Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

Aanhangsel van de Handelingen

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

695

Vragen van het lid **Kathmann** (GroenLinks-PvdA) aan de Ministers van Justitie en Veiligheid en van Economische Zaken en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *de overname van Zivver door een Amerikaans bedrijf* (ingezonden 18 september 2025).

Antwoord van Staatssecretaris **Rutte** (Justitie en Veiligheid) en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, mede namens de Minister van Economische Zaken (ontvangen 16 december 2025). Zie ook Aanhangsel Handelingen, vergaderjaar 2025–2026, nr. 221.

Vraag 1
Bent u bekend met het bericht ««Strategische blunder»: vertrouwelijke data van Nederlanders in handen van Amerikanen»?[1]

Antwoord 1
Ja.[2]

Vraag 2
Wat is uw reactie op dit bericht?

Antwoord 2
Ik heb kennisgenomen van het bericht. In de beantwoording van de hiernavolgende vragen, ga ik nader in op de inhoud.

Vraag 3
Bent u van mening dat vertrouwelijke data van Nederlanders bij voorkeur in Nederlandse handen moet zijn, dan wel Europese? Zo ja, waarom? Zo nee, waarom niet?

Antwoord 3
Het antwoord op de vraag of vertrouwelijke data van Nederlanders bij voorkeur Nederlandse handen moet zijn, is afhankelijk van de aard van de gegevens die worden verwerkt, en is daarom niet in algemene zin te beantwoorden.

---

[1] Follow The Money, 13 september 2025, «Strategische blunder»: vertrouwelijke data van Nederlanders in handen van Amerikanen.
[2] Artikelen 45 AVG en 46 AVG.

ah-tk-20252026-695
ISSN 0921 - 7398
's-Gravenhage 2025

Overheidsorganisaties zijn bij het aangaan van overeenkomsten met leveranciers gebonden aan juridische en beleidsmatige kaders die de bescherming van vertrouwelijke data waarborgen.[3] De Algemene Verordening Gegevensbescherming (AVG) beschermt de rechten en vrijheden van personen bij de verwerking van hun persoonsgegevens, onder meer door te eisen dat organisaties passende beveiligingsmaatregelen nemen om die gegevens te beschermen.[4]
De doorgifte van persoonsgegevens naar een derde land is toegestaan als de Europese Commissie (EC) heeft vastgesteld dat dit land een passend beschermingsniveau biedt, of als de doorgifte is voorzien van passende waarborgen en de betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken. Als geen adequaatheidsbesluit of passende waarborgen beschikbaar zijn, mogen persoonsgegevens alleen worden doorgegeven wanneer één van de in de in artikel 49 AVG genoemde uitzonderingen van toepassing is (zoals expliciete toestemming, contractuele noodzaak, vitaal belang of openbaar belang). Anders is doorgifte enkel toegestaan indien de doorgifte niet repetitief, een beperkt aantal betrokkenen betreft, en noodzakelijk is voor dwingende gerechtvaardigde belangen van de verwerkingsverantwoordelijke die niet ondergeschikt zijn aan de belangen of rechten en vrijheden van de betrokkene. Dan dient de verwerkingsverantwoordelijke alle omstandigheden in verband met de gegevensdoorgifte te hebben beoordeeld en op basis van die beoordeling passende waarborgen voor de bescherming van persoonsgegevens te hebben geboden. Ook moet de doorgifte worden gemeld aan de toezichthouder. Binnen deze kaders zijn verwerkingsverantwoordelijke departementen of overheidsorganisaties zelf verantwoordelijk voor de naleving.[5]
De gegevensbeschermingseffectenbeoordeling (DPIA) speelt daarbij een belangrijke rol. De DPIA brengt de gegevensbeschermingsrisico's van een voorgenomen (grensoverschrijdende) verwerking in kaart, en laat zien welke maatregelen nodig zijn om deze risico's te beperken. Overheidsorganisaties zijn verplicht een DPIA uit te voeren bij (grensoverschrijdende) verwerkingen met waarschijnlijk een hoog risico voor rechten en vrijheden van burgers. De Functionaris Gegevensbescherming (FG) van de verwerkingsverantwoordelijke toetst de DPIA in zijn onafhankelijke rol, en adviseert. Bij het wijzigen van de met de verwerking gepaarde risico's dient opnieuw te worden beoordeeld of de verwerking overeenkomstig de DPIA wordt uitgevoerd.[6]

Vraag 4
Erkent u dat de overname van Zivver door het Amerikaanse bedrijf Kiteworks risico's meedraagt voor de veiligheid en vertrouwelijkheid van de data die wordt uitgewisseld via deze dienst?

Antwoord 4
Ja, het feit dat Zivver nu onder Amerikaans eigenaarschap valt, betekent dat ook Amerikaanse wetgeving, zoals de Cloud Act, van toepassing kan zijn op de dienstverlening. Verwerkingsverantwoordelijke departementen moeten dit gewijzigde stelsel betrekken in hun risicoafweging bij het gebruik van Zivver.

Vraag 5
Kunt u uitsluiten dat gegevens die uitgewisseld worden via deze dienst in de Verenigde Staten of Israël terechtkomen? Zo ja, hoe kunt u dat aantonen?

Antwoord 5
Het kabinet heeft op dit moment geen aanwijzingen dat gegevens in strijd met het gegevensbeschermingsrecht in handen van de overheid in de VS of Israël terechtkomen, maar kan het ook niet met volledige zekerheid uitsluiten.

---

[3] Implementatiekader risicoafweging cloudgebruik | Rapport | Rijksoverheid.nl
[4] Artikel 5, lid 1, onder f, AVG.
[5] Vgl Handleiding Algemene verordening gegevensbescherming, p 86 e.v.
[6] Vgl. de Richtsnoeren gegevensbeschermingseffectbeoordeling (WP248 rec.01, goedgekeurd door de EDPB op 25 mei 2018). Beschikbaar via: https://autoriteitpersoonsgegevens.nl/uploads/imported/wp248_rev.01_nl.pdf

Vraag 6
Op welke manier maken overheidsorganisaties en departementen gebruik van Zivver? In hoeverre is de continuïteit van de overheidsdienstverlening afhankelijk van dit bedrijf?

Antwoord 6
Verschillende overheidsorganisaties maken gebruik van Zivver voor het delen van informatie. Ofwel voor het delen van documenten, ofwel voor beveiligd mailen. Datzelfde geldt voor ketenpartners waarmee door overheidsorganisaties in de uitvoering wordt samengewerkt. De continuïteit van de dienstverlening is niet afhankelijk van Zivver.

Vraag 7
Heeft de Amerikaanse overname van Zivver gevolgen voor het gebruik van deze dienst door Nederlandse overheden? Vindt u het verantwoord om de huidige inzet van Zivver ongewijzigd te laten?

Antwoord 7
Overheidsorganisaties geven binnen hun eigen verantwoordelijkheid invulling aan het gebruik van clouddiensten en de daarbij behorende afwegingen.[7] Deze dienen te berusten op een gedegen risicoanalyse, waaronder in voorkomende gevallen een DPIA en passende mitigerende maatregelen waar nodig. Departementen nemen hierover besluiten binnen hun eigen mandateringsregelingen. Als onderdeel van het cloudbeleid dienen beveiligingsmaatregelen genomen te worden en risicoanalyses geactualiseerd te worden wanneer daartoe aanleiding is.[8]

Vraag 8
Draagt het blijven gebruiken van Zivver, ook nu het is overgenomen door een Amerikaans bedrijf, bij aan de cyberveiligheid en autonomie van Nederland? Zo ja, kunt u onderbouwen waarom dit geen risico vormt? Zo nee, waarom gebruikt u deze dienst dan alsnog?

Antwoord 8
Een dergelijke verandering maakt het wenselijk om risico's opnieuw te beoordelen in de context van het concrete gebruik, de aard van gegevens die worden uitgewisseld, de getroffen beveiligingsmaatregelen, en de specifieke geldende contractuele (juridische) en technische waarborgen.

Vraag 9
Kunt u onafhankelijk aantonen dat Zivver na de overname van een Amerikaans bedrijf een gelijke mate van rechtsbescherming en vertrouwelijkheid waarborgt als voorheen? Zo nee, bent u bereid dit alsnog te onderzoeken en op basis van de uitkomsten het gebruik van deze dienst (her)evalueren?

Antwoord 9
Zoals uiteengezet in het antwoord op vraag 3 en 4 dienen verwerkingsverantwoordelijke overheidsorganisaties bij (mogelijke) verandering van de risico's, zoals in casu de overname van Zivver, te beoordelen of de verwerking nog steeds overeenkomstig de DPIA wordt uitgevoerd. Indien nodig dienen aanvullende maatregelen te worden genomen om de vereiste mate van rechtsbescherming en vertrouwelijkheid te waarborgen.

Vraag 10
Vindt u het wenselijk dat een dienst die wordt gebruikt om vertrouwelijke informatie over burgers uit te wisselen valt onder de Amerikaanse CLOUD Act en de Foreign Intelligence Surveillance Act (FISA), die de regering-Trump toegang geeft tot deze data?

---

[7] Implementatiekader risicoafweging Cloudgebruik.
[8] Artikel 4 en 9 Implementatiekader risicoafweging Cloudgebruik.

Antwoord 10
Het kabinet vindt het, in dergelijke gevallen, niet wenselijk dat vertrouwelijke informatie bij statelijke actoren terecht komt. Het Nationaal Cyber Security Centrum (NCSC) heeft in augustus 2022 een juridische analyse laten uitvoeren door het advocatenkantoor Greenberg Traurig naar de mogelijke impact van de Amerikaanse CLOUD Act. In dit onderzoek kwam destijds naar voren dat het risico op openbaarmaking van Europese (persoons)gegevens onder de Cloud Act klein lijkt.[9]
Tegelijkertijd, en zoals uiteengezet in het antwoord op vraag 3 en 4, dienen verwerkingsverantwoordelijke overheidsorganisaties bij (mogelijke) veranderingen risico's in kaart te brengen door het uitvoeren van een DPIA. Ook de mogelijke implicaties van bijvoorbeeld delen van de Cloud Act voor grondrechten dienen in deze risicoafweging te worden betrokken.

Vraag 11
Welke maatregelen gaat u op korte termijn nemen om de veiligheid en vertrouwelijkheid van burgerdata beter te waarborgen? Zijn er (Europese) alternatieven voorhanden die u kunt gebruiken in plaats van Zivver?

Antwoord 11
Vanuit het Ministerie van BZK zijn, in samenwerking met andere onderdelen van de Rijksoverheid, al verschillende initiatieven gestart. Vanaf 1 januari 2026 gelden er nieuwe beveiligingseisen voor bedrijven die voor de overheid een opdracht uitvoeren met risico's voor de nationale veiligheid. Dat zijn de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO). Door de ABRO gelden binnen de hele Rijksoverheid dezelfde eisen. De ABRO verkleint de risico's voor de nationale veiligheid, zoals cyberaanvallen en spionage. Daarnaast is er recent een handreiking opgesteld voor het risicomanagement binnen departement overstijgende ketens.[10] De BIO2 biedt een uniforme aanpak en een gemeenschappelijk normenkader voor informatiebeveiliging binnen de overheid, waarbij risicomanagement centraal staat.
Met het oog op het selecteren van alternatieven moeten de risico's worden beoordeeld en de noodzakelijke maatregelen voor informatiebeveiliging worden vastgelegd. De in verband met informatiebeveiliging en gegevensbescherming noodzakelijke maatregelen zullen daarbij moeten worden vastgelegd en meegenomen in de aanbesteding en eventuele overeenkomst.

Vraag 12
Beschikt de Rijksoverheid over een eigen infrastructuur om vertrouwelijk te communiceren? Is het mogelijk om op korte termijn de diensten van Zivver in te wisselen voor een eigen alternatief?

Antwoord 12
Binnen de Rijksoverheid maken verschillende departementen reeds gebruik van andere oplossingen voor het veilig uitwisselen van bestanden en berichten. Een voorbeeld hiervan is Securetransfer, dat SSC-ICT aanbiedt vanuit het rijksdatacentrum ODC-Noord.[11]
Er loopt momenteel vanuit de Nederlandse Digitaliseringsstrategie wel een verkenning naar het opzetten van een overheidsbrede soevereine cloud, waarin het voorstelbaar is dat er vertrouwelijke gegevensuitwisseling plaats kan gaan vinden. Het realiseren van een soevereine overheidscloud vraagt wel om de nodige investeringen.

Vraag 13
Bent u van mening dat overnames van bedrijven als Zivver voortaan getoetst moeten worden op gevolgen voor de (cyber)veiligheid? Bieden de Telecommunicatiewet en de Wet veiligheidstoets investeringen, fusies en overnames (Wet Vifo) hier al de mogelijkheid voor?

---

[9] Cloud Act Memo | Publicatie | Nationaal Cyber Security Centrum
[10] https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2025/01/Handreiking-Risicomanagement-Digitale-Weerbaarheid.pdf
[11] Secure Transfer, veilige bestandsuitwisseling ODC-Noord

Antwoord 13
De Wet veiligheidstoets investeringen, fusies en overnames (Wet vifo) en de Telecommunicatiewet bevatten ieder een toetsingskader om risico's voor de nationale veiligheid bij verwervingsactiviteiten te kunnen adresseren. De Wet Vifo is gericht op verwervingsactiviteiten die betrekking hebben op vitale aanbieders, ondernemingen die actief zijn op het gebied van bepaalde sensitieve technologie, en beheerders van een bedrijfscampus. De Telecommunicatiewet kent eveneens een specifiek toetsingsregime voor zeggenschapswijzigingen bij aanbieders van telecompartijen, waaronder aanbieders van gekwalificeerde vertrouwensdiensten. Als een onderneming niet valt onder het specifiek omschreven wettelijk toepassingsbereik (en dus bijvoorbeeld geen specifieke sensitieve technologie heeft, geen betrekking heeft op een vitaal proces, of de criteria uit de Telecommunicatiewet niet haalt), dan is een verwervingsactiviteit ten aanzien van die onderneming niet meldingplichtig en kan de Minister van Economische Zaken niet ingrijpen. Voor dit uitgangspunt is onder andere gekozen met het oog op de proportionaliteit: de *ex ante* meldingplicht en de toetsingsbevoegdheid van de Minister moet niet verder gaan dan strikt nodig is. Ook komt het vooraf vastleggen wanneer een transactie meldingsplichtig is de rechtszekerheid ten goede (door het voorkomen van willekeurig of politiek-gedreven ingrijpen in de markt). Ook heeft het kabinet beoogd alleen de meest risicovolle categorieën ondernemingen af te dekken. Met de bestaande wetgeving bestaat dus de mogelijkheid om overnames die de nationale veiligheid kunnen raken te toetsen, indien deze vallen binnen het toepassingsbereik van die wetten. Indien blijkt dat aanvullende sectoren of technologieën een zodanig veiligheidsbelang vertegenwoordigen dat zij onder de Wet Vifo of de Telecommunicatiewet zouden moeten vallen, kan het toepassingsbereik van de wet worden uitgebreid. Het kabinet volgt relevante ontwikkelingen op dit gebied op de voet. Zo werkt het kabinet momenteel aan een uitbreiding van het toepassingsbereik van de Wet Vifo voor enkele aanvullende sensitieve technologieën.

Vraag 14
Kunt u verklaren waarom bedrijven die de vertrouwelijke communicatie voor overheden verzorgen niet zijn aangemerkt als vitale infrastructuur, ook als de organisaties die ze gebruiken wel aangemerkt zijn als belangrijk/vitaal/essentieel?

Antwoord 14
Zivver is niet als digitale essentiële dienst aangemerkt. De Wet weerbaarheid kritieke entiteiten (Wwke) schrijft ministeries voor om periodiek vitaal beoordelingen uit te voeren, zo ook voor de digitale infrastructuur.

Vraag 15
Biedt de Cyberbeveiligingswet of de Wet weerbaarheid kritieke entiteiten mogelijkheden om niet-Europese overnames van bedrijven als Zivver te voorkomen? Zo nee, vindt u dit wel wenselijk?

Antwoord 15
De NIS2-richtlijn heeft tot doel om de cyberbeveiliging in de EU verder te versterken en de CER-richtlijn tot doel om de weerbaarheid van essentiële diensten binnen de EU te vergroten. Daartoe bevatten de richtlijnen onder meer verplichtingen voor hieronder vallende entiteiten om passende en evenredige technische, operationele en organisatorische (beveiligings)maatregelen te nemen en om significante incidenten te melden. De NIS2-richtlijn en de CER-richtlijn bevatten geen regels die zien op overnames van bedrijven door niet-Europese partijen. In Nederland wordt de NIS2-richtlijn geïmplementeerd met de Cyberbeveiligingswet en wordt de CER-richtlijn geïmplementeerd in de Wet weerbaarheid kritieke entiteiten. Aangezien de NIS2-richtlijn en CER-richtlijn geen regels bevatten over overnames van bedrijven door niet-Europese bedrijven, wordt dit evenmin geregeld in de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten.
In Nederland worden bepaalde verwervingsactiviteiten getoetst door het kabinet krachtens investeringstoetsingswetgeving zoals de Wet Vifo en de Wet ongewenste zeggenschap telecommunicatie. Deze investeringstoetsen zijn landenneutraal. De toetsende autoriteit (het Bureau Toetsing Investerin-

gen van het Ministerie van Economische Zaken) neemt de identiteit van de verwerver mee in de toetsing.

Vraag 16
Hoe beoordeelt u de betrokkenheid van Israëlische oud-spionnen aan de top van het bedrijf Kiteworks? Is dit voor u een reden om het gebruik van Zivver wel of niet te heroverwegen?

Antwoord 16
Er is geen aanleiding om op dit moment aan te nemen dat de betrokkenheid van voormalige Israëlische inlichtingenfunctionarissen bij Kiteworks risico's oplevert voor het gebruik van Zivver binnen de Rijksoverheid. In het rijksbrede cloudbeleid is opgenomen dat indien er een risico afkomstig van statelijke actoren is, de gebruiker van de clouddienst beveiligingsadvies in dient te winnen de AIVD en/of MIVD.[12] Indien gebruikers van de clouddienst een verhoogd risico signaleren in verband met statelijke actoren, is dit de aangewezen route om te komen tot een onderbouwd oordeel over eventuele heroverweging van het gebruik van Zivver als digitale dienst.

Vraag 17
Hoe reageert u op de bevindingen van Follow The Money waaruit blijkt dat informatie verstuurd via Zivver wordt teruggekoppeld naar de servers van het bedrijf? Welke gevolgen heeft dit voor de veiligheid en vertrouwelijkheid van deze informatie?

Antwoord 17
Informatiestromen, zoals de informatiestroom die is beschreven in het artikel op Follow the Money, dienen volgens het rijksbrede cloudbeleid te worden betrokken bij de risicoafweging die verplicht is voorafgaand aan het gebruik van clouddiensten. Zoals ook in het artikel wordt beschreven, kunnen aanvullende lokale veiligheidsinstellingen aangebracht worden, bijvoorbeeld in Outlook of Gmail, om te voorkomen dat gevoelige informatie naar externe servers wordt verzonden. Zivver geeft aan dat vrijwel alle overheidsklanten, zorginstellingen en andere kritieke organisaties de Outlook-integratie om die reden gebruiken.[13]
Het instellen van dergelijke beveiligingsmaatregelen is daarmee een logische uitkomst van de verplichte risicoafwegingen.

Vraag 18
Kunt u deze vragen los van elkaar en zo snel mogelijk beantwoorden?

Antwoord 18
Ja.

[12] Artikel 6 Implementatiekader risicoafweging cloudgebruik
[13] https://www.zivver.com/hubfs/Vragen%2c%20antwoorden%20en%20communicatie%20tussen%20Follow%20The%20Money%20en%20Zivver.pdf