Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

De Voorzitter van de Tweede Kamer der Staten-Generaal
Prinses Irenestraat 6
2593 BN Den Haag

Turfmarkt 147
2511 DP Den Haag
Postbus 20011
2500 EA Den Haag

Onze referentie
2026-0000248158

Uw referentie
2026Z08716

Datum 02 juni 2026
Betreft Beantwoording Kamervragen van het lid Van den Berg (JA21) over de feitelijke veiligheidsrisico's, juridische reikwijdte en afhankelijkheden rond DigiD, Solvinity en Kyndryl.

Hierbij zend ik u, mede namens de staatssecretaris van Economische Zaken, de antwoorden op de vragen van het lid Van den Berg (JA21) over de feitelijke veiligheidsrisico's, juridische reikwijdte en afhankelijkheden rond DigiD, Solvinity en Kyndryl (vraagnummer2026Z08716).

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

Eric van der Burg

1. Bent u bekend met de voorgenomen overname van Solvinity Group B.V. door Kyndryl Netherlands B.V., de rol van Solvinity als leverancier van het platform waarop DigiD draait, en de eerdere beantwoording van Kamervragen over deze casus?

Ja, daar ben ik mee bekend.

2. Kunnen de Verenigde Staten volgens u gezien worden als een bondgenoot? Zo nee, waarom niet?

Ja, de Verenigde Staten zijn een belangrijke bondgenoot van Nederland, zoals ik ook tijdens het vragenuur op dinsdag 26 mei heb benadrukt: “de Verenigde Staten zijn een belangrijke NAVO-partner, handelspartner en bondgenoot”.

3. Acht u het waarschijnlijk dat een NAVO-bondgenoot als de Verenigde Staten doelbewust DigiD of vergelijkbare Nederlandse kritieke digitale overheidsinfrastructuur zou uitschakelen? Graag een onderbouwing op basis van dreiging, intentie, capaciteit, precedent en diplomatieke consequenties.

Het kabinet hecht grote waarde aan de aanwezigheid van buitenlandse, waaronder nadrukkelijk ook Amerikaanse, technologiebedrijven. Het kabinet waardeert hun bijdrage aan de Nederlandse economie en digitale infrastructuur.

Een afhankelijkheid van informatie en diensten uit derde landen, ongeacht welk land het is en of het een NAVO-bondgenoot is, kan onzekerheden met zich meebrengen. Dit blijkt ook uit het Cybersecuritybeeld Nederland Nederland 2025[1]. Het is vervolgens aan de overheid om op een objectieve, risicogebaseerde, landenneutrale en proportionele manier risico’s te wegen. De gevraagde onderbouwing kan niet als generiek standpunt aangeleverd worden. Daarvoor is dit te situationeel afhankelijk en kan het alleen op case-by-case basis worden ingeschat.

Ieder departement is zelf verantwoordelijk voor de inrichting van haar digitale overheidsinfrastructuur en het afwegen van de risico’s van de verschillende schakels binnen die infrastructuur.

4. Acht u een dergelijk scenario realistisch, of gaat het primair om een theoretische mogelijkheid die in de risicoanalyse wel moet worden meegenomen, maar niet gelijkgesteld mag worden aan een waarschijnlijke dreiging? Graag een expliciet onderscheid tussen “mogelijk”, “aannemelijk”, “waarschijnlijk” en “urgent”.

Zie antwoord op vraag 3.

5. Kunt u per juridisch instrument, CLOUD Act, FISA Section 702, Executive Order 12333 en eventuele andere relevante Amerikaanse bevoegdheden, uiteenzetten wat de wettelijke grondslag is, welke autoriteit bevoegd is, welk type gegevens kan worden gevorderd of verzameld, welke rechterlijke toetsing plaatsvindt, of kennisgeving aan de betrokkene, Logius of de Nederlandse Staat verplicht,

[1] https://www.nctv.nl/documenten/2025/11/26/cybersecuritybeeld-nederland-2025

verboden of beperkt kan zijn en hoe dit zich verhoudt tot de Algemene verordening gegevensbescherming (AVG), verwerkersovereenkomsten en contractuele geheimhoudingsplichten?

CLOUD Act
De CLOUD Act is een amendement op de Stored Communications Act (SCA). De CLOUD Act maakt het mogelijk voor Amerikaanse autoriteiten om ten behoeve van wetshandhavingsdoeleinden toegang te verkrijgen tot elektronische communicatie en daaraan gerelateerde gegevens. Bevoegde autoriteiten die een verzoek kunnen indienen zijn bijvoorbeeld de FBI en het Department of Justice. De CLOUD Act kan worden ingezet voor het opvragen van elektronische gegevens in het kader van strafrechtelijk onderzoek en vervolging. Het gaat daarbij in beginsel om de opsporing en vervolging van zware criminaliteit, zoals terrorisme of drugshandel.

Op grond van de CLOUD Act kunnen ondernemingen die onder de Amerikaanse rechtsmacht vallen verplicht worden gegevens te verstrekken, ook wanneer deze gegevens zich (op servers) buiten de Verenigde Staten bevinden. Daarbij is bepalend of de onderneming *"possession, custody or control"* heeft over de gegevens. Het gaat hierbij onder meer om aanbieders van elektronische communicatie- en clouddiensten.

Voor verzoeken die betrekking hebben op de inhoud van elektronische communicatie of bestanden is in beginsel toestemming van een Amerikaanse rechter vereist. Voor bepaalde verzoeken tot verstrekking van metadata, zoals gegevens over gebruikers of toegangsgegevens, kan onder omstandigheden geen voorafgaande rechterlijke toestemming vereist zijn.

Een dienstverlener die een bevel tot gegevensverstrekking ontvangt, hoeft daaraan niet mee te werken indien de gegevens versleuteld zijn en de dienstverlener niet beschikt over de encryptiesleutel. De CLOUD Act verplicht ondernemingen namelijk niet om gegevens te ontsleutelen. Indien een onderneming feitelijk geen toegang heeft tot de gegevens vanwege encryptie, bestaat in beginsel dus ook geen verplichting om deze gegevens te verstrekken.
Daarnaast kan een dienstverlener de rechter verzoeken het bevel te vernietigen of te wijzigen, bijvoorbeeld wanneer de naleving daarvan strijd oplevert met de wetgeving van het land waar de gegevens zich bevinden of indien de persoon op wie het verzoek betrekking heeft geen Amerikaans staatsburger is.

FISA Section 702
FISA Section 702 is in 2008 ingevoerd en maakt onderdeel uit van de Foreign Intelligence Surveillance Act 1978. FISA Section 702 maakt het Amerikaanse inlichtingendiensten, zoals de NSA, CIA en FBI, mogelijk 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 geen vereiste.
Onder het toepassingsbereik van deze wetgeving vallen alle Amerikaanse entiteiten die toegang hebben tot apparaten waarop communicatie wordt opgeslagen of via welke

communicatie wordt verzonden, zoals telecommunicatiebedrijven, internet- en e-maildienstverleners, aanbieders van remote computing services. Zij kunnen worden verplicht toegang te geven tot gegevens, zoals e-mails, elektronische berichten en bestanden. Het kan zowel om de inhoud als metadata gaan.

Executive Order 12333
Executive Order 12333 heeft het meest verstrekkende bereik. Deze regelgeving maakt het mogelijk dat Amerikaanse inlichtingendiensten buitenlandse inlichtingen verzamelen. Daarvoor is geen toestemming van een rechter vereist, mits het gaat om gegevens van niet-Amerikaanse personen. De regelgeving is primair gericht op buitenlandse inlichtingenvergaring ten behoeve van de nationale veiligheid van de Verenigde Staten.

Op grond van Executive Order 12333 kunnen Amerikaanse inlichtingendiensten buitenlandse inlichtingen verzamelen via uiteenlopende middelen, waaronder interceptie van communicatie, radiosignalen en andere elektromagnetische communicatie, maar ook via satellieten, camerasystemen, menselijke bronnen en samenwerking met buitenlandse inlichtingendiensten. Vereist is echter wel dat de verzamelde informatie uitsluitend voor rechtmatige doeleinden onder Amerikaanse wetgeving wordt gebruikt.

Kyndryl Inc. valt als Amerikaanse onderneming binnen het bereik van de bovengenoemde wetten. Kyndryl rapporteert periodiek hoeveel verzoeken om inlichtingen zij heeft ontvangen.[2]

Kyndryl's US zeggenschap over haar buitenlandse dochters, Kyndryl Nederland B.V. en eventueel overgenomen partijen, heeft tot gevolg dat deze ook binnen het bereik vallen van de bovengenoemde wetten.

De verstrekking van persoonsgegevens door Nederlandse dochter(s) op basis van een bevel van een Amerikaanse rechter kan in strijd zijn met de AVG. Daarnaast houdt de Nederlandse dochter zich in dat geval ook niet aan de overeenkomst, inclusief de verwerkingsovereenkomst, met de Nederlandse opdrachtgever.
Kyndryl US heeft wel juridische mogelijkheden om zich te verzetten tegen verzoeken tot verstrekking van persoonsgegevens die worden beheerd door haar Nederlandse dochter(s) op grond van het feit dat voldoen aan een dergelijk verzoek in strijd is met de AVG en de gemaakte contractuele afspraken (o.a. in de verwerkersovereenkomst). Daarover moet de Amerikaanse rechter zich dan uitlaten.

6. Kunt u expliciet onderscheid maken tussen toegang tot gegevens enerzijds en operationele zeggenschap over systemen anderzijds? Klopt het dat wetgeving zoals de CLOUD Act primair ziet op toegang tot elektronische gegevens en niet zonder meer op het met "één druk op de knop" uitschakelen van infrastructuur?

Ja, dat klopt. De Amerikaanse wetgeving als bedoeld bij vraag 5 heeft betrekking op het verzamelen van bewijs c.q. inlichtingen. Deze wetgeving maakt het niet mogelijk om een opdracht te geven tot uitschakeling van infrastructuur.

[2] https://www.kyndryl.com/us/en/privacy/governmental-data-requests

De Amerikaanse overheid kan sancties tegen personen, organisaties of landen uitvaardigen, waarna Amerikaanse bedrijven de dienstverlening moeten staken. Dat gebeurt echter niet op grond van de bovengenoemde wetgeving.

7. Hoe verhoudt de stelling dat Solvinity in beginsel geen toegang heeft tot burgerservicenummers, adres en telefoonnummer van DigiD-gebruikers zich tot de eerdere kabinetsuitspraak dat Amerikaanse autoriteiten 'in theorie' toegang kunnen krijgen tot gegevens die door Solvinity in opdracht van de Staat worden verwerkt?

Medewerkers van Solvinity hebben bij het uitvoeren van reguliere beheerwerkzaamheden geen toegang tot de database waarin gegevens van burgers en gegevens over waar burgers inloggen staan opgeslagen. Dit sluit niet uit dat medewerkers toegang kunnen krijgen tot deze databases. Het zal hierbij dan gaan om (on)geautoriseerde toegang. Mogelijk is daarmee de medewerker strafbaar.

8. Bent u van mening dat er momenteel geen gelijkwaardige technologieën zijn op Nationaal/Europees gebied? Zo ja, bent u dan van mening dat hierdoor de continuïteit van de dienstverlening juist onder druk komt te staan?

Het kabinet is van mening dat er momenteel wel gelijkwaardige technologieën zijn van Nederlandse en Europese aanbieders. In een Kamerbrief in reactie op de motie van het lid Koekkoek (Volt) over ‘in EU verband pleiten voor versnelde investeringen in Europese cloudalternatieven en digitale infrastructuur’ heeft het kabinet de Kamer vorig jaar geïnformeerd dat er kwalitatief hoogwaardige Europese clouddiensten op de markt beschikbaar zijn.

Specifiek ten aanzien van de dienstverlening die door de Rijksoverheid bij Solvinity wordt afgenomen, concludeerde de ACM in haar concentratiebesluit dat er ook na een eventuele overname voldoende concurrentie over zou blijven. Uit het onderzoek blijkt dat afnemers uit de publieke sector op het moment van een (her)aanbesteding voldoende keuze houden uit andere IT-dienstverleners die soortgelijke diensten leveren, waaronder zowel Nederlandse als Europese aanbieders.

Wel kan het versneld onderbrengen van de dienstverlening van Solvinity bij een andere beheerorganisatie leiden tot risico’s. In het geval van Logius geldt een overdrachtsperiode van 6 tot 12 maanden wanneer de dienstverlening die Solvinity levert, ondergebracht wordt bij een andere beheerorganisatie. Deze periode is nodig om een andere beheerorganisatie kennis en ervaring te laten opdoen met het beheer van het platform om zo de continuïteit en veiligheid van DigiD en andere voorzieningen te garanderen. Deze overdrachtsperiode kan pas ingaan wanneer een nieuwe contractant is geworven.

9. Kunt u reflecteren op de gehele Amerikaanse verwevenheid met technologie, zoals de hardware waar de applicaties van Solvinity op draait, de datacenters en eveneens de zeekabels? Zijn deze componenten/diensten ook in handen van Amerikaanse bedrijven? Bent u het daarom eens met de mening dat het

nationaliseren van Solvinity geen enkel effect heeft op deze risico's, gezien de verwevenheid in de keten?

Het kabinet ziet dat de EU erg afhankelijk is geworden van een klein aantal niet-Europese tech-aanbieders, waarbij het kabinet de bijdragen van deze aanbieders aan de Europese en Nederlandse economie waardeert en in algemene zin openstaat voor zakendoen met buitenlandse partijen. Afhankelijkheden kunnen echter ook risico's met zich meedragen, bijvoorbeeld als er geen alternatieven beschikbaar zijn of er risico's zijn voor ongewenste toegang tot data. Voor risicovolle strategische afhankelijkheden zet het kabinet in op mitigatie van de risico's, bijvoorbeeld door het versterken van de Europese markt.

De gevolgen van voortzetting van het huidige eigenaarschap en andere scenario's zijn onderdeel van de analyses die vallen binnen het TFEV-onderzoek van deze casus.

10. Welke concrete risico's bestaan er momenteel volgens u op het gebied van het opvragen van data, inzage in data en het (eenzijdig) stopzetten van dienstverlening, en van welke vormen van dienstverlening maakt de overheid op dit moment gebruik bij niet-Nederlandse of niet-Europese partijen?

Er wordt niet centraal bijgehouden welke overheidsorganisaties gebruik maken van diensten van niet-Nederlandse of niet-Europese leveranciers.

De Nederlandse overheid wil haar digitale autonomie en digitale soevereiniteit versterken om publieke waarden, veiligheid en continuïteit te waarborgen. Het onderbrengen van data bij niet-Nederlandse of niet-Europese leveranciers, kan in specifieke gevallen strategische, juridische en geopolitieke risico's met zich meebrengen. Daarom kiest de overheid voor een risicogebaseerde, strategisch gecoördineerde aanpak.[3]

11. Welke aanvullende (theoretische) risico's zouden volgens u kunnen ontstaan op deze punten als gevolg van de beoogde overname van Solvinity door Kyndryl?

Ik kan in deze openbare beantwoording niet ingaan op risico's die er mogelijk zouden kunnen zijn ten aanzien van gegevensvergaring en stopzetting van dienstverlening. Ik verwijs u door naar de vertrouwelijke technische briefing van BTI. Inmiddels heeft de staatssecretaris Digitale Economie en Soevereiniteit het besluit genomen om de overname te verbieden.

12. Kunt u allen de voorgaande vragen los van elkaar beantwoorden?
Ja.

[3] Visie Digitale autonomie en soevereiniteit van de overheid