheid heb ik Jeugdzorg Nederland afgelopen vrijdag gevraagd om de instellingen te pressen tot alertheid en de risico's in kaart te brengen, en op grond daarvan voor 1 juli met mij te bespreken wat er extra nodig is om aan die risico's inhoud te geven. Ik vind uw suggestie om daarbij pentesten te doen niet alleen een buitengewoon bruikbare suggestie; ik zou daar graag mee aan de slag gaan. Maar dat doe ik natuurlijk in afspraak met zorginstellingen, omdat de verantwoordelijkheid dan ook ligt waar die hoort te liggen.

De **voorzitter**:
We gaan naar meneer Hijink.

De heer **Hijink** (SP):
Dit is echt niet goed genoeg. De minister kan zeggen dat het goed is dat er van die testen gaan komen, maar je kunt dat natuurlijk niet overlaten aan organisaties zelf. Het hele punt is nou juist: als jij als zorginstelling weet dat je de boel niet op orde hebt, dan ga je dat oplossen. Waarom zou een instelling die de dataveiligheid niet op orde heeft zichzelf gaan testen? Je moet de inspectie en de controle natuurlijk ook tot je nemen als onderdeel van het toezicht. Onze suggestie is om dat juist vanuit de rol van de minister te doen, niet bij iedere instelling en niet iedere dag overal, maar wel steekproefsgewijs. Dat is ook een signaal naar de rest van de sector: je kunt een controle krijgen; wij gaan die testen doen en je kunt op een gegeven moment een briefje van ons op de mat verwachten waarin staat dat we je hebben getest en dat je bent gezakt. En dat moet consequenties hebben. Dat is toch een hele logische manier om het te doen, als onderdeel van het toezicht?

Minister **De Jonge**:
In de manier waarop de handhaving van de AVG nu is ingericht, is de Autoriteit Persoonsgegevens daar de toezichthouder. Daarnaast ligt er natuurlijk ook een verantwoordelijkheid bij de IGJ — in toenemende mate, moet ik daarbij zeggen, want het is nog niet zo heel lang zo dat de Inspectie Gezondheidszorg en Jeugd daarmee te maken heeft. Maar die ziet erop toe dat zorgaanbieders voldoen aan de juiste randvoorwaarden voor de inzet van ICT en voor de kwaliteit en veiligheid van de zorg. De veiligheid van de zorg heeft natuurlijk ook te maken met de veiligheid van de gegevensdeling. Het onderwerp informatiebeveiliging is onderdeel van het toetsingskader e-health van de inspectie. De inspectie verwacht dat zorgaanbieders aantoonbaar werk maken van een managementsysteem voor informatiebeveiliging dat voldoet aan de wettelijke norm. Daar zou je dit natuurlijk heel goed onder kunnen scharen. Vanaf 2018 besteedt de inspectie structureel aandacht aan het thema e-health bij zorginstellingen. In het najaar van 2017 is de inspectie daarom begonnen met een reeks verkennende bezoeken aan de hand van het toetsingskader e-health, dat met name hierover, over veilige gegevensdeling, gaat. De inspectie bezocht ziekenhuizen, ggz-instellingen en instellingen voor gehandicaptenzorg. Op basis daarvan heeft de inspectie haar toezicht op e-health in het afgelopen jaar verder ingericht en het toetsingskader e-health verder aangescherpt. De inspectie gaat nu eerst na of het huidige toetsingskader bruikbaar en formeel juridisch geschikt is voor het jeugdveld. Daarvoor doet de inspectie een aantal pilots bij jeugdzorginstellingen.

Maar als ik u zo hoor, en ook als ik de heer Raemakers zo hoor, dan denk ik dat ... Laat ik beginnen met te zeggen dat ik ook Jeugdzorg Nederland als brancheorganisatie en de VNG hun rol wil laten pakken. Maar eigenlijk zegt u: zou je ook niet vanuit een toezichthoudersrol zelf proactief pentesten kunnen doen? Ik denk dat het antwoord "ja" is. Maar dat zou betekenen, en dat staat op dit moment niet op het werkprogramma van de inspectie en volgens mij ook niet op dat van de Autoriteit Persoonsgegevens, dat je meer een thematisch onderzoek doet naar hoe het staat met gegevensbeveiliging, databeveiliging in de jeugdzorgsector. Voor zo'n themaonderzoek zou de inspectie inderdaad pentesten kunnen gebruiken. Ik ben er niet voor om dat op alle zorginstellingen of alle jeugdzorginstellingen te doen, omdat dat gewoon ook een enorme belasting geeft. Er zijn alleen al 6.000 jeugdzorginstellingen, ook al zitten daar ook kleintjes tussen. Het moet allemaal ook wel een beetje te behappen blijven. Maar die suggestie, als u dat een suggestie vindt, zou ik kunnen doen. Ik zou dan graag het gesprek met de inspectie, ook in samenwerking met de AP, aangaan over hoe dat te doen zou zijn. Een pentest zou daar dan bij kunnen horen. Dat laat onverlet het werk dat instellingen ook nu al gewoon te doen hebben.

De heer **Hijink** (SP):
Het spreekt voor zich dat in beginsel de verantwoordelijkheid moet liggen bij de organisatie zelf. Daar ben ik het 100% mee eens. Het zou wel heel makkelijk worden als je dat kon afschrijven. Ik ben echt blij dat de minister nu deze suggestie overneemt, want dit is precies wat ik bedoel: de inspectie gaat in overleg en in samenwerking met de Autoriteit Persoonsgegevens niet alleen achteraf vaststellen dat er iets ernstigs is gebeurd, maar maakt het onderdeel van de controle en het toezicht op de zorg. Het gaat dan

eigenlijk precies zoals er ook toezicht is op de kwaliteit van de zorg zelf: de inspectie wandelt op de werkvloer naar binnen, kijkt hoe het gaat en kijkt in de dossiers of alles op orde is. Met zo'n test kan dat natuurlijk makkelijk op afstand. Maar het gaat erom dat die praktische invulling bij de inspectie komt te liggen. Dus als de minister daarvoor openstaat, dan zou ik zeggen: laten we dat vooral gaan doen.

Minister **De Jonge**:
Zeker. Ik sta daar open voor. Ik wil nog wel even nadenken over de vorm waarin we dat kunnen gieten en over het tempo waarin het kan. Het vraagt namelijk wel iets nieuws in zowel het werkprogramma van de inspectie als in het werkprogramma van de Autoriteit Persoonsgegevens. Die zijn er niet onmiddellijk morgen op berekend om zo'n onderzoek, dat volgens mij veel vergt, te starten. Maar ik snap wel wat u bedoelt. Ik ben het overigens niet eens met de kwalificatie die de heer Mulder zojuist gaf over Zorg-CERT. Een brandweer heeft niet alleen te blussen. Een brandweer heeft wel degelijk ook preventief te werken. En een goede brandweer werkt preventief. Volgens mij is Zorg-CERT dus in zichzelf een belangrijke waarde. Ik denk ook, en dat is even naar aanleiding van het debat dat ik had met de heer Raemakers, dat we niet de verantwoordelijkheid moeten wegnemen bij degenen die de eerste verantwoordelijkheid dragen, juist ook omdat werkgevers nu heel veel mogelijkheden hebben om hun mensen te scholen, om hun mensen alert te maken en om ook een eigen verantwoordelijkheid te dragen. Ik kom daar zo nog op terug. Daar zit ook een tuchtrechtelijke kant aan.

Er zijn veel vragen gesteld als: dit geldt voor Samen Veilig Midden-Nederland (SAVE), maar hoe zit het eigenlijk bij andere jeugdzorginstellingen? We hebben nergens een realtimeoverzicht van hoe het zit met instellingen. De AP heeft dat natuurlijk ook niet. Dat heeft de inspectie ook niet. Dat heeft niemand. Dus is het, denk ik, zinvol om die test in te zetten — en daarbij ook gebruik te maken van pentesten of van ethische hackers, zoals dat volgens mij heet — om daarmee de alertheid in de sector te vergroten. Dat lijkt mij een zinvolle stap, jazeker.

Mevrouw **Tielen** (VVD):
Ik hoor de minister een voorzichtige toezegging doen, met "zou kunnen" en "misschien" en "in gesprek gaan". Dat waardeer ik heel erg. Maar volgens mij is de bedoeling van dit debat vanavond ook dat we ook buiten deze zaal duidelijk maken dat veiligheid en vertrouwen wat betreft persoonsgegevens echt hoog op onze gezamenlijke agenda staan.

Minister **De Jonge**:
Zeker.

Mevrouw **Tielen** (VVD):
En we vinden — en dat hoor ik de minister ook zeggen — dat de Autoriteit Persoonsgegevens en de Inspectie Gezondheidszorg en Jeugd daar ook een rol in te nemen hebben. Moeten ze de verantwoordelijkheid overnemen? Nee, zeker niet. Maar ze moeten wel een aanspreekpunt zijn vanuit het land en ook actief laten zien dat ze op zoek gaan naar de risico's en de gaten. Dus ik hoor deze minister die toezegging doen. Tegelijkertijd zou ik het wel fijn vinden als we aan het eind van de avond een wat minder voorzichtige benadering hebben. Kan de minister nu al een directere toezegging doen of vraagt hij de Kamer om daarover straks een uitspraak in zwart-op-wit uit te voeren?

Minister **De Jonge**:
Vraagt deze minister om een motie? Dat is eigenlijk de vraag. Nou, niet per se. Dat staat u overigens wel vrij, maar laat ik zo precies mogelijk formuleren wat ik denk dat goed is. Het is eigenlijk mijn tweede blokje, maar ik ga zo precies per verantwoordelijkheidslaag na wat ik denk dat de volgende acties moeten zijn. Wat u op voorhand al toevoegt aan wat ik zou zeggen is eigenlijk dat wij aan de toezichthouders vragen om proactief — dus niet reactief maar proactief — iets als een themaonderzoek te doen naar de dataveiligheid, de gegevensbescherming in de jeugdzorg. Laat ik het zo maar noemen, omdat de inspectie vaak themaonderzoeken doet. De suggestie van Hijink en Raemakers daarbij was om gebruik te maken van pentesten. Ik doe die toezegging graag. Ik zeg er alleen wel bij dat ik daarover het gesprek aan moet met zowel de AP alsook de inspectie om te kijken op welke manier en in welk timeframe dat op een zinvolle manier is vorm te geven.

Mevrouw **Tielen** (VVD):
Ik hoor de toezegging en ik hoor ook dat de minister nog terugkomt op de verantwoordelijkheden. Ik wacht nog even af, maar dit klinkt al veelbelovend.

Minister **De Jonge**:
Dan kom ik bij mijn tweede blokje dat gaat over hoe we in het algemeen in de zorg omgaan met gegevensbescherming, op basis waarvan, en hoe we datalekken voorkomen. Daar zijn veel vragen over gesteld en ik denk dat ik ze redelijk samenhangend kan beantwoorden.

Een aantal sprekers heeft gevraagd hoe we tot structurele oplossingen komen. Hoe kom je tot het voorkomen ervan en niet meer alleen maar achteraf repareren ervan? Allereerst even de cijfers, daar heeft de heer Raemakers volgens mij naar gevraagd. Ook werden hier een aantal cijfers genoemd, en wel de cijfers van het aantal datalekken bekend bij de Autoriteit Persoonsgegevens. In 2018 heeft de Autoriteit Persoonsgegevens over alle sectoren ruim 20.000 datalekken gemeld gekregen. De meeste datalekken werden gemeld door organisaties uit de sectoren zorg en welzijn met 29%, financiële dienstverlening 26%, en openbaar bestuur 17%. Dan gaat het in de totale sector zorg en welzijn over 6.055 wettelijke meldingen. Daarvan is 6% meldingen in de jeugdsector. Als ik het heel snel uitreken is 6% een dikke 300. De voorzitter zal mij corrigeren als ik niet goed heb gerekend.

Dat zijn grote getallen, dat is de ene kant daarvan. Tegelijkertijd zeg ik: ja, dat is dus op 1,3 miljoen mensen die werken in de zorgsector. Het aantal meldingen lijkt mij niet onmiddellijk gelijk te stellen aan het aantal risico's. Je kunt daar niet onmiddellijk de conclusie aan verbinden dat het dus zo erg gesteld is. Je kunt ook zeggen dat het iets zegt over de alertheid waarmee de sector ermee omgaat.

Daar wil ik zeker waar het gaat over de zorg op voorhand iets extra's aan toevoegen wat in dit debat volgens mij nog onvoldoende is belicht. Veel mensen die werken in de zorgsector hebben, naast uiteraard een wettelijke verantwoordelijkheid om gegevens netjes te verwerken en zich aan de AVG en de bepalingen in de Jeugdwet te houden, zich ook te houden aan het tuchtrecht. Men is tuchtrechtelijk aansprakelijk voor de manier waarop om wordt gegaan met gegevensdeling. Dat geldt voor de medisch-specialistische sector helemaal. Daar is men zeer gewend om met het tuchtrecht te werken, maar inmiddels is men in de jeugdzorgsector ook zeer gewend om met het tuchtrecht te werken. Zeker in de jeugdbeschermingskant van de zaak wordt het tuchtrecht veel toegepast, juist waar het gaat over gegevensdeling. Kortom, ik durf de stelling wel aan dat je op zichzelf genomen niet kunt zeggen dat in de zorg slordig wordt omgegaan met gegevens. Dat laat onverlet dat een meldenswaardig datalek bij de Autoriteit Persoonsgegevens geregeld voorkomt. Dat men daar alert op is en dat meldt, is niet iets om je zorgen over te maken, maar is juist een goed ding. Ik voeg er nog enkele voorbeelden aan toe. Als een medewerker zijn telefoon in de trein heeft laten liggen, is dat een meldenswaardig datalek. Als je je tas in de trein hebt laten staan met een dossier erin, niet digitaal maar van papier, is dat een meldenswaardig datalek. Als je als instelling niet digitaal verhuisd bent zoals Bureau Jeugdzorg Utrecht, maar fysiek verhuisd bent van de ene straat naar de andere straat en er komt post op je oude adres binnen, is dat een meldenswaardig datalek. Bij de 1,3 miljoen mensen die alle dagen omgaan met zeer beschermenswaardige persoonsgegevens komen datalekken voor. Die zullen ook in de toekomst blijven voorkomen.

De heer **Raemakers** (D66):
Ik begrijp de nuancering van de cijfers van de minister enerzijds wel, maar anderzijds vind ik haar ook problematisch. De minister zegt dat er 6.000 datalekken zijn en 6% daarvan in de jeugdzorg. Dat zijn er 360 als je het precies narekent. Dat is bijna hetzelfde aantal als het aantal gemeenten dat we hebben. Ik geloof dat dat er 380 zijn of misschien inmiddels weer wat minder. Dat zou betekenen dat in iedere gemeente ieder jaar, gemiddeld genomen, ongeveer één datalek plaatsvindt. Als je het van die kant bekijkt, is het hartstikke ernstig dat er heel veel gemeenten zijn die totaal niet met het onderwerp bezig zijn. Kan de minister aangeven wat hij ervan vindt dat er gemiddeld genomen per jaar in iedere gemeente een datalek in de jeugdzorg plaatsvindt?

Minister **De Jonge**:
Dat is ernstig. Datalekken zijn ernstig. Ik heb niet willen betogen dat het niet ernstig is, maar ik heb willen betogen dat de mate waarin datalekken worden gemeld niet per se iets zegt over de onzorgvuldigheid waarmee met data wordt omgegaan, maar vooral over de alertheid waarmee met data wordt omgegaan. De alertheid dat als je je tas met dat dossier bent vergeten, je weet dat dat een meldenswaardig datalek is. Dat is één. Twee is dat de getallen groot zijn, heel groot. Tegelijkertijd horen die 6.000 meldingen bij een zorgsector waar 1,3 miljoen mensen werken. Ik maak daarin niks kleiner, maar wil wel benadrukken dat we gewoon nuchter en eerlijk naar mekaar moeten zijn. 100% garantie dat er nooit meer een datalek zou kunnen plaatsvinden, bestaat niet in een sector waarin zo veel wordt omgegaan met gevoelige gegevens. We moeten daar eerlijk in zijn.

De heer **Raemakers** (D66):
Maar dit is toch een vreemde argumentatielijn: als iemand zijn tas in de trein laat liggen, is het maar goed dat dat iedere keer gemeld wordt. Hoe kan deze minister hier zeker weten dat iedere jeugdzorgmedewerker die zijn tas een keer in de trein vergeet, dit meldt? Hij weet toch helemaal niet in welke gevallen er niet gemeld wordt? Ik vind dat een kromme argumentatielijn. Zo kun je altijd zeggen dat de cijfers wel meevallen "want alles wordt gemeld". Maar dat is nou net het probleem. We weten niet wat er niet wordt gemeld.

Minister **De Jonge**:
Klopt. Dat heb ik ook niet beweerd. Klopt. Ik zeg een aantal dingen. Een. De hoogte van het cijfer is niet per se een blijk van onzorgvuldigheid; het kan ook een blijk van alertheid zijn. Dat is het eerste wat ik zeg: kán zijn. Dat weet ik niet zeker. Dat is het eerste wat ik erover zeg. Twee. Je kunt de getallen ook duiden in relatie tot de totale omvang van de sector en de mate waarin wordt omgegaan met vertrouwelijke gegevens. Die is in de zorgsector meer dan in welke sector dan ook aan de orde. Dat de zorg de grootste melder is, vind ik niet gek. Dat vind ik normaal. Sterker nog, als de zorg niet de grootste melder zou zijn, zou ik me veel meer zorgen maken, want dat zou betekenen dat kennelijk de zorgsector wel heel weinig alert is. Kortom, ja, het is een buitengewoon serieus te nemen fenomeen. Iedereen heeft dit onderstreept en volgens mij zijn we het op dat punt ook helemaal eens. Waar ik alleen voor wil waken, is dat we elkaar op enig moment zouden wijsmaken — dat doet u niet hoor, overigens — in de wil om er echt iets aan te doen, dat we naar een 100% voorkomen van datalekken zouden kunnen gaan. Dat gaat niet. Waarom noem ik die telefoon in de trein? Dat is een zaak die ik zelf heb meegemaakt. Een van onze wijkteammedewerkers in Rotterdam had inderdaad de telefoon in de trein laten liggen. Die zegt tegen haar baas: ik heb mijn telefoon in de trein laten liggen. Vervolgens vraagt die baas: zat daar een wachtwoord op? Nee, er zat geen wachtwoord op. Superstom natuurlijk. Dat is wel de meest simpele beveiliging die je kunt toepassen. Kortom, vanaf dat moment hebben we extra instructies gegeven aan alle wijkteammedewerkers: jongens, beveilig je telefoon op alle mogelijke fronten. Natuurlijk zijn we ook gaan werken met beveiligde mail en zo. Kortom, die datalekmelding, het melden alleen al en vervolgens het met elkaar erover hebben en met elkaar actie ondernemen, helpt gewoon om het telkens beter te doen. Dat is ook de ratio achter de AVG en de meldingsplicht die in de AVG zit.

Mevrouw **Van Kooten-Arissen** (PvdD):
Ik wil de minister hier toch even op doorvragen. Hoe verhoudt zich dit tot het feit dat de toezichthouder van de Autoriteit Persoonsgegevens over die 20.881 datalekken van vorig jaar zegt dat het een structureel privacyprobleem is in de zorg? Dat is dus een verdubbeling ten opzichte van het jaar ervoor, wat ook wel weer begrijpelijk is omdat er meer media-aandacht was vanwege de AVG. 29% van de datalekken vindt plaats in de zorg. Hoe verhoudt zich dat tot de uitspraak van de minister dat het eigenlijk niet zo'n groot probleem is?

Minister **De Jonge**:
Maar dat zeg ik dus niet. Ik zeg niet dat het geen heel erg groot probleem is. Het is wél een groot probleem. Ik probeer alleen aan te tonen dat ik het niet onlogisch vind dat de zorgsector de grootste melder is van alle sectoren in Nederland. Sterker nog, als de zorgsector niet de grootste melder zou zijn, zou ik me pas zorgen maken, want dat zou wijzen op een gebrek aan alertheid. Het gaat om een sector met 1,3 miljoen mensen, veel groter dan welke sector dan ook. Eén op de zeven mensen met werk werkt in de zorg. In die zorg gaat iedereen alle dagen met vertrouwelijke gegevens om. Dus als niet een groot deel van de meldingen bij de AP uit de zorg zou komen, dan zouden we ons daadwerkelijk zorgen moeten maken.

Heeft de zorgsector daarmee een grote opdracht? Ja, natuurlijk heeft de zorgsector een hele grote opdracht, want er gaan zo veel mensen met zo veel vertrouwelijke gegevens om. En dus heeft de zorgsector een hele grote opdracht. Die grote opdracht moeten we ook waarmaken. Ik schets straks welke stappen we daarin kunnen nemen. Maar ik heb het op geen enkele manier kleiner willen maken dan de werkelijkheid en wat er daadwerkelijk speelt. Wat ik alleen wel zeg, is dat uit de omvang van de aantallen niet zozeer een gebrek aan zorgvuldigheid valt op te maken, maar eerder een voldoende alertheid. Daar ben ik op zichzelf genomen blij mee. Ik sluit ook niet uit dat het volgend jaar nog meer is. Sterker nog, misschien moeten we met elkaar hopen dat het aantal meldingen vanuit de zorg volgend jaar meer is. Dat zou namelijk wijzen op een groter wordende alertheid en met die alertheid moet het beginnen. Wij kunnen niets. Wij kunnen regels maken tot we een ons wegen en we kunnen systemen inrichten, brandweerfuncties inrichten, maar het begint echt met gewoon gezond verstand. Mevrouw Kuiken zei dat zeer terecht. De heer Peters zei het ook. Gezond verstand. En ook: hetgeen gij niet wilt dat u geschiedt ... als het gaat om gegevens delen. Dat is eigenlijk de meest simpele regel, überhaupt in het leven, maar zeker als het gaat om gegevens delen. Wat zou je zelf vinden als het jouw gezin betrof, als het jouw kind betrof? Zou je het fijn vinden als het allemaal open en bloot in te zien was? Nee natuurlijk. En dus: gezond verstand en behandel een ander qua informatie zoals je zelf graag behandeld wilt worden. Dat is eigenlijk de eerste verdedigingslinie of verdedigingswal tegenover datalekken.

Mevrouw **Van Kooten-Arissen** (PvdD):
De reden dat ik hier zo op aansla, is dat de minister wel onderkent dat het een probleem is — dat hoor ik hem zeggen — maar dat hij het beschouwt als een wake-up call. Dit datalek bij jeugdzorg was een wake-upcall, terwijl de Autoriteit Persoonsgegevens zegt dat er sprake is van een structureel probleem. Ik heb ook in mijn bijdrage een hele waslijst aan voorbeelden van datalekken uit het afgelopen halfjaar opgesomd. Daaruit blijkt ook dat er een structureel probleem is met privacy in de zorg. Ik wil heel graag dat de minister de urgentie ervan erkent en gaat vertellen wat hij daaraan gaat doen in plaats van dat hij dit een wake-up call noemt.

Minister **De Jonge**:
Ik zocht even naar de brief die ik gisteren aan de Kamer heb gestuurd samen met collega Bruins. Ja, het is een wake-upcall. Sommige datalekken waren in potentie heel lelijk, met heel grote gevolgen voor de privacy van al die ouders en kinderen die dachten dat hun verhaal veilig was. Gelukkig lijkt het erop dat de informatie niet bij verkeerde mensen terechtgekomen is. Gelukkig lijkt het niet door andere onbevoegden te zijn ingezien dan RTL Nieuws en de melders, maar het had natuurlijk wel gekund. In die zin is het absoluut een wake-upcall. Laten we het ook benutten als een wake-upcall in de richting van de jeugdzorgsector. Als mevrouw Arissen dat tegelijkertijd uitlegt als: ja maar, het is toch niet dat je daar pas sinds vorige week mee bent begonnen, dan is dat zeker zo. Kijk wat allemaal hebben gedaan. We hebben het feitenrelaas, de lange opsomming van alle acties die er zijn ondernomen vanaf mijn voorganger, door collega Bruins en door mijzelf, op een rij gezet — en dat zijn nogal wat acties — om telkens weer beter te worden in die gegevensbescherming en dataveiligheid, wetend dat je het nooit helemaal 100% sluitend kunt krijgen.

Ik ga opsommen wat wij te doen hebben, want dat was eigenlijk de vraag. Ik zal proberen dat een beetje bondig te doen. Als ik dat niet zelf zou zeggen, dan had de voorzitter dat op dit moment gezegd, denk ik. We kennen elkaar inmiddels een beetje.

De **voorzitter**:
Het brandt mij op de lippen.

Minister **De Jonge**:
Waar begint het mee? Het begint bij alle 1,3 miljoen mensen in de zorg zelf, gezond verstand en het behandelen van een ander zoals je zelf ook behandeld wilt worden als het gaat over gegevensdeling. Deel natuurlijk alsjeblieft die gegevens die juist helpen om de veiligheid te bevorderen, maar het is altijd need to know en nooit nice to know. Dus zorg dat je terughoudend bent als het gaat over gegevens die je niet hoeft te delen. We hebben daarop een handhavingsregime tot op het niveau van de individuele medewerker gezet. Dat heet het tuchtrecht. Ik denk dat in die zin de vraag of er extra nodig regels zijn, ook is beantwoord. Ik vraag me eerlijk gezegd af of dit met extra regels te voorkomen was geweest. Ik denk het niet, want volgens de regels mocht het namelijk al niet. Het is gewoon een stommiteit geweest. Is dat met regels te voorkomen? Ik denk het niet, maar wel met gezond verstand. Dat is een.

Twee. Er is een verantwoordelijkheid voor de zorgaanbieders. Die verantwoordelijkheid ligt in eerste instantie bij de zorgaanbieders zelf, want zij zijn de werkgever, zij zijn de uitvoerende instantie van de zorg. Juist aan die zorg is een aantal regels gekoppeld. Dat is de tweede kant: de wettelijke bepalingen en de Autoriteit Persoonsgegevens. Waar hebben die instellingen zich dan aan te houden? Ze hebben zich te houden aan wettelijke voorschriften, de AVG, de Algemene verordening persoonsgegevens, zoals hier is vastgesteld in de Kamer. Ze hebben zich te houden aan specifieke bepalingen in de Jeugdwet, de Wmo 2015 en de regelgeving die daarop is gebaseerd voor jeugdhulpaanbieders en gecertificeerde instellingen, de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, een aantal zorgbrede Nederlandse normen voor informatieveiligheid, de NEN-normontwikkeling; een van de acties die we in de afgelopen tijd hebben ondernomen. Daarbij geldt dat elke inbreuk in verband met persoonsgegevens, waaronder een datalek of een ICT-incident, binnen 72 uur gemeld

moet worden bij de Autoriteit Persoonsgegevens. De zorgaanbieders worden gehouden aan deze strikte regels. De AP ziet toe op de naleving ervan.

Maar niet alleen de Autoriteit Persoonsgegevens heeft een toezichthoudende rol, ook de Inspectie Gezondheidszorg en Jeugd neemt steeds meer een toezichthoudende rol. De AP waar het gaat over verwerking van persoonsgegevens, want dat is de wettelijke taak van de AP. Maar de verwerking van persoonsgegevens is onderdeel van veilige zorg, onderdeel van kwaliteitsmanagement, en daarop ziet de inspectie toe. Die heeft, juist omdat dataveiligheid en gegevensbescherming een steeds belangrijkere rol spelen, in de afgelopen tijd een steeds belangrijkere rol genomen. Ik noemde dat volgens mij in antwoord op mevrouw Tielen in ons debatje van zojuist ook. Ik noemde dat het toetsingskader e-health eigenlijk steeds belangrijker is geworden. Men heeft het ontwikkeld, men heeft het toegepast op ziekenhuizen, ggz-instellingen en gehandicaptenzorginstellingen. Mede op basis van die bevindingen is de inspectie bezig geweest haar toezicht op e-health in de afgelopen jaren verder in te richten en het toetsingskader e-health verder aan te vullen en aan te scherpen. De volgende stap is dat de inspectie pilots gaat doen in de jeugdzorg om te zien of datzelfde toetsingskader e-health ook toepasbaar is in de jeugdzorg. Wat het driemanschap Tielen, Raemakers, Hijink daar zojuist eigenlijk aan toevoegde, was: oké, maar wij willen eigenlijk dat er vanuit de IGJ aan de ene kant en de AP aan de andere kant proactief en thematisch een onderzoek wordt gedaan naar hoe het in de jeugdzorgsector is gesteld als het gaat over databescherming en informatieveiligheid en dat daarbij gebruik wordt gemaakt van pentesten als onderdeel van zo'n thematisch onderzoek. Daarvan zeg ik graag toe dat ik daarover in gesprek ga met de inspectie en de AP, en dat ik de Kamer laat weten op welke manier daar vorm en inhoud aan te geven is.

De heer **Hijink** (SP):
Ik hoor graag een iets preciezer antwoord op dit punt. Ik zou ervoor zijn dat dit op de langere termijn een structureel onderdeel wordt van de werkwijze van de inspectie.

Dit is dan niet een eenmalig onderzoek waarbij we her en der wat testjes gaan doen, maar dit zou bij de vaste werkwijze van de inspectie kunnen gaan horen. Logischerwijs komt die taak daar terecht: net zoals de inspectie een verpleeghuis binnen kan vallen om te kijken hoe daar de kwaliteit van de zorg is, zo valt de inspectie ook af en toe digitaal een instelling binnen om te kijken hoe het met de kwaliteit van de gegevensbescherming is.

Minister **De Jonge**:
Ja. Ik snap die wens ook. Maar dan gaat u eigenlijk nog een stap verder. Ik gaf net aan dat de inspectie, door te werken aan dat toezichtkader e-health, eigenlijk ook al stappen zet om het toezicht op de gegevensbescherming onderdeel te maken van het reguliere toezicht. Het gaat dan ook om al dan niet digitale gegevensdeling.

Maar zo ver is men nog niet. Eerst moet echt getest worden of het toetsingskader dat nu ontwikkeld is ook werkzaam kan zijn binnen de jeugdzorgsector. Laat ik op voorhand aangeven dat ik heel beducht ben voor een enorme bureaucratische last. Ik kom daar zo op terug in reactie op vragen van de heer Peters. Dat is namelijk wel degelijk mogelijk. Daarom denk ik dat het goed is als de inspectie gewoon doorgaat met waar ze mee bezig is, namelijk dat toezichtkader gewoon testen in de praktijk: op welke manier zou dat ook kunnen werken bij de jeugdzorgsector? Maar voordat dat goed getest is, zitten we echt wel in het einde van het jaar, en volgens mij is uw behoefte om al eerder te weten hoe het nu eigenlijk zit in de jeugdzorgsector. Daarom zeg ik u toe, en dat zeg ik ook in de richting van mevrouw Tielen en de heer Raemakers, om de inspectie te vragen samen met de AP een proactief, thematisch onderzoek te doen naar de vraag hoe het nu eigenlijk zit met dataveiligheid en de bescherming daarvan met pentesten.

Op basis daarvan zouden we best eens de conclusie kunnen trekken dat dat dus onderdeel moet worden van het reguliere inspectietoezicht. Het kan zijn dat we tot de conclusie komen dat dat behulpzaam kan zijn en dat daar een groot vraagstuk ligt. De wijze waarop dat toezichtkader nu al wordt uitgetest zou dan ook antwoord kunnen geven op de vraag hoe je dat dan onderdeel kunt maken van het reguliere toezicht. Ik zou dat thematisch onderzoek dus eigenlijk ook willen gebruiken om te weten te komen wat we aan extra stappen moeten zetten. Het zou zo maar een van die extra stappen kunnen zijn, dat dit integraal onderdeel wordt van dat toezicht.

Dat was het wat betreft die inspectie, voorzitter. Dan gaat het natuurlijk ook over onze stelselverantwoordelijkheid. Daar heeft de heer Raemakers een aantal dingen over gezegd. Wij hebben daar net al deels bij stilgestaan, maar laat ik een aantal voorbeelden noemen van hoe wij die stelselverantwoordelijkheid hebben waargemaakt en hoe we die ook willen waarmaken.

Allereerst zijn er NEN-normen ontwikkeld voor de beveiligde e-mail. Daar hebben we opdracht toe gegeven. Dat is heel belangrijk omdat e-mailveiligheid niet een zo veel voorkomend gebruik is dat daar geen aanvullende aandacht voor moet zijn. Beveiligde e-mailverbindingen zijn natuurlijk helemaal nodig op het moment dat er tussen instellingen wordt gemaild. Maar ook binnen instellingen is het goed dat e-mail, zeker als daar dossierinformatie in staat, altijd via een beveiligde verbinding gaat. Wij hebben gevraagd om die NEN-norm. Deze zal in mei beschikbaar zijn, en dat betekent dat vanaf dat moment ook alle aanbieders van beveiligde e-mailverbindingen altijd zullen moeten werken conform die NEN-norm.

Dat is een voorbeeld. Wij hebben net ook al veel gesproken over de hulp en ondersteuning door Zorg-CERT. Laat ik dat allemaal niet herhalen, maar daar gaan we natuurlijk mee door. Sterker nog, wij hebben de jeugdzorgsector nu gevraagd om zich aan te sluiten. Op basis van de motie-Ellemeet, zo heb ik net aangegeven, zullen we voor de zomer terugkomen op de vraag hoe die aansluiting plaats kan vinden en welke implicaties dat dan heeft.

Dan is er nog een aantal overige acties, zoals bijvoorbeeld de AVG-Helpdesk die we in mei hebben ingericht samen met de zorgkoepels. Aan actieve informatiebeveiliging hebben we natuurlijk gedaan door dat eerdere actieplan informatiebeveiliging. Dat bestaat onder andere uit bewustwordingscampagnes en het bieden van ondersteuning, ook aan leden van verschillende koepelorganisaties.

Voorzitter, ik denk dat ik de vragen in dit blok heb gehad. Ik wil even testen of dat ook echt zo is. Nee. De heer Hijink vroeg nog of de AP wel in staat is om de taken in de zorg uit te voeren. Is de omvang van de AP daar wel op berekend? Dit is eerlijk gezegd meer een vraag om met collega Grapperhaus te bespreken. Ik durf er nu geen klip-en-klaar ja of nee op te geven. Ik ga ervan uit dat er ieder jaar wordt gekeken of het werkplan voldoende tegemoetkomt aan de wettelijke taak die wij de autoriteit hebben gegeven, zoals wij ook omgaan met inspecties en andere onafhankelijke toezichthouders. Zoals wij dat doen, doen alle departementen dat met hun toezichthouders. De autoriteit is een onafhankelijk orgaan. Die bepaalt haar eigen werkprogramma en maakt eigen keuzes in de handhaving ervan. De vraag is wel gerechtvaardigd of men opgewassen is tegen deze taak. Vindt de heer Hijink het goed als ik deze vraag met collega Grapperhaus bespreek? Omdat de AP onder Justitie valt, wil ik deze vraag dus met de heer Grapperhaus opnemen.

Ik denk dat ik daarmee de meeste vragen in dit blok heb gehad. Ik heb nog een aantal overige vragen te beantwoorden.

De Partij voor de Dieren stelde vragen over de verplichting om aan elektronische gegevensuitwisseling te doen. Ik meen dat u daar niet zo heel lang geleden een debat over heeft gehad met mijn collega Bruins. Dat zult u in de toekomst nog wel vaker hebben, want collega Bruins heeft een uitgebreide brief gestuurd om stapsgewijs te kiezen voor meer digitalisering. Ik denk dat we dat debat niet moeten overdoen. Vorige week heeft mijn collega een soort eerste roadmap geschetst voor hoe we overgaan tot het stap voor stap steeds verdergaand verplichten van een gegevensuitwisselingsstandaard waarmee alle digitale applicaties in de zorg hebben te werken.

Ik wil daar nog iets aan toevoegen als het gaat over veiligheid, waarover uw achterliggende zorg gaat. In de huidige constellatie verplichten we vrij weinig. Sinds het epd is gestrand in de Eerste Kamer is er een soort huivering in de politiek om überhaupt nog iets met ICT en zorg te durven doen als het gaat over patiëntendossiers. Dat heeft niet alleen geleid tot zorgen bij werknemers over de uitwisselbaarheid van gegevens als het echt nodig is, maar ook tot een wildgroei aan gegevensstandaarden. We hebben aanvankelijk al actie ondernomen met het Informatieberaad. Nu gaan we dat stap voor stap steeds verplichtender doen. Ik denk dat dit de veiligheid juist tegemoetkomt. Naar aanleiding van het debatje dat u erover had met collega Raemakers zou ik willen zeggen: de enige conditie waaronder die verdere digitalisering kan plaatsvinden, is natuurlijk een goede gegevensbescherming. Het is dus: met beschermde gegevens of niet.

Dat wil niet zeggen dat je, voordat je kunt digitaliseren, eerst honderd procent garantie zult moeten geven op de gegevensdeling en of dat allemaal veilig gaat. Voor een veiliger gegevensuitwisseling is die digitalisering nou juist nodig. Kijk wat er nu nog aan papieren dossiers wordt gebruikt. Kijk wat er nu nog aan onuitwisselbaarheid van gegevens speelt, ook bijvoorbeeld in de acute zorg, tussen ziekenhuis en wijkverpleging en tussen huisarts en wijkverpleging. Kijk naar wat daar aan gegevens verloren gaat. Gegevens worden niet gedeeld omdat ze niet kunnen worden gedeeld, gewoon omdat gegevensstandaarden niet op elkaar zijn geënt. Kijk naar wat dat betekent voor de inefficiëntie en de onveiligheid van sommige zorgoverdrachtsmomenten, die er altijd zijn. Ik denk dat we, als het gaat over de veiligheid in de zorg, juist een wereld te winnen hebben met digitalisering. Kortom, ik ben echt van harte voor stap voor stap verder digitaliseren en wil daar een ferm pleidooi voor houden. Daarbij zeg ik wel in uw richting: het kan alleen maar als het ook veilig kan.

Mevrouw **Van Kooten-Arissen** (PvdD):
De minister zegt terecht dat het LSP, het elektronisch patiëntendossier, is gestrand in de Eerste Kamer; het is daar weggestemd. Alleen is oud-minister Schippers vervolgens via een achterdeurtje verdergegaan met het LSP als infrastructuur voor het delen van medischezorgdossiers. Dat raakt aan het punt dat ik hier ook wil maken, namelijk dat dat juist hetgeen is wat niet in overeenstemming te brengen is met de privacywetgeving en het medisch beroepsgeheim. Privacyexperts waarschuwen daar dan ook voor. Ik zou de minister daarom ook echt met klem willen vragen om die versnelde verplichte digitalisering een halt toe te roepen, want als we het LSP als onomstreden bouwsteen gaan zien voor de toekomstige uitwisseling van medische gegevens, dan blijven we stuiten op dit soort grote veiligheidsproblemen.

Minister **De Jonge**:
Dit is het moment waarop we eigenlijk het debat gaan overdoen dat u al een keer met collega Bruins heeft gehad en dat u ook nog vaker zult gaan hebben met collega Bruins. Het LSP is overigens geen verplichte infrastructuur, maar als ik dat soort nuances ga aanbrengen, gaan we, denk ik, wel heel diep de techniek in. Het ging mij meer om het algemene punt.

Ik snap eigenlijk heel goed waar uw zorg zit. U bent namelijk bezorgd over de veiligheid. Zijn onze gegevens veilig bij verdergaande digitalisering? Ik heb eigenlijk de omkering daarvan willen onderstrepen: juist als wij niet kiezen voor verdergaande digitalisering, doen we de veiligheid in de zorg tekort. Maar als we kiezen voor verdergaande digitalisering — dat doen we overigens stap voor stap — dan kunnen we dat alleen maar doen als dat veilig kan. Zo zullen we ermee aan de slag moeten.

Voorzitter. Dan gaan we verder met ...

De **voorzitter**:
Eerst nog even de ontknoping van deze interruptie.

Mevrouw **Van Kooten-Arissen** (PvdD):
Voorzitter, dank u wel. Ik ben blij dat de minister erkent dat de veiligheid voorop moet staan bij het delen van medische gegevens. Ik neem aan dat hij daarom ook nog terugkomt op mijn vraag hoe het zit met de uitvoering van mijn motie om bij medische gegevens te werken met end-to-endencryptie.

Minister **De Jonge**:
Ja.

De **voorzitter**:
Raemakers nog even.

De heer **Raemakers** (D66):
Op dit punt, voorzitter, want wij hebben hier in het debat ook naar gevraagd. De minister geeft heel duidelijk aan dat cyberveiligheid een randvoorwaarde is, maar we zien ook dat het met name bij Z-CERT en de instellingen wordt neergelegd. Kunnen wij hier ook met elkaar afspreken dat de minister voor de zomer met een brief komt over hoe de minister kan garanderen dat de veiligheid bij digitale gegevensuitwisseling altijd gegarandeerd is? Kan de minister dat nu gewoon toezeggen?

Minister **De Jonge**:
Met het woord "garantie" kan ik, eerlijk gezegd, helemaal niks als het gaat over de zorg. Zorg is mensenwerk en garanties zijn vanuit dit huis niet te geven. Als ik dat wel zou doen, zou u mij niet moeten geloven! Met het woord "garantie" kan ik dus niet zo veel.

Ik zal een aantal reacties gegeven. De eerste is dat ik zojuist heb gezegd dat ik afspraken ga maken met de jeugdzorginstellingen, de VNG et cetera. Ik heb hun gevraagd om mij voor 1 juli te berichten en dat betekent uiteraard dat ik op basis daarvan de Kamer zal informeren over welke extra stappen er nodig zijn. De tweede toezegging die ik mij heb laten ontfutselen, is dat ik met de AP en de IGJ ga kijken of we een proactieve thematische manier van onderzoeken kunnen vinden om te kijken hoe het gesteld is met de dataveiligheid in de zorg. Ik zou het mooi vinden als het in de tijd een beetje bij elkaar kwam, omdat ik dan op basis van én datgene wat Jeugdzorg Nederland en de VNG naar boven halen én op basis van het onderzoek van de AP en de IGJ kan kijken wat er van onze kant aan aanvullende maatregelen nodig is. Het gaat dan dus om aanvullende maatregelen die wij zouden moeten nemen. Dat is één kant. Dit doen we mede naar aanleiding van dit debat en mede naar aanleiding van wat we in Utrecht hebben gezien.

Het tweede deel is eigenlijk een heel ander debat, maar het raakt hier natuurlijk wel aan. Dat is het debat dat ook de Partij voor de Dieren zoekt. Als we kiezen voor die verdergaande digitalisering, dan zullen we dat moeten doen onder de randvoorwaarde van databescherming en dataveiligheid. Dat is een sine qua non. Dat is een randvoorwaarde die uiteraard te gelden heeft. Met collega Bruins voert u het debat over de stappen die we met elkaar te zetten hebben in die verdere digitalisering. Vorige week — volgens mij heeft u dat nog niet kunnen bespreken in de Kamer — heeft hij nog een brief aan de Kamer gestuurd waarin hij alle stappen schetst die we te nemen hebben onderweg naar een verplicht stellen van niet zozeer digitalisering als wel de standaarden van gegevensuitwisseling, om daarmee juist de veiligheid in de zorg te vergroten. Dat is eigenlijk een ander debat. Maar ik zeg natuurlijk wel dat dat alleen maar kan onder de conditie van databescherming en dataveiligheid.

De heer **Raemakers** (D66):
Ik wil een minister die erbovenop zit en niet een minister die afwacht. Ik hoor nu toch te veel in het antwoord terug dat de minister aangeeft waar hij allemaal op wacht en dat het dan de portefeuille van collega Bruins is. Maar dat vind ik niet zo relevant. Ik sta hier nu in het debat met de minister van VWS. We hebben heel duidelijk, met meerdere fracties, in het debat de vraag naar voren gebracht: kan dat als randvoorwaarde worden opgenomen? Dan geeft de minister aan: ja, dat moet een randvoorwaarde zijn. Maar dat wordt dan toch belegd bij allerlei clubs en allerlei zaken. Wat kan de minister nu gewoon de komende tijd doen? Mijn vraag was heel simpel: kan hij voor de zomer een brief sturen over hoe hij bij al die ontwikkelingen waarbij het gaat om het makkelijker elektronisch delen van patiëntengegevens, op alle terreinen in de zorg, ervoor kan zorgen dat dat op een goede manier gebeurt? Kan hij, terwijl die ontwikkeling gaande is, daarop nu maatregelen nemen en nog voor de zomer met concrete acties komen?

Minister **De Jonge**:
Ik begrijp, werkelijk waar, na het debat dat we zojuist hebben gevoerd en na het antwoord dat u zojuist heeft gekregen, niet waarom u deze vraag nog stelt. Naar aanleiding van deze casus in de jeugdzorg heb ik namelijk uitgelegd wat ik aan extra maatregelen ga nemen. Ja, inderdaad, ik snap dat u daar graag voor de zomer een recap van wilt hebben en wilt weten wat we daarmee dan gaan doen en hoe we daarmee verdergaan. Dat is dat spoor.

Het tweede spoor — dat is niet afwachten, juist niet; daar is collega Bruins ontzettend intensief mee bezig — gaat over het verplichten van gegevensstandaarden en daarmee het stimuleren van het verder digitaliseren van de gegevensuitwisseling in de zorg: het werken met persoonlijke gezondheidsomgevingen en het verplichten van gegevensstandaarden zodat alle leveranciers in de zorg van dezelfde gegevensstandaarden gebruikmaken. Collega Bruins heeft gezegd — volgens mij is dat precies wat u wilt — dat we daarvan een wettelijke verplichting gaan maken. Dat is overigens een razendcomplexe wet. Toch gaan we dat doen, omdat we denken dat dat de enige manier is om het snel te doen, maar ook volgens de randvoorwaarde die u nu juist schetst, namelijk veilig. We gaan dus niet zitten afwachten; daar zijn we juist alle dagen mee bezig. We maken die wet namelijk, en die wet kan er alleen maar komen onder de randvoorwaarde van dataveiligheid. Dat is dus niet afwachten, dat is handelen. Dat zijn we al aan het doen.

De heer **Raemakers** (D66):
Eerst zegt de minister: ik begrijp de vraag niet. Uiteindelijk beantwoordt hij hem toch heel goed. Daar ben ik dan ook blij mee.

De **voorzitter**:
Ouwe truc.

De heer **Raemakers** (D66):
Wel een mooie retorische truc van de minister!

Minister **De Jonge**:
U heeft het door!

De heer **Raemakers** (D66):
Die hebben we dan toch wel ontrafeld, samen, zeg ik tegen de voorzitter.

Minister **De Jonge**:
Ja, exposed.

De heer **Raemakers** (D66):
Maar het ging ook over wat de heer Hijink terecht in een interruptie aan mij vroeg over bijvoorbeeld de PGO's, de persoonlijke gezondheidsomgevingen. Dat is natuurlijk een traject dat loopt. Ik vind dat deze minister niet kan zeggen dat dat helemaal het pakkie-an is van collega Bruins. Ook bij de minister van VWS zitten zaken in portefeuille — ik noem de jeugdzorg, de langdurige zorg — waarbij die PGO's gewoon een rol spelen. Onze vraag is heel helder: bij de ontwikkeling van die PGO's moet de veiligheid een randvoorwaarde zijn. Dit is een ontwikkeling die volgens mij al in 2018 is gestart. Dat gaat maar door. Mijn vraag is dus heel reëel: dan wil ik voor de zomer ook een brief waarin staat hoe voor de bestaande ontwikkelingen de veiligheid extra in de gaten wordt gehouden. Ik vind gewoon dat die er moet komen.

Minister **De Jonge**:
Nu niet bedoeld als retorische truc — zojuist overigens natuurlijk ook niet — maar dan vraag ik: wat wilt u dan extra? In de gegevensstandaarden om die PGO's überhaupt ooit tot vliegen te krijgen, MedMij, zit de veiligheid gewoon helemaal ingebakken. De MedMij-gegevensstandaarden kunnen alleen maar bestaan als die veiligheid gegarandeerd is, dus onder de conditie van veiligheid. Daar zit de veiligheid dus in. Dus wat wilt u dan extra? Want die MedMij-standaarden zouden we nooit mogen vaststellen als daarin niet "veiligheid" gewoon was gestandaardiseerd. Dus wat wilt u dan extra?

De heer **Raemakers** (D66):
Een brief voor de zomer. Waarin de minister uitvoerig toelicht hoe hij, gelet op wat er vorige week is gebeurd en wat heel ernstig is, bij alle ontwikkelingen in de zorg betreffende het digitaliseren van gegevens gaat zorgen dat de veiligheid een absolute randvoorwaarde is. Natuurlijk zijn er al stappen gezet om dat te waarborgen, maar de casus van vorige week laat ons zien dat we hier een tandje extra bij moeten zetten. Daarom vraag ik dus een brief voor de zomer. Dat is het, niet meer en niet minder.

Minister **De Jonge**:
We zetten een aantal stappen extra, zoals ik u zojuist schetste, als het gaat over het jeugdzorgdomein, naar aanleiding van de casuïstiek van vorige week. Die stappen zetten we. Dat heb ik u net allemaal al geschetst. Daarnaast vraagt u: hoe zit het dan met PGO's, gegevensstandaarden, digitalisering, wat doen we daar dan extra? Dit ook naar aanleiding van een vraag van de Partij voor de Dieren. Nou, we doen niet zozeer iets extra, maar we zijn natuurlijk wel bezig met die standaardisering. Die standaardisering werkt met de MedMij-standaarden en daarin zit veiligheid gewoon ingebakken als een keiharde eis.

Maar laat ik u het volgende toezeggen. Ik zal kijken of in de brief van vorige week die collega Bruins heeft gestuurd, voldoende ingegaan wordt op de veiligheid. Als dat onvoldoende het geval is, zal ik u in aanvulling daarop voordat u deze brief bespreekt, laten zien op welke manier in die hele PGO-ontwikkeling en die standaardisering van MedMij de veiligheid gewoon is ingebakken. Die maakt daar namelijk onderdeel van uit. Dat is helemaal geen ingewikkelde brief om te schrijven. Ik denk dat er niks extra's voor nodig is, omdat dataveiligheid gewoon een sine qua non is als het gaat om gegevensstandaardisering en standaardisering van gegevensuitwisseling.

De **voorzitter**:
Kunnen wij al naar een tweede termijn?

Minister **De Jonge**:
Nee, want ik heb één vraag van de Partij voor de Dieren nog niet beantwoord, en dat moeten we niet willen met elkaar. Dat is de vraag naar de stand van zaken van het onderzoek naar end-to-endencryptie. Die vraag is aan NEN gesteld. Er is gevraagd of dit kan worden meegenomen bij een herziening en aanscherping van de NEN-normen. Zodra daar meer over bekend is, zal collega Bruins u daarover informeren.

Dat antwoord had u niet willen missen, voorzitter.

De **voorzitter**:
En mevrouw Van Kooten-Arissen kijkt ook blij.

Bestaat er behoefte aan een tweede termijn? Het hoeft niet. Ik zie nu dat de heer Hijink eerst nog een vraag heeft. Het woord is aan hem.

De heer **Hijink** (SP):
Met het risico dat ik het antwoord gewoon heb gemist. Ik heb de minister gevraagd wat hij ervan zou vinden om alsnog te onderzoeken of de gezondheidszorg in zijn geheel niet zou moeten vallen onder de essentiële diensten, wat binnen de Cybersecuritywet betere bescherming kan garanderen.

Minister **De Jonge**:
Ik ga u vragen of ik het antwoord uitvoeriger schriftelijk mag geven. Maar zoals ik het begrepen heb en zoals ik het goed tot mij kon nemen tussen de eerste termijn van de Kamer en mijn eigen eerste termijn, is het zo dat essentiële diensten worden gedefinieerd als: als die wegvallen, is er iets niet meer voorhanden wat wel voorhanden zou moeten zijn. Denk aan de dieselvoorziening, zeg ik in de richting van GroenLinks, of aan de drinkwatervoorziening. Het gaat dus over essentiële functies die het maatschappelijk leven volstrekt ontregelen als er van buitenaf op wordt ingebroken door een statelijke of niet-statelijke actor. Omdat we heel veel ziekenhuizen hebben en heel veel zorginstellingen is dat over een instelling in de zorg niet als zodanig te zeggen. Tenzij de zorg als geheel in gevaar komt, maar daar is niet noodzakelijkerwijze sprake van.

Ik meen dat dit de afweging is geweest om "de" zorg niet als zodanig te benoemen. Maar als het bijvoorbeeld gaat over de acute zorg, wordt er natuurlijk wel altijd gekeken of er voldoende mogelijkheid is tot opschalen als er sprake is van een grote ramp of een grote inbreuk of zo. Maar dat gaat dan niet zozeer over een hack op een zorginstelling, maar over andere rampen, waarbij veel slachtoffers vallen. Dan is het de vraag of de beddencapaciteit wel voldoende is berekend op de zorgvraag, die op dat moment enorm explodeert. Maar dat is iets anders dan de zorg als geheel benoemen als essentiële functie.

De heer **Hijink** (SP):
Maar dat is ingewikkeld, want je kunt natuurlijk niet één onderdeel benoemen als essentiële functie. Het punt is dat er verschillende redenen zijn om iets als essentiële dienst aan te wijzen. Het kan bijvoorbeeld zijn als er bij uitval heel veel doden kunnen vallen of als er miljarden schade ontstaan. Maar een van de andere redenen om dat te doen, die ook in die wet staat, is als er grote emotionele schade kan ontstaan bij een aanzienlijke groep mensen. In het voorbeeld dat we vanavond bespreken, zouden duizenden kinderen in heel grote problemen zijn gekomen als deze data op straat waren beland. Dat zou bij andere instellingen ook kunnen gebeuren. Misschien kun je redeneren dat de schade niet groot genoeg is als het maar bij één instelling gebeurt — ik denk van wel, maar je zou kunnen zeggen dat het niet zo is — maar de opstelsom van datalekken in zijn geheel kan er natuurlijk wel voor zorgen dat heel grote groepen mensen in ons land grote emotionele schade oplopen. Dat zou wat mij betreft een reden kunnen zijn om nog eens te overwegen of het toch niet onder die voorwaarden zou moeten vallen. Ik vind het prima als de minister een brief stuurt. We hebben hierover al een keer een brief van collega Bruins gehad. Neem dit element dan mee in die brief en maak een soort heroverweging of dit wel de juiste keuze is geweest.

Minister **De Jonge**:
Of het een heroverweging moet zijn weet ik niet, maar u heeft me zojuist op de koffie gestuurd bij collega Grapperhaus. De Cybersecuritywet valt onder zijn verantwoordelijkheid. Het is ook een Europese verplichting om die te hebben en daarin essentiële functies aan te wijzen. Ik denk dat het goed is als ik ook dit punt nog eens even herneem en naga of de argumentatie die is gebruikt om tot deze keuze te komen, een adequate argumentatie is. Ik kom ook op dit punt nog terug in antwoord op de heer Hijink.

Mevrouw **Westerveld** (GroenLinks):
Ik had de minister nog gevraagd hoe het zit met jongeren van wie wij vaak horen dat zij graag inzage willen hebben in hun dossier, terwijl ze dat niet krijgen.

Minister **De Jonge**:
De eerste persoon aan wie jongeren dat zouden kunnen melden, zeker als het jongeren zijn die in een instelling zitten, zijn natuurlijk de vertrouwenspersonen. Daarover hebben we uitvoerig gesproken bij de centralisatie van de vertrouwensfunctie. De mensen van AKJ kunnen jongeren hier echt in bijstaan. Een tweede mogelijkheid, als men echt het gevoel heeft dat een instelling hier niet levert, is de inspectie, want de wet moet worden nageleefd en de inspectie heeft daarop toe te zien.

Mevrouw **Westerveld** (GroenLinks):
Is de minister misschien bereid om hier bijvoorbeeld een termijn aan te koppelen voor jongeren die niet meer in de instelling zitten, maar wel hun dossier willen opvragen? Ik krijg van jongeren terug dat ze hiermee bezig zijn, maar dat het soms maanden kan duren voordat ze wat terug horen. Kunnen we de regels niet wat meer aanscherpen en zeggen dat je dossier gewoon binnen drie weken geleverd moet worden als je dat aanvraagt?

Minister **De Jonge**:
Tja. Weet u, dit is de manier waarop er telkens weer nieuwe regels de zorg insluipen. Ik weet niet of we dat moeten doen. Volgens mij is het goed geregeld in die zin dat het AKJ, de vertrouwenspersoon, als die toegankelijk is en ook wordt gebruikt, deze rol kan spelen. Daar hadden we net zo'n mooi amendement voor na ons dispuutje bij de vorige wet. Daarnaast hebben we gewoon de inspectie, die op basis van signalen acteert. In dit geval kan het signaal zowel door de jongere alsook door de betrokken vertrouwenspersoon aan de inspectie worden gegeven, of door iedere andere betrokkene bij die jongeren. Dus mocht u in de mailbox een jongere treffen die met dit verhaal komt, dan zou ik zeggen: laten we zorgen dat het terechtkomt bij de inspectie, opdat de inspectie daarin haar rol kan waarmaken. Dat mag overigens ook via mij.

De heer **Raemakers** (D66):
Ik wilde het net over de mailbox gaan hebben, want ik heb nog twee onbeantwoorde vragen. Ik had de minister gevraagd of hij weet hoeveel jeugdzorginstellingen hun informatie, e-mails en voicemails niet versleutelen, en wat hij daartegen doet. Het belang daarvan is dat gebleken is dat medewerkers van jeugdzorginstellingen informatie gewoon als plain text, dus gewoon als tekst, in een mail naar elkaar of naar anderen doorsturen, en niet in een versleutelde bijlage. Heeft de minister een idee hoe vaak dat voorkomt? En wat kan hij daartegen doen?

Minister **De Jonge**:
Het antwoord heb ik gegeven, namelijk dat wij dat niet weten. Dat kunnen we ook niet weten, want dat zou betekenen dat we een reallifedatabase hebben van de manieren waarop alle tienduizenden zorginstellingen in Nederland hun e-mail beveiligen. Dat kunnen we niet doen. Wel laten we de e-mail-NEN-norm ontwikkelen. Die wordt in mei bekend. Vanaf dat moment is dat de geldende NEN-norm waar alle instellingen in de zorg zich aan te houden hebben, dus ook de jeugdzorginstellingen. Daar kan dan dus ook op worden getoetst. Wie toetst dat vervolgens? Bij een bezoek aan een instelling is dat de inspectie op basis van dat toezichtkader e-health. En als het op basis van een melding is, dan meldt de Autoriteit Persoonsgegevens dat. Het onbeveiligd mailen van dossiers mag gewoon niet. Punt.

De heer **Raemakers** (D66):
Dat is helder. Het is dan toch wel ernstig dat we geen idee hebben hoe vaak het voorkomt. We weten dat het voorkomt

en dat het makkelijk te hacken is. Dat hebben we gezien. Dan zou ik naar mijn tweede onbeantwoorde vraag willen gaan. Het is dus des te belangrijker dat alle medewerkers die bij een jeugdzorginstelling in Nederland werken, weten dat ze dit niet moeten doen. Kan de minister aangeven hoe alle medewerkers van jeugdzorginstellingen worden getraind op cyberveiligheid, cyberhygiëne, zoals dat dan heet? Wat is de rol van de inspectie daarin? En ziet de minister in hetgeen wat er vorige week gebeurd is, ook aanleiding om daar extra acties op uit te zetten?

Minister **De Jonge**:
Ja, ik zie daar wel aanleiding toe, namelijk de extra actie om aan instellingen te vragen om hun eigen risico's in kaart te brengen: kijk nou eens eventjes of wat er in Utrecht is gebeurd, bij jullie ook zou kunnen gebeuren. Wat betekent dat voor de training van je medewerkers die je te doen hebt? Ik weet niet of er trainingen worden gegeven zoals u dat net verwoordde. Het woord "cyberhygiëne" hoor ik voor het eerst, maar ik ga het morgen wel op een onverwacht moment gebruiken en dan kijk ik er heel intelligent bij. Dan zal ik overigens ook aan bronvermelding doen. Maar het gaat erom dat mensen uiteraard getraind moeten worden in het omgaan met gegevensdeling en gegevensbescherming. Dat kent ook een tuchtrechtelijke bescherming in de zorg, in ieder geval voor een groot deel van de zorgprofessionals, zeker ook in de jeugdzorg. Het grootste gedeelte van de mensen in de jeugdzorg valt onder het tuchtrecht.

Dus gegevensdeling en secuur zijn op gegevens is geen kwestie van óf men zich daar druk over zou moeten maken; daar hééft men zich druk over te maken. Dit hoort gewoon bij de professionalisering in de zorg waar werkgevers voor te zorgen hebben. Ik hoop op het volgende en daarom noemde ik ook het woord "wake-upcall". In die zin is Utrecht echt wel een wake-upcall. Dat was een relatief kleine stommiteit met in potentie zulke grote gevolgen. Die lijkt het gelukkig niet gehad te hebben, maar dat had gekund. Daarvan vind ik dat alle instellingen zich druk te maken hebben in de zin van: had dat ook bij ons kunnen gebeuren? Hoe zit het überhaupt met onze dataveiligheid? Wat hebben we daaraan te doen? Wat kunnen wij als werkgever doen in de training van onze medewerkers? Ik denk dat de toezegging aan uw collega's Tielen en Hijink ertoe gaat leiden dat we meer een beeld krijgen over de sector als geheel. Op basis daarvan kunnen we bekijken wat er nog extra nodig zal zijn, maar dat zal dan rond de zomer zijn.

De heer **Edgar Mulder** (PVV):
Ik ga net als de minister ook een paar dingen oplezen, maar voordat ik dat doe nog iets over die wake-upcall. Het lijkt me een beetje laat. In 2017 heeft exact ditzelfde met domeinadressen gespeeld binnen de politie, dus het was allang bekend. Waarschijnlijk heeft die brandweerfunctie dus niet goed gewerkt. Los daarvan staat in de AVG, waar iedereen aan moet voldoen, gewoon beschreven hoe je gevoelige content moet versturen: "Content van unencrypted e-mails mag nooit gevoelige informatie bevatten." Als er volautomatisch e-mails gegenereerd worden, minister, dan staat er in een e-mail altijd een link die verwijst naar een websysteem waar de ontvanger zich op een of andere wijze moet identificeren. Afhankelijk van je rechten mag je dan informatie inzien. Dus ja, een medewerker moet leren dat hij niet zomaar gevoelige informatie verstuurt, maar een fatsoenlijke ICT-oplossing à la 2019 helpt wel. We zijn niet meer bij MS-DOS en de Atari. We zitten in 2019. We gaan naar Mars. Je kan gewoon een systeem maken. De jeugdzorginstelling, ook in Utrecht, heeft gewoon een dure ICT-afdeling met een ICT-directeur en een ICT-medewerker. Die moeten hier gewoon aan voldoen. Dan hadden wij al uw woorden van het afgelopen uur niet nodig gehad. Gewoon voldoen aan uw eigen regels!

Minister **De Jonge**:
Het is bijna aandoenlijk dat u denkt dat als iets in een wet staat, het dan ook morgen in de werkelijkheid gebeurt. Dat is namelijk niet zo. Je zult altijd extra dingen moeten doen om ervoor te zorgen dat de werkelijkheid zich op enig moment verhoudt tot de wet. Daar ging volgens mij ons debat van de afgelopen anderhalf uur over. In dit geval mag het natuurlijk niet. Onbeveiligd mailen mag natuurlijk niet, maar we weten dat het wel gebeurt. Wat er aan extra actie is ingezet vanuit het departement, is dat er om een NEN-norm is gevraagd met eisen waaraan aanbieders die dat soort beveiligde mailapplicaties daadwerkelijk leveren aan instellingen — dat zijn gewoon commerciële instellingen — hebben te voldoen opdat het voldoende veilig is. Dus: ja, we hebben de wet, de AVG. Daarnaast hebben we een NEN-norm, waaraan al die applicaties die worden ingehuurd hebben te voldoen. Vervolgens hebben die applicaties op een adequate manier gebruikt te worden door medewerkers in de zorg. Dat is een kwestie van regelgeving maar ook een kwestie van houding en gedrag. Het is ook een kwestie van scholing, zoals de heer Raemakers aangeeft. Kortom, alleen met wetten kom je er niet.

De heer **Edgar Mulder** (PVV):
Nee, zeker niet als we geen poging doen om ze te handhaven en te controleren, maar we zullen zo meteen een motie indienen om de minister daartoe te dwingen. Wat uw verhaal betreft dat het aandoenlijk is dat wij denken dat het met wetten opgelost is: op het moment dat wij hierover vragen stellen, komt de partij waardoor u de wei bent in gestuurd ook nog eens met de opmerking dat we om meer regels vragen. Dat is natuurlijk niet zo. We willen gewoon dat er gecontroleerd wordt wat we gezamenlijk hebben afgesproken. Dat is een taak die u heel serieus zou moeten nemen.

Minister **De Jonge**:
Die neem ik ook serieus. Maar bij uitstek de zorg is mensenwerk. Wetten geven geen zorg, stelsels geven geen zorg, beveiligde systemen geven ook geen zorg, maar mensen geven zorg en die maken weleens fouten. Het gedrag en de houding van mensen is zeker zo belangrijk als wetten. Daarom herhaal ik wat uw collega, mevrouw Kuiken, zojuist zei: het gaat om gezond verstand. Het gaat om gezond verstand in de first place. Een ander behandelen zoals je zelf graag behandeld wilt worden als het gaat om het delen van gegevens in de zorg.

Mevrouw **Van Kooten-Arissen** (PvdD):
De minister gaf wel heel snel antwoord op mijn vraag over de motie. Hij zei: minister Bruins komt erop terug. De motie vroeg inderdaad om een NEN-norm in verband met end-to-endencryptie, maar ook om een onderzoek naar welke

systemen dit al mogelijk kunnen maken. Daar is de minister niet op ingegaan. Dat zou ik graag nog heel even van hem willen horen.

Minister **De Jonge**:
Voorzitter. Dan vraag ik uw permissie om daar in tweede termijn op terug te mogen komen, want u overvraagt me hiermee een beetje.

De **voorzitter**:
Ja. Wilt u met z'n allen meteen doorgaan met de tweede termijn? Dat is het geval. Dan geef ik graag het woord aan mevrouw Westerveld, die als eerste spreekt. Zij heeft een derde van haar spreektijd uit eerste termijn, ruwweg 1 minuut en 30 seconden. Het woord is aan haar.

Mevrouw **Westerveld** (GroenLinks):
Voorzitter, dank u wel. Ik dank ook de minister voor de antwoorden. Het is goed dat we het probleem serieus nemen: het probleem dat er in de zorg veel misgaat ten aanzien van de privacy van heel gevoelige gegevens. Er had hier iets heel grondig mis kunnen gaan als klokkenluiders maar ook RTL niet zo deskundig en goed met de gegevens waren omgegaan.

We hadden een aantal moties in voorbereiding. Die ga ik niet indienen, want ik ben best tevreden met een heel aantal antwoorden van de minister op mijn vragen. Ik zie de minister een beetje verbaasd kijken.

De **voorzitter**:
Ik heb hem nog nooit zien stralen.

Mevrouw **Westerveld** (GroenLinks):
Ik hoor ook van een aantal collega's dat ze een aantal voorstellen zullen doen die we wellicht zullen steunen.

Voorzitter. Ik heb nog wel twee vragen aan de minister. Tijdens het debat kwam mij de informatie ter ore dat veel ouders en jongeren niet op de hoogte zijn gesteld. Het gaat daarbij juist om deze regio. Ouders en jongeren zitten dus nog steeds in onzekerheid over wat er met hun gegevens is gebeurd en vragen zich af of hun gegevens wel veilig zijn. Zou de minister daar nog op in kunnen gaan? Het lijkt me van het grootste belang dat mensen weten of hun gegevens veilig zijn.

Voorzitter, dan mijn tweede punt. De minister gaf aan dat er ongeveer 6.000 aanbieders zijn en stelt in zijn plan van aanpak dat hij een groot deel daarvan via Jeugdzorg Nederland wil bereiken. Nu heeft Jeugdzorg Nederland een flink aantal leden, maar niet al die 6.000 aanbieders vallen daaronder. Ik zou de minister dus nog willen vragen hoe hij ook die andere gaat bereiken. Als het gaat om de gegevens van jongeren is veiligheid namelijk heel belangrijk. We moeten er echt voor zorgen dat alle instellingen goed op de hoogte zijn.

De **voorzitter**:
Dank u wel. Dan de heer Edgar Mulder van de fractie van de Partij voor de Vrijheid.

De heer **Edgar Mulder** (PVV):
Voorzitter. In mijn inleiding vroeg ik aan de minister of hij bereid was om alle jeugdzorgbureaus door te lichten. De minister kwam daar in zijn tweede blok op terug door te zeggen dat hij themaonderzoek wil laten doen door toezichthouders. Dat zie ik als een toezegging. Ik wil dat nog motiveren met de volgende motie.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat naast de jeugdzorginstelling Samen Veilig Midden-Nederland ook andere instellingen in de fout zijn gegaan inzake de beveiliging van medische gegevens en de uitwisseling van privacygevoelige informatie;

verzoekt de regering alle jeugdzorginstellingen door te lichten of zij voldoen aan de Algemene verordening gegevensbescherming en de Kamer hierover voor het einde van het jaar te informeren,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Edgar Mulder. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 638 (31839).

De heer **Edgar Mulder** (PVV):
En dan de beroemde kers.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat de jeugdzorginstelling Samen Veilig Midden-Nederland ernstig in de fout is gegaan in de omgang met de medische gegevens van hun cliënten;

van mening dat waarborgen omtrent veiligheid en privacybewaking bij deze jeugdzorginstelling in hoge mate ontbreken;

verzoekt de regering de jeugdzorginstelling Samen Veilig Midden-Nederland onder verscherpt toezicht te stellen, en de Kamer maandelijks te informeren over de stand van zaken,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Edgar Mulder. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 639 (31839).

De heer **Edgar Mulder** (PVV):
Dank u wel.

De **voorzitter**:
Dan de heer Hijink van de fractie van de SP.

De heer **Hijink** (SP):
Voorzitter. Ik denk dat wij de klokkenluiders en de journalisten die het datalek in Utrecht aan het licht hebben gebracht dankbaar kunnen zijn voor de zorgvuldige manier waarop ze dat hebben gedaan, maar ook voor het feit dat ze ons allemaal weer eens even wakker hebben geschud over hoe het met de dataveiligheid met de zorg is gesteld. Uiteindelijk is de instelling zelf natuurlijk verantwoordelijk voor de veiligheid van de data. Maar we zien dat iedereen, waaronder de gemeenten, de Autoriteit Persoonsgegevens en de inspectie, betrokken is en een bepaalde verantwoordelijkheid heeft, maar dat het uiteindelijk ontbreekt aan iets of iemand die onverwacht en onaangekondigd kan testen of de data in goede handen is. De minister wil een soort van onderzoek om te kijken wat de inspectie mogelijkerwijs zou kunnen. Wij denken — en dan spreek ik ook namens collega Raemakers — dat we een stap verder moeten gaan en dat het testen onderdeel zou moeten worden van het reguliere toezicht. Daarom de volgende motie.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat datalekken in de gezondheidszorg ernstige gevolgen hebben voor zorgbehoevende kinderen en volwassenen;

overwegende dat het van belang is om proactief in alle zorgsectoren de gegevensbescherming te testen op veiligheid en toegang door onbevoegden;

verzoekt de regering in samenwerking met brancheorganisaties, cybersecurityexperts en ethische hackers, de Autoriteit Persoonsgegevens en de Inspectie Gezondheidszorg en Jeugd pentests te laten uitvoeren bij zorgorganisaties in alle zorgsectoren, om zo te onderzoeken of zij toegang kunnen krijgen tot medische dossiers, waarbij ingezet wordt op minimaal inzicht in toegankelijk gemaakte medische dossiers,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Hijink en Raemakers. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 640 (31839).

Mevrouw Van Kooten-Arissen ziet af van haar spreektijd. Dan mevrouw Tielen.

Mevrouw **Tielen** (VVD):
Dank, voorzitter. Ook dank aan de minister. Wat mij betreft was de bedoeling van het debat van vanavond om het vertrouwen en de veiligheid van persoonsgegevens aan de orde te stellen en daarmee ook weer een zeker vertrouwen terug te brengen bij de mensen in het land. Wat dat betreft had ik vanavond ook een aantal heldere uitspraken nodig van deze minister om dat te kunnen doen. In het debat laat de minister in ieder geval urgentie zien, misschien wat meer dan in de brief. Dat doet mij deugd, want dat wilde ik ook graag zien. Dat is dus mooi. Ik heb nog wel een paar vragen. De minister spreekt over de onderzoeken die worden gedaan door SAVE Midden-Nederland en de betrokken regiogemeenten. Ik ben heel benieuwd wanneer die beschikbaar zijn, omdat die ons wellicht ook weer meer inzicht geven wat betreft andere instanties.

Ik heb de minister ook heel duidelijk horen zeggen — meneer Mulder gaf dat ook al aan — dat de betrokken autoriteiten, de IGJ en de Autoriteit Persoonsgegevens, een proactief en thematisch onderzoek zullen uitvoeren naar e-health en het gebruik van data in de jeugdzorg. Wanneer kan de minister enige uitkomsten daarvan met ons delen? Wat mij betreft op zijn laatst rond de zomer.

Voorzitter. Ik heb nog een extra toezegging nodig en ik heb twee cliffhangers. Ik zou, ten eerste, graag willen dat de minister, als hij toch in gesprek gaat met de Inspectie Gezondheidszorg en Jeugd en de Autoriteit Persoonsgegevens, deze autoriteiten er ook toe oproept duidelijk te maken dat jongeren en andere mensen met signalen over dataonveiligheid ook daadwerkelijk bij hen terechtkunnen.

Dan de twee cliffhangers. Morgen is er een debat in de gemeenteraad van Utrecht. Ik krijg nog steeds signalen van mensen in de regio Utrecht dat zij hierover niet zijn geïnformeerd door SAVE. Laten we de gemeenteraad van Utrecht oproepen om dat ook daar neer te leggen. Dan de tweede. Is het mogelijk om een dossier of delen van een dossier gewoon te laten vernietigen? Daar hoef ik nu geen antwoord op, maar ik kom daar graag volgende week op terug.

Dank u wel.

De **voorzitter**:
Dank u wel. Dan de heer Raemakers van de fractie van D66.

De heer **Raemakers** (D66):
Voorzitter, dank u wel. We hebben een goed debat gehad over een heel ernstige zaak. D66 is het met de minister eens dat digitalisering heel waardevol kan zijn. We zijn het er

ook mee eens dat cyberveiligheid een randvoorwaarde moet zijn. Maar ik zie een minister die er nog niet genoeg bovenop zit, die te veel afwacht. Eerder moest de Kamer de minister ook al aansporen om ervoor te zorgen dat alle zorginstellingen aangesloten werden op Z-CERT. En nu sporen collega Hijink en ik de minister aan om ervoor te zorgen dat alle organisaties structureel met pentesten werken. We hebben dat ook vastgelegd in een motie. Maar ik verwacht nog meer. Daarom de volgende motie.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat zorg- en ICT-experts aangeven dat het slecht gesteld is met de cyberveiligheid in de zorg;

overwegende dat de jaarcijfers van de Autoriteit Persoonsgegevens laten zien dat zorg en welzijn een van de sectoren is waar de meeste datalekken worden gemeld;

constaterende dat cyberaanvallen, zoals WannaCry, regelmatig leiden tot datalekken en verstoring van de zorgverlening;

verzoekt de regering voor de zomer te komen met een plan van aanpak om de cyberveiligheid in de gehele zorgsector op een hoger niveau te brengen door middel van een breed palet van maatregelen, waaronder het versterken van Z-CERT, verplichte deelname van zorginstellingen aan Z-CERT, training van medewerkers op cyberhygiëne, het versterken van de inspectie op het gebied van cyberveiligheid en periodieke pentests bij zorginstellingen,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Raemakers. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 641 (31839).

De heer **Raemakers** (D66):
Dank u wel.

De **voorzitter**:
De laatste spreker van de zijde van de Kamer is de heer Peters van de fractie van het CDA.

☐

De heer **Peters** (CDA):
Dank u wel, voorzitter. We hebben een debat gehad over de misstanden ... Nee, dat hadden we vanmiddag. We hadden het nu over een datalek. We nemen het allemaal heel serieus. Ik heb de minister, geloof ik, zelfs wel vijftien keer horen zeggen dat hij het erg serieus neemt. Ik hoorde overigens ook dat hij geen garanties kan geven, hoewel dat toch steeds van hem wordt gevraagd.

Voor mij en voor het CDA heeft verantwoordelijkheid te maken met antwoord geven. Wat doe je nou als instelling aan een zorgvuldige omgang met data? Hoe gebruik je je gezond verstand, zoals een paar keer werd gezegd? Volgens het CDA werkt die verantwoordelijkheid via het subsidiariteitsbeginsel: in eerste instantie is de persoon zelf, de medewerker, verantwoordelijk, dan de instelling, dan de opdrachtgever, dan de inspectie en in laatste instantie de minister als stelselverantwoordelijke. Ik had vanavond wel af en toe het idee dat we denken dat de minister het hoogstpersoonlijk allemaal zelf moet gaan doen. Ik denk niet dat dat kan.

We stellen ook allemaal vragen. Meer onderzoeksvragen. Hoe vaak komt iets voor? Dan moeten we gaan turven. Controle van alle instellingen. Wie gaat dat doen? Hoeveel tijd gaat dat kosten? Wat gaan we daarmee doen? We gaan hacken en dan gaan we het in de krant zetten, zo heb ik meneer Hijink horen zeggen. De vraag is: wat doet dat dan met het vertrouwen van mensen? Ik denk er anders over. Daarom de volgende motie.

Motie

De Kamer,

gehoord de beraadslaging,

overwegende dat fouten zoals het datalek bij Samen Veilig Midden-Nederland doorgaans het gevolg zijn van een menselijke fout en/of het niet goed navolgen van al bestaande regels en protocollen;

overwegende dat als dergelijke fouten aan het licht komen de reflex doorgaans is dat er nieuwe, strengere regels moeten komen;

van mening dat deze risicoregelreflex op termijn meer schade veroorzaakt omdat het risicomijdend gedrag en bureaucratie in de hand werkt;

verzoekt de regering met organisaties in de jeugdzorg in gesprek te gaan over het beter naleven van de bestaande regels en protocollen en alleen over te gaan tot nieuwe regelgeving als er daadwerkelijk een gemis in de bestaande regels wordt geconstateerd,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Peters. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 642 (31839).

Mevrouw **Westerveld** (GroenLinks):
De heer Hijink, de heer Raemakers en ik sprongen alle drie tegelijk op omdat dit een beetje raar is. Ik heb een aantal mensen hier horen zeggen dat we bestaande regelgeving beter moeten naleven, dat we moeten inzetten op bestaande instrumenten. Ik heb volgens mij niemand een nieuwe set aan regels horen voorstellen in moties, maar wel een aantal pilots.

De heer **Peters** (CDA):
Een breed palet aan nieuwe regels.

De **voorzitter**:
Even wachten.

Mevrouw **Westerveld** (GroenLinks):
Voorzitter, ik vind dit een heel bijzondere motie en ik wil aangeven dat wij dit debat op een goede manier hebben gevoerd, dat we als Kamer verantwoordelijk zijn om de minister te controleren. Ik heb hier niet een hele nieuwe set aan regels gehoord en ik zou daar afstand van willen doen. Dat is natuurlijk niet aan mij, maar ik denk dat mijn punt duidelijk is.

De heer **Peters** (CDA):
Geen steun van GroenLinks voor deze motie.

De **voorzitter**:
Sorry?

De heer **Peters** (CDA):
Maar mag ik daarop reageren, want ik heb net nog een motie gehoord waarbij gevraagd werd naar een heel breed palet aan nieuwe maatregelen, dus ja. Maar goed, dat heeft u niet gehoord.

De heer **Hijink** (SP):
Ik stoor me echt aan de niks-aan-de-handhouding van de heer Peters. U zegt dat we een heel serieus debat hebben gehad, maar uit uw inbreng in eerste termijn en ook nu weer maak ik alleen maar op dat u zegt: met een beetje gezond boerenverstand komt het allemaal wel goed. Daar gaat het natuurlijk juist niet om. Collega Raemakers en ik vragen om pentesten, om meer controle en toezicht, maar dat is geen nieuwe set van regels. Dat is dat er iets of iemand op een bepaald moment opstaat om toe te zien dat de regels die er zijn, ook nageleefd worden. Dat er iets of iemand is die op het moment dat er risico's bestaan op gevaarlijke dataleks bijtijds kan ingrijpen en dat we hier niet iedere keer staan als het kalf al verdronken is. Dat is precies waar het hele debat over ging. Ik vind dat de heer Peters niet alleen zichzelf hier tekort doet, maar ook het hele debat neerzet als "laten we een beetje gezond verstand gebruiken, dan komt het wel goed." Ik vind dat echt slecht.

De heer **Peters** (CDA):
Als ik dat zou hebben gedaan, zou dat ook slecht zijn, meneer Hijink. Ik heb dat niet willen doen. Ik heb ook een paar keer gezegd dat zorgvuldig omgaan met data uiterst belangrijk is, zeer belangrijk. U heeft het gezegd, ik heb het gezegd, iedereen heeft het gezegd: dit had gierend fout kunnen gaan tot enorme schade van heel veel mensen. Dat vind ik dus heel belangrijk. Wat ik heb proberen te aan te geven, en ik zeg het hier nog een keer, is onze reflex voor nieuwe regels. Ik heb het even niet over uw motie, want die gaat niet over nieuwe regels. Ik heb er net een paar genoemd: controle van alle instellingen, een breed palet aan nieuwe maatregelen. Dat verzin ik niet, dat zijn moties die net zijn ingediend. Ik reageer daarop en ik zeg: volgens mij is het heel belangrijk om te zorgen dat we de bestaande regels goed handhaven en dat mensen doen waarvoor ze zijn opgeleid en wat ze zouden moeten doen.

De **voorzitter**:
De heer Raemakers nog even heel kort, want ik denk dat het punt is gemaakt.

De heer **Raemakers** (D66):
Ik heb eigenlijk maar één, hele korte vraag aan de heer Peters, aan het CDA. Vertrouwt u gemeenten, vertrouwt u instellingen altijd op hun blauwe ogen?

De heer **Peters** (CDA):
Nee, natuurlijk niet. Bij vertrouwen hoort een zekere mate van controle, maar dat betekent niet dat we alles tot op de vierkante centimeter kunnen controleren of garanties kunnen geven. U stelt een vraag waar ik het mee eens ben. Nee, ik vertrouw niet altijd iedereen op zijn blauwe ogen.

De **voorzitter**:
Heel goed. Was dit uw bijdrage?

De heer **Peters** (CDA):
Ja hoor.

De **voorzitter**:
Hartelijk dank daarvoor. Kan de minister meteen antwoorden op de moties en zo? Hij had zesenhalve minuut gevraagd. Zijn tijd gaat nu in.

De vergadering wordt van 22.59 uur tot 23.05 uur geschorst.

De **voorzitter**:
Het woord is aan de minister.

Minister **De Jonge**:
Voorzitter, dank u wel. Dank ook voor de vragen en de moties die zijn ingediend in de tweede termijn. Volgens mij was het een goed en grondig debat en hebben we werk te doen. Ik ga daar graag mee aan de slag. Ik denk dat het voor nu goed is als ik de vragen geef op de antwoorden, sorry, andersom, de antwoorden geef op de vragen die zijn gesteld —het is een latertje vandaag — en de moties van een oordeel van het kabinet zal voorzien.

Eerst is er de vraag van GroenLinks, en dat is eigenlijk dezelfde vraag die ook mevrouw Tielen stelde, over de ouders die kennelijk nog niet in alle opzichten geïnformeerd zijn. Ik heb zojuist aangegeven dat de ouders worden geïnformeerd via een algemeen bericht op de site van SAVE Midden-Nederland. Daarnaast is er een apart e-mailadres en telefoonnummer geopend waarop iedereen kan vragen hoe het met zijn of haar gegevens zit. Daarnaast kunnen in het dagelijks contact tussen SAVE Midden-Nederland en ouders en kinderen dit soort vragen aan de orde komen. Alle medewerkers zijn daarop berekend. Als het gaat over brieven die sowieso gestuurd worden, zal er altijd een informatievel bijgevoegd zijn waarop deze zaak nader wordt toegelicht. Er wordt bijgehouden of een cliënt zo'n brief heeft ontvangen wegens het ontvangen van überhaupt correspondentie van SAVE Midden-Nederland. Daarnaast

zijn de gezinswerkers van de buurtteams geïnformeerd. Dat is ongeveer wat je zou kunnen doen om de groep zo goed mogelijk te bereiken.

Tegelijkertijd heeft SAVE Midden-Nederland natuurlijk ook oud-cliënten die willen weten hoe het zit. Die kunnen niet op voorhand allemaal proactief worden benaderd, omdat er adressen gewijzigd kunnen zijn. Als je per ongeluk het risico neemt om naar een oud adres te mailen of te schrijven, ga je juist een gegevenslek creëren. Het kan inderdaad zo zijn dat er ouders of kinderen zijn die nog niet geïnformeerd zijn. De beste oplossing is dan om zelf, mocht u dat soort signalen krijgen, actie te ondernemen in de richting van SAVE Midden-Nederland, via dat e-mailadres of telefoonnummer die op de website genoemd staan. Daarnaast zal ik dat signaal zoals u het overbrengt ook weer overbrengen aan Utrecht opdat men daarnaar kan handelen.

GroenLinks maakte een terecht punt over de aanbieders die geen lid zijn van Jeugdzorg Nederland. Die moeten we natuurlijk wel willen bereiken. Ik ga kijken op welke manier we dat kunnen doen, via andere brancheorganisaties. Er is een brancheorganisatie voor kleine jeugdzorgaanbieders, maar als je die optelt heb je ze ook weer niet allemaal te pakken. We gaan zo goed als mogelijk zorgen dat we alle aanbieders bereiken.

Dan kom ik bij de motie op stuk nr. 638 van de PVV, die vraagt om alle jeugdzorginstellingen door te lichten of zij voldoen aan de AVG en de Kamer hierover te informeren. In het licht van het thematisch onderzoek wat ik heb toegezegd, lijkt me dit overdoing en daarnaast niet zo makkelijk uitvoerbaar, want het gaat om ruim 6.000 jeugdzorginstellingen. Dat lijkt mij een tamelijk onuitvoerbaar gebeuren. Deze motie ontraad ik.

De motie op stuk nr. 639 verzoekt de regering om de jeugdzorginstelling Samen Veilig Midden-Nederland onder verscherpt toezicht te stellen. Zo werkt het natuurlijk niet. De inspectie doet constateringen en kan op basis daarvan overgaan tot handhavingsmaatregelen. De inspectie is onafhankelijk in haar oordeel en onafhankelijk in het treffen van maatregelen, gelukkig maar. Dus deze motie ga ik ook ontraden.

Dan hebben we de motie op stuk nr. 640. De SP verzoekt de regering hierin om in samenwerking met brancheorganisaties, cybersecurity-experts en ethische hackers de AP en de Inspectie voor de Gezondheidszorg en Jeugd pentests te laten uitvoeren bij zorgorganisaties. Als u bedoelt dat te doen in het licht van een thematisch onderzoek zoals ik u heb aangegeven bereid te zijn om te doen, kan ik het oordeel aan de Kamer laten. Ik ga er geen aparte actie of apart onderzoek op uitvoeren. Als u dat bedoelt, laat ik het oordeel aan de Kamer.

De heer **Hijink** (SP):
Ja, waarbij ik dan wel zou willen meenemen dat mijn gedachte erbij is dat dit een onderdeel kan worden van de werkwijze van de inspectie, ook na het onderzoek dat de minister voorstelt.

Minister **De Jonge**:
Ja, dat zou kunnen, maar we bekijken op grond van het thematisch onderzoek of dat iets toevoegt en of het noodzakelijk is. In die context laat ik het oordeel aan de Kamer.

Dan heb ik de motie op stuk nr. 641 die de regering verzoekt om voor de zomer te komen tot een plan van aanpak om de cyberveiligheid in de gehele zorgsector op een hoger plan te brengen door middel van een breed palet aan maatregelen, waaronder het versterken van Zorg-CERT, verplichte deelname aan Zorg-CERT, training van medewerkers op cyberhygiëne, het versterken van de inspectie op het gebied van cyberveiligheid en een periodieke pentest.

Je kunt op een aantal manieren naar deze motie kijken. Je kunt zeggen dat het wel ongeveer is wat ik zojuist tijdens het debat heb uitgelegd om te gaan doen. We zullen dat thematische onderzoek doen. Daarbij zullen pentests aan de orde zijn. We zullen zorgen dat wij met de gemeente en met Jeugdzorg Nederland kijken wat we moeten versterken op basis van hun eigen observaties: welke risico's zijn er en welke risico's moeten worden weggenomen? We zullen de verplichting om deel te nemen aan Zorg-CERT onderzoeken. Daar was al een motie over ingediend door mevrouw Ellemeet. Ik heb aangegeven: het is niet zozeer de vraag of, maar meer de vraag hoe we dat gaan doen. Met welke implicaties komen we erachter weg en hoe zullen we dat doen? Als je er op zo'n manier naar kijkt, dan is dat ongeveer wat we van plan zijn te doen. Maar ik denk wel dat we het echt op die manier moeten doen.

Om op voorhand een heel groot plan te bestellen, terwijl we eigenlijk eerst met Jeugdzorg Nederland — en een zo breed mogelijk bereik natuurlijk in de jeugdzorgsector — moeten kijken wat er extra nodig is. Ook op basis van het themaonderzoek moeten we kijken wat er extra nodig zal zijn. Dan vind ik het in de volgorde der dingen het beste als we dat eerst gaan doen en daarna, op basis daarvan, kijken welk plan van aanpak het beste passend is. In die volgorde. Om nu gelijktijdig aan de acties die we uitzetten een plan van aanpak te maken, lijkt me niet verstandig. Ik denk dat we dan heel veel drukte tegelijkertijd gaan organiseren, ook voor de instellingen die dit allemaal moeten verstouwen. Het is namelijk niet de enige opdracht die ze van ons meekrijgen. We hebben eens in de zoveel weken een jeugdzorgdebat.

De heer **Raemakers** (D66):
Deze motie moet ook echt in de context worden gezien van het debat dat we vanavond hebben gevoerd over de brief die vorige week door minister Bruins is uitgezet. Minister De Jonge heeft vanavond gezegd: ik zal nog eens kijken naar die brief, of er voldoende wordt ingegaan op cyberveiligheid. Ik heb de brief er ook nog even bij gepakt. Er staat een hele korte passage in over cyberveiligheid. Dat komt in de verste verte niet in de buurt van wat wij willen. Het woord "privacy" wordt niet eens in de brief genoemd. Ik heb dus een voorwaardelijke toezegging gekregen vandaag. Die vind ik eigenlijk onvoldoende. In dat licht moet deze motie gezien worden. Voor de zomer moet er echt een nadere invulling van die brief van vorige week komen. Daar moeten deze elementen allemaal in meegenomen worden en er moet voor gezorgd worden dat het allemaal voor de zomer gebeurd is. Dat ter verduidelijking.

Minister **De Jonge**:
Ja, dat maakt het overigens in het oordeel niet makkelijker. Ik heb gezegd dat je er op een aantal manieren naar kunt kijken. Of het is ongeveer wat we gaan doen, maar dan zou ik zeggen: laten we de dingen in de goede volgorde doen. Namelijk eerst het themaonderzoek om te kijken wat er extra nodig zou zijn. Daar worden pentests bij betrokken. Daarnaast de acties die we in samenwerking met de VNG, Jeugdzorg Nederland en de andere brancheorganisaties gaan ondernemen. Maar ik zou het in de juiste volgorde willen doen. Ik zou dat eerst willen doen en dan kijken wat er als plan van aanpak nodig is. Nu verwijst u echter naar die brief van vorige week. Die gaat over het verplicht maken van gegevensstandaarden bij uitwisseling van data in de zorg. Ik zie niet goed wat de motie en de brief met elkaar te maken hebben. De brief gaat over het digitaliseren van de zorg en dat is een ander soort thema dan waar het debat vanavond over ging. Dit was een zijspoortje in dat debat en daarover heb ik gezegd: veiligheid is een conditio sine qua non. Is er dan voldoende aandacht aan besteed in die brief? U heeft hem al kunnen nalezen, ik nog niet. Ik heb gezegd dat ik de brief zal gaan nalezen en dat ik erop terugkom. Ik zal u een aanvullende brief schrijven waarin staat dat we de brief gaan schrijven over de gegevenswisseling, de veiligheid en hoe we dat waarborgen. Dat heb ik u al toegezegd, maar dat zie ik echt als iets anders dan de motie die u hier voor u heeft.

De heer **Raemakers** (D66):
Dat is juist het punt. Hier staat duidelijk om tot een plan van aanpak te komen om de cyberveiligheid in de gehele zorgsector op een hoger niveau te brengen. Dat gaat er juist over dat als wij de gegevensuitwisseling, ook elektronisch, makkelijker willen maken — en dat moeten we echt doen — de randvoorwaarde altijd moet zijn dat de veiligheid in orde is. Het lek van vorige week laat zien dat we daar gewoon meer stappen in moeten nemen. De minister schuift in zijn antwoord opnieuw een aantal zaken af. Hij wil weer eerst een aantal dingen onderzoeken. Daarom heb ik het op schrift gesteld en daarom heb ik deze motie ingediend: om heel duidelijk aan te geven wat D66 vindt dat er voor de zomer moet gebeuren, dus zoals het er staat.

Minister **De Jonge**:
Dan denk ik dat het het beste is om de motie gewoon te ontraden, want anders gaan we een hele exegetische toestand krijgen over wat we precies moeten lezen in deze motie. Ik denk dat wat we doen, ongeveer is wat hier staat, zij het dat ik het graag in de goede volgorde wil doen. Ik wil niet een thematisch onderzoek en een plan van aanpak door elkaar laten lopen, maar eerst het een doen om te kijken wat je in het ander moet opschrijven. Dus eerst een thematisch onderzoek doen om te kijken wat je in het plan van aanpak moet opschrijven. Die volgorde vind ik altijd een aardige manier van werken. Deze motie stelt het eigenlijk andersom, of in ieder geval gelijktijdig. Dat spreekt mij wat minder aan en daarom hecht ik net iets meer aan datgene wat ik zojuist aan u heb toegezegd.

De vraag over veiligheid, gegevensuitwisseling en databescherming en het verplicht maken van die gegevensstandaarden, vind ik echt een andere vraag. Ik ga en kan die ook echt los beantwoorden. Daarvoor zal ik de brief nog een keer goed nalezen. Overigens komt voor de zomer al de derde brief over gegevensuitwisseling. Ik zal zorgen dat daarin in ieder geval uitvoerig op veiligheid wordt ingegaan. Maar in de context van het een, namelijk de toezeggingen die ik al heb gedaan, en de context van de andere toezegging die ik al heb gedaan, ga ik deze motie ontraden, ook om allerlei mystificatie te voorkomen.

Voorzitter. Dan de motie op stuk nr. 642 van de heer Peters, waarin wordt gevraagd om met organisaties in gesprek te gaan over het beter naleven van de bestaande regels en alleen over te gaan tot nieuwe regels als er daadwerkelijk een gemis in de bestaande regels wordt geconstateerd. Daar zou ik een beetje op dezelfde manier op kunnen reageren. Je kunt daar namelijk ook op twee manieren naar kijken. Dat is ook wel hoe ik erin zit. Regels kunnen soms nodig zijn. Een eventuele verplichting om bijvoorbeeld allemaal deel te nemen aan Zorg-CERT zou echt een nieuwe regel zijn, die ik om die reden ook goed op de implicaties zou willen onderzoeken voordat we die met elkaar treffen. Je zou ook kunnen zeggen: laten we ook hier de dingen in de goede volgorde doen. Laten we aan de slag gaan zoals ik zojuist heb toegezegd, goed kijken wat er extra nodig is, en daarna een plan van aanpak maken. Vervolgens is het weer aan u om elkaar en om mij scherp te houden en de vraag te stellen: gaan we niet voor niks nieuwe regels bedenken? Ik zou u willen vragen: heeft u deze motie echt nodig om erop te kunnen vertrouwen dat het kabinet de juiste dingen doet? Dat is een gewetensvraag.

De heer **Peters** (CDA):
Nee, voorzitter. Ik vertrouw erop als de minister zegt het in de geest van wat we hebben gezegd te gaan doen. Dan trek ik de motie terug.

Minister **De Jonge**:
Dank u wel.

De **voorzitter**:
Aangezien de motie-Peters (31839, nr. 642) is ingetrokken, maakt zij geen onderwerp van beraadslaging meer uit.

Minister **De Jonge**:
Das war es dann: aan het werk! Dank.

De **voorzitter**:
Nou, niet te vroeg juichen, want we hebben mevrouw Tielen nog in de aanbieding voor u.

Minister **De Jonge**:
Excuus. Ik sta heel dapper mijn stapeltje moties door te werken, terwijl ik een hele lijst aan vragen heb van mevrouw Tielen.

De **voorzitter**:
Ja, en iedereen accepteerde het.

Minister **De Jonge**:
Leek het te accepteren.

Mevrouw **Tielen** (VVD):
Met uitzondering van. Die cliffhanger is voor volgende week, dus daar hoeft u niet op te reageren, maar wel nog even op de vraag wanneer de onderzoeken rondom SAVE beschikbaar zijn en op de vraag over het gesprek met de IGJ en AP over de mogelijkheid voor meldingen van mensen uit het land.

Minister **De Jonge**:
Ja. Eén is het onderzoek van SAVE en van Utrecht. Ik verwacht dat rond de zomer. Zodra die onderzoeken er zijn, zal ik u op basis daarvan ook berichten over wat de te trekken lessen zijn. Ik hoop ook een beetje rond de zomer, want dat zou betekenen dat ik dat kan combineren met de uitkomsten van de gesprekken die wij hebben met de VNG en met Jeugdzorg Nederland. Dan kan ik daaruit destilleren wat er aan extra acties moet worden ondernomen.

Het tweede punt betreft een vraag die u in eerste termijn al stelde en waar ik in mijn eerste termijn onvoldoende op heb gereageerd. Is het nu helder voor iedereen waar men zich kan melden? Men kan zich melden bij de inspectie en men kan zich melden bij de AP. Het kan dus allebei en het zou eigenlijk niet uit moeten maken wie van de twee men belt: "no room door" moet daar het uitgangspunt zijn, want de inspectie en de AP hebben hier allebei werk te doen. Als het elkaars werk is, dan is het aan de inspectie en de AP om dat onderling op te lossen. Ik heb mij laten verzekeren dat dat onderling ook op die manier geregeld is. Wie je ook belt, er wordt even achter de schermen contact gezocht opdat de vraag ook adequaat kan worden opgepakt.

De vraag over de informatie heb ik eigenlijk al beantwoord in de richting van mevrouw Westerveld.

Dan kom ik op de cliffhangervraag, maar laten we die volgende week behandelen, want het antwoord is vrij gedetailleerd en vrij lang. Maar het antwoord is een vorm van "ja": het is inderdaad mogelijk om dingen te vernietigen.

De **voorzitter**:
Een vorm van "ja".

Minister **De Jonge**:
Onder condities.

De **voorzitter**:
Mevrouw Van Kooten-Arissen, gaat u het even aftoppen vandaag voor ons? Kom er maar in.

Mevrouw **Van Kooten-Arissen** (PvdD):
Voorzitter, dank u wel. Ik heb nog geen antwoord gehoord op een vraag over mij motie over de end-to-endencryptie. Het ging dan om de vraag wanneer het onderzoek daarnaar zou plaatsvinden en over de mogelijkheid van end-to-endencryptie in de huidige systemen.

Minister **De Jonge**:
Dat is jammer. Ik had zo'n heroïsch slotakkoord in gedachten en dan eindigt het er toch mee dat ik mevrouw Van Kooten-Arissen moet bekennen dat ik het antwoord op deze vraag nu eventjes niet paraat heb maar dat ik schriftelijk in een pracht van een brief hierop zal moeten terugkomen.

Hartelijk dank.

De **voorzitter**:
Dan zeg ik deze minister hartelijk dank voor zijn bijdrage aan dit debat.

De beraadslaging wordt gesloten.

De **voorzitter**:
Dinsdag stemmen we over de overgebleven vier moties.