

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

764

Vragen van het lid **Stoffer** (SGP) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *de verkoop van het cloudbedrijf van DigiD en MijnOverheid en de dreiging voor onze digitale autonomie* (ingezonden 19 november 2025).

Antwoord van Staatssecretaris **Van Marum** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 19 december 2025). Zie ook Aanhangsel Handelingen, vergaderjaar 2025–2026, nr. 632.

Vraag 1

Bent u bekend met het bericht in het Financieele Dagblad van 12 november jongstleden over de verkoop van het Nederlandse cloudbedrijf Solvinity aan Kyndryl, een Amerikaanse partij, en de daaruit voortvloeiende onrust bij overheden die afhankelijk zijn van de diensten van Solvinity, zoals DigiD, MijnOverheid en Digipoort?¹

Antwoord 1

Ja, ik ben bekend met dit bericht.

Vraag 2

Deelt u de zorg dat door deze overname essentiële overheidsdiensten, waaronder DigiD en MijnOverheid, feitelijk in buitenlandse handen komen, met alle risico's van dien, bijvoorbeeld op het gebied van digitale soevereiniteit en (data)veiligheid?

Antwoord 2

Ik heb begrip voor de zorgen van de Tweede Kamer over de voorgenomen overname van het bedrijf Solvinity door een Amerikaans bedrijf. Solvinity is betrokken bij belangrijke diensten van de overheid zoals bijvoorbeeld DigiD. Het is belangrijk dat de veiligheid van vertrouwelijke gegevens van en de dienstverlening aan burgers niet in het gedrang komen door deze overname. Daarom wordt momenteel, naast de onderzoeken van de wettelijke toezicht-houders, onder mijn regie onderzoek gedaan naar de operationele, juridische en contractuele gevolgen van de voorgenomen overname. Als het onderzoek

¹ Het Financieele Dagblad, 12 november 2025, «Onrust bij overheden over verkoop cloudbedrijf aan Amerikaanse IT-gigant», fd.nl/tech-en-innovatie/1577303/onrust-bij-overheden-over-verkoop-cloudbedrijf-aan-amerikaanse-it-gigant

naar de gevolgen van de beoogde overname een onacceptabel risico laat zien, worden passende maatregelen genomen. De veiligheid en bescherming van essentiële gegevens van Nederlandse burgers staan voorop.

Vraag 3

Welke juridische en bestuurlijke instrumenten staan u ter beschikking om dergelijke overnames van strategisch vitale ICT-dienstverleners te reguleren of te keren? Zijn er mogelijkheden om een overname te verbieden of voorwaarden te stellen?

Antwoord 3

Het waarborgen van onze digitale autonomie is een belangrijke ambitie van het kabinet, zoals ook is beschreven in de Agenda Digitale Open Strategische Autonomie². Voor onze digitale autonomie is het van belang dat we een sterkere Nederlandse (en Europese) techsector opbouwen. Voor een klein handelsland als Nederland zijn een open economie en toegang tot internationale kapitaalmarkten hiervoor essentieel. Dat zorgt ervoor dat Nederlandse bedrijven internationaal innovatief en concurrerend kunnen zijn. Tegelijkertijd betekent dit dat bedrijven overgenomen kunnen worden door buitenlandse partijen. Waar investeringen in Nederlandse marktpartijen impact hebben op onze nationale veiligheid, hebben we instrumenten tot onze beschikking om die impact te toetsen en – indien noodzakelijk – ons hiertegen te beschermen, zoals de Wet veiligheidstoets investeringen, fusies en overnames (Wet Vifo) en de Wet ongewenste zeggenschap telecommunicatie (WOZT).

Vraag 4

Bent u vooraf betrokken geweest bij de overnamebesprekingen, en is er door de departementen gemonitord wat de gevolgen zijn van de overname specifiek voor overheidsklanten zoals DigiD, het Centraal Justitieel Incassobureau (CJIB) en andere kritieke publieke diensten?

Antwoord 4

Nee, ik ben niet betrokken geweest bij overnamebesprekingen. Voor de zomer van 2025 heeft Solvinity bij Logius aangegeven dat een overname op handen was zonder details van de overnamekandidaat te delen. Onder regie van BZK wordt op dit moment het totale risicobeeld bij overheidsorganisaties geïnventariseerd.

Vraag 5

Hoe beoordeelt u de kans dat door deze overname buitenlandse entiteiten inzage of controle zouden kunnen krijgen in kritische overheidsdata, bijvoorbeeld op grond van buitenlandse wetgeving zoals de Cloud Act of andere wet- en regelgeving?

Antwoord 5

Ten tijde van het afsluiten van de contracten zijn met Solvinity afspraken gemaakt over de vertrouwelijkheid en veiligheid van de bij deze onderneming ondergebrachte gegevens. Een overname van Solvinity door een partij in de VS betekent dat die afspraken nader moeten worden ingevuld, om te voorkomen dat de vertrouwelijkheid en veiligheid van die gegevens in het geding kan komen.

De wettelijke Amerikaanse instrumenten maken het, in ieder geval in theorie, mogelijk dat autoriteiten in de VS onder de in deze wetgeving genoemde voorwaarden toegang kunnen krijgen tot de gegevens waarover een onderneming in de VS beschikt, óók wanneer de gegevens zich bevinden onder een dochtervennootschap en op servers buiten de VS. Als Solvinity wordt overgenomen door een onderneming in de VS brengt dit Solvinity onder de reikwijdte van deze wetgeving. Het gevolg daarvan kan, in ieder geval in theorie, zijn dat autoriteiten in de VS in voorkomend geval toegang krijgen tot de gegevens die door Solvinity in opdracht van de Staat worden verwerkt.

De overeenkomsten tussen de Staat en Solvinity bieden aanknopingspunten om ten minste van Solvinity te verlangen dat er technische en organisatori-

² <https://www.rijksoverheid.nl/documenten/rapporten/2023/10/17/bijlage-agenda-dosa-tgpdfa>

sche maatregelen worden getroffen om te waarborgen dat de gegevens waartoe zij toegang heeft op een wijze worden verwerkt die voldoet aan de in de EU geldende regels, zoals die uit de Algemene verordening gegevensbescherming. Welke maatregelen dat zullen zijn vormt onderwerp van de gesprekken tussen de Staat en Solvinity.

Vraag 6

Wat is op dit moment de eigendomsstructuur van de IT-diensten achter DigiD, MijnOverheid en Digipoort? Welke onderdelen zijn in handen van Solvinity, en wat betekent de overname praktisch voor de eigendom en exploitatie van deze cruciale infrastructuur?

Antwoord 6

Voorzieningen zoals DigiD, MijnOverheid en Digipoort zijn specifieke applicaties ontwikkeld door en voor Logius. De applicaties DigiD en MijnOverheid draaien op het door Solvinity beheerde ICT-infrastructuurplatform «PICARD». Op dit platform kunnen de gebruikersrechten en het beheer per laag (infrastructuur, applicatie, netwerk) verschillen en/of door verschillende partijen worden uitgevoerd.

Het uitgangspunt is dat de Staat der Nederlanden eigenaarsrechten van de software en data van voorzieningen als DigiD, MijnOverheid en Digipoort bezit. Leveranciers hebben, afhankelijk van de dienstverlening, gebruikersrechten om toegang te krijgen om hun beheertaken te kunnen uitvoeren. Er zijn twee vormen van beheer te onderscheiden: technisch beheer en applicatiebeheer. Het technische beheer (o.a. infrastructuur, servers) van het «PICARD» ICT-platform is uitbesteed aan Solvinity.

Het applicatiebeheer dat zich richt op de werking van de applicatie zelf wordt uitgevoerd door eigen Logius medewerkers, eventueel aangevuld met inhuur of uitbesteed. Dit verschilt per voorziening. Beide vormen van beheer zijn uitvoerende taken en staan los van eigendomsrechten t.a.v. software en data.

Vraag 7

Hoe waarborgt u dat andere belangrijke overheidsdiensten, die nu in Nederlandse handen zijn, niet op termijn eveneens kunnen worden overgenomen door buitenlandse partijen? Welke preventieve strategie wordt hierbij door het kabinet gehanteerd?

Antwoord 7

Het in Nederlandse handen houden van alle bedrijven is op zichzelf geen doel van het kabinet. Nederland hanteert een stelsel van investeringstoetsingen gericht op het mitigeren van risico's voor de nationale veiligheid. Mocht de beoogde overname onder het bereik van de investeringstoetsing vallen zal het reguliere, zorgvuldige proces daartoe gevolgd worden.

De nieuwe Rijksbrede Strategie IT-sourcing, onderdeel van de Nederlandse Digitaliseringsstrategie (NDS), geeft aandacht aan het verkrijgen van een sterkere regie op digitale autonomie, soevereiniteit en veiligheid. Voor situaties waarin leveranciers worden overgenomen door buitenlandse partijen wordt een handreiking ontwikkeld om de afnemers te helpen met het in kaart brengen van de mogelijke risico's die daarmee gepaard gaan en de mogelijkheden tot mitigatie.

Vraag 8

Erkent u de bredere zorgen over de afhankelijkheid van buitenlandse cloudbaanbieders die in het artikel naar voren worden gebracht? In hoeverre heeft het kabinet concrete stappen gezet om te investeren in digitale autonomie, bijvoorbeeld op het gebied van een nationale of «soevereine» overheidscloud?

Antwoord 8

Het kabinet erkent de zorgen over de afhankelijkheid van buitenlandse cloudbaanbieders. De Rijksoverheid streeft dan ook naar het tot stand komen van een «soevereine overheidscloud» voor kritieke overheidsdienstverlening. Binnen de Nederlandse Digitaliseringsstrategie (NDS) wordt verkend hoe een soevereine overheidscloud eruit kan zien; dit geldt als belangrijke prioriteit. Tevens recent de Visie Digitale Autonomie vastgesteld. Naast het onderstrepen van het belang van digitale autonomie, worden ook de strategische

bouwstenen benoemd die nodig zijn om te komen tot een digitale overheid die grip heeft op autonomie, zeggenschap heeft over haar data (soevereiniteit) en cyberveilig en weerbaar is. Deze casus onderstreept het belang van de NDS.

Vraag 9

Hoe verhoudt deze overname zich tot het bestaande Rijksbreed Cloudbeleid? Worden er in dat beleid mechanismen opgenomen om toekomstige overnames van (voormalig-) Nederlandse cloudleveranciers door buitenlandse partijen te beperken?

Antwoord 9

In het Rijksbreed cloudbeleid is een risicoanalyse verplicht. Hierin moeten ook de risico's van mogelijke buitenlandse inmenging op de dienstverlening op het gebied van vertrouwelijkheid en beschikbaarheid worden meegewogen. Waar nodig moeten die risico's worden gemitigeerd, dan wel moet een andere leverancier worden gezocht. Deze risico's gelden niet voor elke overheidsdienst waardoor een risico-gebaseerde aanpak het gehanteerde mechanisme is.

Vraag 10

Bent u bereid de Kamer halfjaarlijks te informeren over de risico-inschatting, de maatregelen die worden genomen én de mogelijke vervolgacties in het kader van digitale autonomie over Nederlandse overheidswebsites?

Antwoord 10

Het Forum Standaardisatie voert periodiek onderzoeken³ uit naar de toepassing van open standaarden, de naleving van de «pas toe of leg uit»-lijst en de informatiebeveiliging bij overheidsorganisaties, waarmee zij inzicht geeft in de interoperabiliteit en digitale weerbaarheid van de Nederlandse overheid om daarmee vendor lock-in te voorkomen en kwetsbaarheden in kaart te brengen.

Daarnaast wordt in de eerste helft van 2026, vanuit het NDS Programma, een verkenning uitgevoerd naar realisatie van een overheidsbrede soevereine cloudvoorziening. Deze cloudvoorziening is een belangrijke prioriteit van het NDS programma. Ik zal de uitkomsten van deze verkenning met uw Kamer delen.

³ <https://www.forumstandaardisatie.nl/metingen>