AH 292

2026Z16981

Antwoord van minister Sterk (Langdurige Zorg, Jeugd en Sport), mede namens de staatssecretaris van Economische Zaken en Klimaat (ontvangen 5 oktober 2026)

Zie ook Aanhangsel Handelingen, vergaderjaar 2025-2026, nr. 2955

Vraag 1

Bent u ermee bekend dat de Amerikaanse CLOUD (Clarifying Lawful Overseas Use of Data) Act (2018) Amerikaanse aanbieders verplicht gegevens te verstrekken die zij in bezit, beheer of onder zeggenschap hebben, ongeacht of die gegevens fysiek in Nederland zijn opgeslagen?

Antwoord 1

Zoals eerder aan uw Kamer medegedeeld in Kamervragen van het lid Jansen op 26 november 2025 maakt (onder meer) de CLOUD Act (Clarifying Lawful Overseas Use of Data Act), het 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[1].

Vraag 2

Deelt u de constatering dat de CLOUD Act de zeggenschap van de aanbieder volgt en niet de opslaglocatie, en dat opslag in een Nederlands datacenter van een Amerikaans bedrijf die gegevens dus niet onder Nederlandse jurisdictie brengt? Zo nee, waarop baseert u het tegendeel?

Antwoord 2

In het geval dat een leverancier mede onder Amerikaanse jurisdictie valt, kan ook specifieke Amerikaanse wetgeving, zoals de CLOUD Act, van toepassing zijn. De CLOUD Act stelt dat data die in ‘possession, custody or control’ van een Amerikaanse leverancier, of één van haar dochtermaatschappijen, is onder die wetgeving valt, ongeacht het land waar deze data is opgeslagen[2].

Vraag 3

---

[1] https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2026D26573&did=2026D26573
[2] https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2026D26573&did=2026D26573

Bestaat er op dit moment een internationale overeenkomst tussen de Europese Unie en de Verenigde Staten op grond waarvan een Amerikaans bevel tot verstrekking van persoonsgegevens erkend of afdwingbaar is in de zin van artikel 48 van de Algemene verordening gegevensbescherming? Zo nee, welke van beide rechtsordes overtreedt een Amerikaanse aanbieder die zo'n bevel ontvangt ten aanzien van Nederlandse patiëntgegevens?

Antwoord 3

Indien een in Nederland gevestigde dochteronderneming van een Amerikaans bedrijf voldoet aan een Amerikaans bevel tot gegevensverstrekking, kan dit in strijd zijn met de AVG. Daarnaast kan het zo zijn dat de dochteronderneming zich in dat geval mogelijk niet houdt aan de verwerkersovereenkomst met de

Nederlandse opdrachtgever, wat een grond kan vormen voor ontbinding van de overeenkomst. Weigert de aanbieder aan het bevel te voldoen, dan kan dit in strijd zijn met de Amerikaanse wetgeving.

Vraag 4

Klopt het dat een verzoek onder de CLOUD Act vergezeld kan gaan van een geheimhoudingsbevel (FISA Section 702), waardoor de betrokken zorginstelling niet mag worden geïnformeerd? Zo ja, hoe kan een zorgaanbieder onder die omstandigheid voldoen aan de verantwoordingsplicht uit de AVG, aan NEN 7510 en aan het medisch beroepsgeheim?

Antwoord 4

Ja, dat klopt. Een verzoek om gegevensverstrekking op grond van de CLOUD Act kan samengaan met een geheimhoudingsbevel. De CLOUD Act en FISA Section 702 zijn daarbij twee verschillende wettelijke kaders. De CLOUD Act voorziet in rechterlijke toetsing en biedt organisaties onder omstandigheden de mogelijkheid een verzoek aan te vechten. FISA Section 702 maakt het mogelijk voor Amerikaanse inlichtingendiensten om zonder gerechtelijk bevel informatie te verzamelen over niet-Amerikaanse staatsburgers waarvan wordt aangenomen dat zij zich buiten de Verenigde Staten bevinden en die mogelijk betrokken zijn bij terrorisme, spionage, massavernietigingswapens, beïnvloedingsactiviteiten in opdracht van een vijandige buitenlandse mogendheid of cybercriminaliteit. Kennisgeving aan de betrokkene is bijvoorbeeld geen vereiste[3].

Bij FISA Section 702 kan een geheimhoudingsplicht gelden. De betrokken dienstverlener mag zijn klant dan niet informeren over de gegevensverstrekking. Een Nederlandse zorgaanbieder kan daardoor niet op de hoogte zijn van een dergelijke verstrekking.

[3] https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2026D26573&did=2026D26573

Het tweede deel van de vraag kan ik kort beantwoorden met de constatering dat een zorgaanbieder aan de verplichtingen kan voldoen, voor zover hij passende maatregelen heeft getroffen. Toch zal ik de drie genoemde verplichtingen lansglopen.

Voor zover het de AVG-verantwoordingsplicht betreft, is het voor de zorgaanbieder van groot belang dat doorgiften van persoonsgegevens aan derde landen in overeenstemming met de AVG plaatsvinden. Als daarvan geen sprake is, bijvoorbeeld vanwege de mogelijkheid dat Amerikaanse autoriteiten door middel van een geheimhoudingsbevel toegang tot gegevens kunnen verkrijgen, is de zorgaanbieder bij doorgifte verplicht passende aanvullende waarborgen te treffen om een gelijkwaardig beschermingsniveau te waarborgen. Wanneer hij dat niet doet, of niet kan doen, dan kan de doorgifte niet in overeenstemming met de AVG plaatsvinden.

Genoemde maatregelen spelen ook een rol bij de naleving van de NEN 7510. Dit is namelijk een op een risico-afweging gebaseerde norm: de zorgaanbieder moet de risico’s op het gebied van vertrouwelijkheid, integriteit en beschikbaarheid identificeren en aan de hand daarvan passende maatregelen treffen. Het gaat er

dus om dat hij die risico’s die samenhangen met het geheimhoudingsbevel heeft geïdentificeerd en vervolgens passende maatregelen heeft getroffen en dat kan aantonen.

De passende maatregelen komen ook terug bij het medisch beroepsgeheim. Ook een geheime opvraging waarvan de zorgaanbieder geen weet heeft, doorbreekt het medisch beroepsgeheim. Om dit te voorkomen zijn de passende maatregelen vereist.

De kern van mijn antwoord is dus dat de zorgaanbieder vooraf het risico van dergelijke buitenlandse toegang moet onderkennen en passende maatregelen dient te treffen. Juist de keuze voor een cloud-leverancier is daarbij van belang.

Vraag 5

Kunt u aangeven hoeveel verzoeken van Amerikaanse autoriteiten aan aanbieders bekend zijn die Nederlandse zorgdata betroffen? Indien u dit niet kunt aangeven, erkent u dan dat het uitblijven van bekende gevallen geen enkele indicatie is dat zulke verzoeken niet plaatsvinden?

Antwoord 5

Hierover zijn geen cijfers bekend. Bovendien is het inderdaad zo, dat het niet bekend zijn van deze cijfers, niet betekent dat dergelijke verzoeken niet plaatsvinden. Ten eerste zijn bedrijven niet verplicht melding te maken van deze verzoeken. In de tweede plaats kunnen dergelijke verzoeken van de Amerikaanse overheid ook vergezeld gaan van een zogenaamde ‘gag order’, waarbij het deze bedrijven uitdrukkelijk verboden wordt melding te maken van het feit dat een dergelijk verzoek is gedaan.

Vraag 6

Kunt u bevestigen dat volgens de marktinventarisatie van M&I/Partners van begin 2026 76% van de Nederlandse ziekenhuizen ChipSoft gebruikt, 16% het Amerikaanse Epic en 8% het Duitse NEXUS (circa 95% in handen van de Amerikaanse investeerder TA Associates)?[1]

Antwoord 6

Het betreft een eigenstandige marktinventarisatie van M&I partners. Deze percentages komen overeen met ons beeld.

Vraag 7

Deelt u de constatering dat het EPD slechts één laag is en dat ook software van Nederlandse leveranciers volledig op Amerikaanse cloudinfrastructuur kan draaien, zoals bij de ingebruikname van HiX in de Azure-cloud door Zuyderland MC? Bent u bereid in kaart te brengen bij hoeveel zorginstellingen het EPD of ECD draait op infrastructuur van een niet-Europese aanbieder, en de Kamer hierover te informeren?

Antwoord 7

Ja, de constatering wordt gedeeld dat het elektronisch patiëntendossier (EPD) slechts één laag is en dat ook software van Nederlandse leveranciers op Amerikaanse cloud-infrastructuur kan draaien. Mijn ministerie beschikt niet over een overzicht van welke zorginstelling op welke infrastructuur draait. De zorg is privaat georganiseerd en dient volgens NEN 7510 zelf alle risico’s in beeld te brengen en waar nodig passende maatregelen te treffen.

Vraag 8

Beschikt u over een overzicht van het aantal zorginstellingen dat Microsoft 365 of Google Workspace gebruikt voor communicatie waarin patiëntgegevens voorkomen? Zo nee, bent u bereid dit alsnog te laten inventariseren?

Antwoord 8

Nee, mijn ministerie beschikt niet over een dergelijk overzicht. De zorg is privaat georganiseerd en dient volgens NEN 7510 zelf alle risico’s in beeld te brengen en waar nodig passende maatregelen te treffen.

Vraag 9

Is bij de keuze van UMCG, Treant en Ommelander Ziekenhuis Groningen voor een gezamenlijk EPD op basis van Epic, met ingebruikname in 2027 [2], expliciet getoetst op de gevolgen voor jurisdictie en toegang door buitenlandse autoriteiten? Zo ja, kan de Kamer die toets ontvangen? Zo nee, waarom is die toets achterwege gebleven?

Antwoord 9

Een gezamenlijk EPD kan voordelen hebben voor de samenwerking tussen zorgaanbieders. Zorginstellingen, zoals UMCG, Treant en Ommelander Ziekenhuis Groningen, kunnen zelf de keuze maken om dergelijke systemen te implementeren. Specifieke toetsing behorend bij een dergelijke keuze valt onder de verantwoordelijkheid van de betrokken zorgaanbieders zelf. Het ministerie van VWS is geen partij bij deze keuze en heeft derhalve ook geen informatie over of inzage in de toetsingen die hierop zijn uitgevoerd.

Vraag 10

Geldt de door de Kamer aanvaarde doelstelling dat de continuïteit van digitale dienstverlening niet rechtstreeks afhankelijk is van partijen uit de Verenigde Staten (Kamerstuk 26 643, nr. 1320) ook voor de zorgsector? Zo nee, waarom geldt voor de meest gevoelige persoonsgegevens die de samenleving kent een lichter regime dan voor de rijksoverheid zelf?

Antwoord 10

De motie waarin deze doelstelling is opgenomen ziet, zoals u zelf ook al aangeeft, specifiek op de rijksoverheid. Die doelstelling geldt daarmee niet automatisch voor andere domeinen. Zorgdata vallen onder de reikwijdte van de AVG, wat een voldoende zwaar regime is voor de bescherming van deze persoonsgegevens.

Vraag 11

Welk normatief kader verplicht een ziekenhuis, GGZ-instelling of VVT-organisatie op dit moment tot een jurisdictietoets voordat zorgdata bij een niet-Europese

aanbieder wordt ondergebracht? Indien zo'n verplichting ontbreekt, acht u dat aanvaardbaar?

Antwoord 11

Wanneer (zorg)data wordt ondergebracht bij een buitenlandse aanbieder (buiten AVG gebied), dan moet verplicht een toets worden gedaan of de geldende wet- en regelgeving binnen dat land een voldoende beveiligingsniveau biedt. Hieruit volgt dat een jurisdictie toets gedaan moet worden. Immers, moet een opdrachtgever eerst weten welke jurisdictie van toepassing is voordat deze kan worden getoetst.

Vraag 12

Bent u bereid een "nee, tenzij"-regime in te stellen voor nieuwe migraties van zorgdata naar niet-Europese aanbieders, waarbij migratie alleen is toegestaan na een expliciete, gedocumenteerde toets op jurisdictie en continuïteit? Zo nee, met welk instrument voorkomt u dan dat de afhankelijkheid verder toeneemt terwijl de Kamer het tegenovergestelde heeft uitgesproken?

Antwoord 12

Nee. Op dit moment zet het kabinet niet in op een “nee, tenzij”-regime. De AVG bevat voldoende verplichte elementen om de veiligheid van gegevens te borgen. Wanneer zorgdata wordt ondergebracht bij een buitenlandse aanbieder, buiten het gebied van de AVG, dan moet verplicht een toets worden gedaan of de geldende wet- en regelgeving binnen dat land een voldoende beveiligingsniveau biedt. Onderdeel hiervan is een jurisdictietoets.

Vraag 13

Welke ruimte biedt het aanbestedingsrecht om jurisdictie en Europees sleutelbeheer als zwaarwegend gunningscriterium te hanteren bij aanbestedingen van zorg-ICT? Bent u bereid die ruimte actief te laten benutten en zorgaanbieders daarover te instrueren?

Antwoord 13

In het reguliere aanbestedingsrecht is het niet toegestaan om Europese bedrijven gunstiger te behandelen dan bedrijven uit landen waarmee de Europese Unie een handelsovereenkomst heeft of landen die onderdeel zijn van de Government Procurement Agreement (GPA) van de WTO. Dit betekent dat geen eisen gesteld mogen worden in een aanbesteding die direct of indirect discriminatoir zijn voor bedrijven uit deze landen buiten de EU. De Aanbestedingswet op Defensie- en Veiligheidsgebied (ADV) biedt meer mogelijkheden om risico’s voor de nationale veiligheid te mitigeren. Zo kan een aanbestedende dienst wel ondernemers

uitsluiten die niet in EU-lidstaten gevestigd zijn of er kunnen eisen gesteld worden aan gegevensbeveiliging.

In Nederland zijn van de zorgaanbieders enkel academische ziekenhuizen aanbestedingsplichtig, alle overige zorgaanbieders zijn dus niet gebonden aan bovenstaande aanbestedingsregelgeving. Via PIANOo, het expertisecentrum aanbesteden, worden aanbestedende diensten (waaronder academische ziekenhuizen) actief geïnformeerd over de mogelijkheden om veiligheidsaspecten in te brengen in hun aanbestedingen. Daarnaast vindt op dit moment in Europa een herziening van de aanbestedingsregelgeving plaats, het voorstel van de Europese Commissie hiervoor is gepresenteerd op 9 september. Zoals al eerder aan uw Kamer meegegeven, zet het kabinet zich bij deze herziening in voor meer ruimte voor aanbestedende diensten om bij aanbestedingen beter rekening te houden met strategische belangen zoals economische weerbaarheid en veiligheid. Dit zal academische ziekenhuizen mogelijk in de toekomst de ruimte geven meer te sturen op Europees sleutelbeheer of jurisdictie bij zorg-ICT.

Vraag 14

Erkent u dat het risico zich niet beperkt tot inzage maar ook uitschakeling omvat, gelet op het feit dat Microsoft na Amerikaanse sancties de toegang tot het e-mailaccount van de hoofdaanklager van het Internationaal Strafhof heeft afgesloten? [3] Welke exitstrategie of terugvaloptie hebben Nederlandse ziekenhuizen indien een Amerikaanse leverancier de dienstverlening opschort?

Antwoord 14

Het kabinet erkent dat het risico zich niet beperkt tot inzage, maar zich ook kan uitstrekken tot het beëindigen of opschorten van toegang tot dienstverlening. Afhankelijkheid van leveranciers, binnen en buiten Europa, kan risico’s met zich meebrengen zoals bijvoorbeeld uitval van systemen. Daarom heeft de toenmalige minister van Volksgezondheid, Welzijn en Sport de zorgsector in een Kamerbrief van december 2025[4] opgeroepen afhankelijkheid van leveranciers mee te nemen in hun risicoafweging. De continuïteit van zorg moet altijd zeker zijn gesteld.

[4] Kamerstukken II, 2025/26, 27529 nr. 353.

Zorgverlening is vaak dienstverlening die niet een paar weken kan wachten. Het is dan ook belangrijk om als zorgaanbieder na te denken over een exitstrategie. Dit is onderdeel van de wettelijk verplichting van de norm voor informatieveiligheid in de zorg, de NEN 7510. Nederlandse zorgaanbieders zijn zelf verantwoordelijk voor het treffen van beveiligingsmaatregelen en het naleven van de NEN 7510.

Het kabinet ziet daarmee geen rol voor de Rijksoverheid bij het opstellen van individuele exitplannen van zorgaanbieders, maar volgt via het toezicht van de IGJ of zorgaanbieders aantoonbaar aan NEN 7510 voldoen.

Vraag 15

Het kabinet heeft de overname van Solvinity door een Amerikaanse partij geblokkeerd vanwege risico's voor de nationale veiligheid en de continuïteit van DigiD, bent u bereid dezelfde afweging structureel toe te passen op overnames van leveranciers van zorg-ICT, en zo nodig het toepassingsbereik van de investeringstoets daarop uit te breiden?

Antwoord 15

Het is belangrijk te benadrukken dat digitale autonomie en soevereiniteit de volle aandacht heeft van het kabinet. Het kabinet blijft zich daarnaast onverminderd inzetten om risicovolle strategische afhankelijkheden goed in kaart te brengen en de mogelijke handelingsopties uit te werken.

Voor leveranciers van zorg-ICT en de bescherming van medische gegevens en veiligheidsbelangen bestaat reeds een robuust stelsel van wet- en regelgeving.

Onder andere is er de Algemene Verordening Gegevensbescherming (AVG) voor de zorgen omtrent jurisdictie over Nederlandse zorgdata (zoals de Amerikaanse CLOUD Act) en de mogelijke internationale doorgifte van deze gegevens. De AVG stelt zeer strikte voorwaarden aan de verwerking en doorgifte van persoonsgegevens, waaronder patiëntendata. Het is in de eerste plaats aan zorgaanbieders en hun toeleveranciers om binnen dit kader te borgen dat buitenlandse wetgeving niet leidt tot onrechtmatige toegang tot patiëntendata.

Daarnaast is de afgelopen periode ingezet op het verhogen van de digitale en fysieke weerbaarheid van dienstverleners. Leveranciers van (zorg-)ICT vallen onder de verscherpte eisen voor risicobeheersing en meldplichten van de Cyberbeveiligingswet (Cbw), de implementatie van de NIS2-richtlijn. Tevens zullen zij in bepaalde gevallen onder de reikwijdte vallen van de nieuwe Wet weerbaarheid kritieke entiteiten (Wwke). Met deze instrumenten wordt de

continuïteit van deze diensten structureel en aan de voorkant geborgd, ongeacht de eigendomsverhoudingen van de leverancier.

De Wet vifo fungeert als een instrument om risico's voor de nationale veiligheid bij investeringen, fusies en overnames te mitigeren, voor zover deze niet al worden afgedekt door sectorspecifieke wetgeving. Ten behoeve van het Nederlandse investeringsklimaat en ter beperking van de lastendruk voor bedrijven is het toepassingsbereik van de Wet vifo zo specifiek mogelijk bepaald op basis van risico’s voor onze nationale veiligheid en wordt zorg-ICT vooralsnog niet toegevoegd aan de reikwijdte van de wet. Ik ben hier wel over in gesprek met het ministerie van EZK.

Het is belangrijk om onderscheid te maken tussen de WOZT-casus Solvinity en de bredere markt van leveranciers van zorg-ICT. Die casus raakt direct aan vraagstukken rond digitale (open) strategische autonomie, strategische afhankelijkheden en economische veiligheid.

Kabinetsbeleid in investeringstoetsingscasuïstiek vindt risico gebaseerd plaats. Het is een combinatie van het risicoprofiel van een verwerver, kenmerken van de transactie en activiteiten van een doelonderneming. De risico’s voor de nationale veiligheid die mogelijk bestaan in een specifieke transactie worden proportioneel gewogen aan de hand van de specifieke kenmerken in die zaak.

[1] MXI, 15 januari 2026, 'EPD-landschap 2026: tussen standaardisatie en innovatie', https://mxi.nl/kennis/746/epd-landschap-2026-tussen-standaardisatie-en-innovatie.

[2] Skipr, 21 november 2025, 'UMCG, Treant en Ommelander willen in 2027 gezamenlijk epd', https://www.skipr.nl/nieuws/umcg-treant-en-ommelander-willen-in-2027-gezamenlijk-epd/.

[3] NOS/AP, 20 mei 2025; Binnenlands Bestuur, 'Wake-up call: Microsoft sluit e-mail ICC zonder pardon af'.

[4] Kamerstukken II, 2025/26, 27529 nr. 353.