Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

Aanhangsel van de Handelingen

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

1597

Vragen van de leden **Kathmann** (GroenLinks-PvdA) en **Six Dijkstra** (Nieuw Sociaal Contract) aan de Staatssecretaris en de Minister van Binnenlandse Zaken en Koninkrijksrelaties over *de nieuwe werkplek van SSC-ICT* (ingezonden 7 maart 2025).

Antwoord van Staatssecretaris **Szabó** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 12 maart 2025).

Vraag 1
Is de gedeeltelijke migratie van de 58.000 digitale werkplekken van ambtenaren naar de *public cloud* strikt noodzakelijk? Waaruit blijkt dit?[1]

Antwoord 1
De migratie van de werkplekken van de Rijksoverheid die SSC-ICT aan het voorbereiden is, is noodzakelijk omdat meerdere componenten van de huidige werkplek op korte termijn niet meer ondersteund worden (End of Support) of zelfs het einde van hun levensduur hebben bereikt (End of Life). Het eerste geldt bijvoorbeeld voor Windows 10 (oktober 2025) en het tweede voor Ivanti (december 2026). Om continuïteit te borgen is het dus noodzakelijk deze componenten te vervangen. Daarnaast is het vanuit beveiligingsoogpunt van belang om over te stappen naar een modernere en veiligere werkplek. De migratie naar de nieuwe werkplek betreft overigens geen migratie naar de cloud. Alle documenten en mails blijven in de eigen overheid-datacenters; alleen bepaalde beheerapplicaties gaan deels naar de cloud[2].

Vraag 2
Hoeveel zou de voorgenomen cloudmigratie kosten?

Antwoord 2
De migratie wordt deels bekostigd uit het al aan SSC-ICT beschikbaar gestelde ICT-budget dat bedoeld is voor doorontwikkeling van haar ICT-diensten. Daarnaast is een aanvullend budget van € 8,7 mln. voorzien voor migratie- en uitrolkosten.

[1] Kamerstuk 26 643, nr. 1282
[2] Voor alle beheerfuncties die in de cloud worden belegd zal een exitstrategie worden opgesteld.

ah-tk-20242025-1597
ISSN 0921 - 7398
's-Gravenhage 2025

Vraag 3
Deelt u de mening dat cloudmigraties van overheids-ICT naar Amerikaanse techgiganten geen vanzelfsprekendheid meer moeten zijn, gezien de onvoorspelbare geopolitieke situatie en de reële kans op een handelsoorlog met de Verenigde Staten?

Antwoord 3
Iedere cloudmigratie moet weloverwogen plaatsvinden, conform de waarborgen zoals gesteld in onder meer het Rijksbreed cloudbeleid 2022. Daarnaast is het voorkomen van risicovolle strategische afhankelijkheden een belangrijk onderdeel vanuit de Agenda DOSA.[3]
Een van de maatregelen die het kabinet neemt, is de herziening van het rijksbrede cloudbeleid, dat u medio 2025 ontvangt. In dit beleid wordt het gebruik van public cloud aangescherpt. Cloudtechnologie biedt onmiskenbare voordelen, zoals flexibiliteit, innovatie en gebruiksgemak, maar vereist ook zorgvuldige afwegingen om de digitale autonomie en veiligheid te waarborgen. Deze aspecten krijgen nadrukkelijker een plek in het nieuwe beleid. Daarnaast wordt actief met Europese partners samengewerkt aan alternatieve oplossingen en een goed functionerende Europese markt. Het blijft daarom van belang om risico's zorgvuldig af te wegen en waar nodig passende maatregelen te treffen, zoals ook bij de nieuwe werkplek van SSC-ICT is gebeurd. De uiteindelijke acceptatie van de (rest)risico's zal voorgelegd worden (ter acceptatie) aan de afnemers van de werkplek van SSC-ICT.[4]

Vraag 4
Klopt het dat DICTU en de Belastingdienst ook voornemens zijn om de digitale werkplekken (gedeeltelijk) naar de *public cloud* verhuizen?[5]

Antwoord 4
In het Jaarplan 2025 Belastingdienst dat uw Kamer op 11 december 2024 heeft ontvangen, is aangegeven dat de Belastingdienst voornemens is om in 2025 alle werkplekken naar M365 te migreren. Dit gebeurt gecontroleerd en weloverwogen. De implementatie van de migratie is op dit moment nog niet gestart. De Belastingdienst volgt de recente geopolitieke ontwikkelingen en zal in lijn handelen met het herijkte Cloudbeleid en implementatieplan dat door BZK wordt opgesteld en medio 2025 zal worden opgeleverd.
DICTU maakt in zijn digitale werkplek gebruik van public clouddiensten van Microsoft, maar niet van de gehele Microsoft werkplek. De belangrijkste public cloudapplicaties die door DICTU worden ingezet zijn Teams, Onedrive en Exchange Online. Deze zijn beschikbaar voor de ca. 20.000 werknemers van de Ministeries EZ, KGG en LVVN.
Voordat bovenstaande clouddiensten in gebruik genomen zijn, zijn risicoanalyses uitgevoerd op het gebied van dataprivacy en security conform het Rijkscloudbeleid.

Vraag 5
Welke cruciale software-componenten van de huidige digitale werkplek worden vanaf eind 2026 niet meer ondersteund door de leverancier(s)? Is dit door de leverancier(s) aan u bevestigd? Om welke leverancier(s) gaat het?

Antwoord 5
De software die nu nog wordt gebruikt en die na december 2026 niet meer wordt ondersteund, betreft Ivanti Workspace Control. Dit is bevestigd door de leverancier Ivanti.
Ivanti Workspace Control is een softwareoplossing die IT-beheerders helpt bij het beheren en beveiligen van gebruikersomgevingen in Windows-omgevingen. Het zorgt ervoor dat medewerkers altijd en overal toegang hebben tot hun persoonlijke werkplek, ongeacht het apparaat of de locatie. Ook Windows 10 dat op de meeste werkplekken in gebruik is, is aan het eind van de levenscyclus. Hier is wel nog (tegen additionele kosten) ondersteuning

[3] Agenda Digitale Open Strategische Autonomie, 2023. Link: Agenda Digitale Open Strategische Autonomie | Rapport | Rijksoverheid.nl.
[4] In overeenstemming met artikel 4 van het Implementatiekader dat een formele vaststelling van de risicoanalyse vereist.
[5] Naar de cloud nu je er nog mee wegkomt: is dat het? (berthub.eu, 1 maart 2025)

voor beschikbaar, maar gelet op de noodzakelijke werkzaamheden is het raadzaam om deze vernieuwingsacties te combineren.

Vraag 6
Heeft de leverancier / hebben de leveranciers van deze cruciale software-componenten bevestigd dat een oplossing, waarbij de gegevens en verwerking daarvan binnen de overheid blijven, definitief niet meer beschikbaar zal zijn?

Antwoord 6
Zie het antwoord op vraag 5. De software van Ivanti die op dit moment in gebruik is, is na 2026 niet meer te gebruiken; ook niet in een on premise variant.

Vraag 7
In de nieuwe digitale werkplek wordt volgens u «beperkt gebruik gemaakt van cloud-gebaseerde beheertoepassingen.» Om welke toepassingen van welke leverancier(s) gaat dit?

Antwoord 7
Om de nieuwe DWR2.0 werkplek te kunnen beheren en up-to-date en veilig te houden, wordt in die werkplek gebruik gemaakt van een aantal clouddiensten, waaronder Netskope, Microsoft inTune en Microsoft Defender. Deze slaan de inhoudelijke data niet op, maar zorgen ervoor dat de omgeving veilig blijft (zoals het voorkomen van malware, phishing links, etc.). Dit wordt ook wel aangeduid als «data in transit». Om dit mogelijk te maken, slaan de applicaties tijdelijk metadata en logging data op. Dat is informatie over de data, zoals de gebruikers-id, de naam van de gebruikte applicaties, het aantal up- en downloads, de datum waarop de gegevens zijn aangemaakt, het gebruikte toestel, etc. Deze gegevens staan tijdelijk in de public cloud van de leverancier (6 maanden voor MS en een zelf te configureren periode voor Netskope), t.b.v. monitoring door het Security Operations Center (SOC) van SSC-ICT. Inhoudelijke data worden hierbij niet opgeslagen.

Vraag 8
Uit welk land komt de beoogde leverancier / komen de beoogde leveranciers? Waar vindt de opslag en verwerking van gegevens plaats in deze «cloud-gebaseerde beheertoepassingen»? Welke gegevens betreft dit? En gaat overheidscommunicatie in zichtbare (onversleutelde) vorm door de servers van deze leverancier(s)?

Antwoord 8
Netskope en Microsoft zijn Amerikaanse leveranciers. Zoals aangegeven bij het antwoord op vraag 7, gaat het om data in transit. Alle data in transit is versleuteld.

Vraag 9
Is de CLOUD Act of soortgelijke wetgeving, die geforceerde toegang tot data mogelijk maakt, van toepassing op gegevens die verwerkt worden onder de «cloud-gebaseerde beheertoepassingen»?

Antwoord 9
In algemene zin geldt dat de potentiële extraterritoriale werking van Amerikaanse wetgeving ertoe kan leiden dat Amerikaanse cloudaanbieders in specifieke situaties verplicht worden om gegevens van cloudgebruikers over te dragen aan Amerikaanse inlichtingendiensten. Op verzoek van het NCSC heeft Greenberg Traurig onderzoek gedaan naar onder andere de kans dat gegevens van Europese burgers op basis van de CLOUD-act verstrekt zullen worden aan de Amerikaanse overheid. Op basis van de daaromtrent beschikbare informatie is geconcludeerd dat deze kans laag is[6].
In de casus van de nieuwe werkplek van SSC-ICT wordt echter geen overheidsdata opgeslagen op de Amerikaanse cloud; documenten en mail

[6] Nationaal Cybersecurity Centrum, *Rapport Cloud Act requests,* 2022: link Cloud Act requests | Rapport | Nationaal Cyber Security Centrum.

blijven in de eigen datacenters staan. De enige data die door deze leveranciers verwerkt wordt is metadata en logging data (zie ook vraag 8).

Vraag 10
U kondigt aan «nieuwe aanpassingen zoals de gereduceerde afhankelijkheid van de publiek cloud, de ingebouwde waarborgen.» Welke afhankelijkheden blijven er over? Om welke waarborgen gaat het?

Antwoord 10
De gereduceerde afhankelijkheid zit in het feit dat al het interne verkeer, dus tussen werkplek en alles wat in de eigen datacenters draait (eigen applicaties, mail, documenten, etc.), uitsluitend over eigen infrastructuur loopt en niet door de Netskope-cloudoplossing wordt verwerkt. Daarnaast laat ik onderzoeken of hier bovenop ook onderdelen van de cloudoplossing «on premise» (in het volledig in eigen beheer zijnde OverheidsDataCenter (ODC)) kunnen worden opgesteld en beheerd, zodat ook verkeer naar externe bronnen via de eigen datacenters loopt.
Mitigerende maatregelen worden tevens besproken in het antwoord op vraag 12

Vraag 11
Kunt u toezeggen om in de aangekondigde pilot te meten hoeveel data wordt gestuurd naar / via derde partijen, en ook om te meten wanneer het niet duidelijk is om welke partijen het gaat? Kunt u duidelijk maken of het gaat om persoonsgegevens, en zo ja, om welke persoonsgegevens? Kunt u dit in ieder geval meten voor processen zoals printen, mailen en tekstverwerking, en verslag uitbrengen aan de Kamer en extern laten valideren?

Antwoord 11
Zoals hierboven aangeven, wordt alleen de metadata en logging data van de transactie gerapporteerd. Zie hiervoor het antwoord op vraag 7. Het gaat dus niet om persoonsgegevens.

Vraag 12
Hoe gaat u komen tot een betrouwbare digitale werkplek waar alle afhankelijkheden zijn weggenomen?

Antwoord 12
Als onderdeel van de implementatie van de nieuwe werkplek door SSC-ICT zijn er al diverse risicoanalyses uitgevoerd, ook op het gebied van betrouwbaarheid, beveiliging en privacy. Naar aanleiding daarvan is een groot aantal maatregelen op deze gebieden afgesproken, die voor de start van de uitrol geïmplementeerd en getoetst zullen worden. M.b.t. afhankelijkheden zal ik blijven onderzoeken hoe deze zoveel mogelijk weggenomen kunnen worden. Op periodieke basis worden de verschillende onderdelen van de werkplek heroverwogen waarbij rekening wordt gehouden met effecten op gebruikersbeleving, security, privacy, beheersbaarheid, kosten, autonomie & continuïteit. Hierbij wordt bijvoorbeeld ook gekeken naar mogelijkheden op het gebied van open source.
Het volledig wegnemen van alle afhankelijkheden bij een digitale werkplek is in de praktijk niet realistisch en ook niet altijd noodzakelijk. Verschillende componenten in de digitale wereld zijn inherent met elkaar verbonden en kennen wederzijdse afhankelijkheden. Het streven is om risico's te beheersen tot een aanvaardbaar niveau en weloverwogen keuzes te maken. In het herziene rijksbrede cloudbeleid, dat u medio 2025 ontvangt, wordt deze aanpak verder uitgewerkt. Tegelijkertijd blijft het kabinet innovatie en digitale transformatie mogelijk maken waar dat verantwoord kan.

Vraag 13
Bent u bereid om onze inlichtingen- en veiligheidsdiensten om advies te vragen over de afhankelijkheden die zullen ontstaan door de voorgenomen migratie van de digitale werkplek? Kunt u dit advies op hoofdlijnen delen met de Kamer en meewegen in uw overwegingen over de migratie?

Antwoord 13
Er is aan meerdere partijen advies gevraagd, waaronder inlichtingen- en veiligheidsdiensten. Ik ben nog in overleg hoe we op hoofdlijnen, al dan niet vertrouwelijk, de adviezen van de inlichtingen-en veiligheidsdiensten kunnen delen. Hun adviezen zijn ter harte genomen en meegewogen in het huidige ontwerp.

Vraag 14
Wordt data uit de door SSC-ICT-ontworpen werkplekken straks lokaal én in de cloud opgeslagen, of alleen nog maar lokaal? Zijn er derde partijen die, door hun positie in de gekozen oplossing, tijdelijk zicht krijgen op onze data als deze door hun toepassingen heenstroomt?

Antwoord 14
Zie antwoord op vraag 7.

Vraag 15
Wat betekent het dat data «vooralsnog» op de eigen datacenters wordt opgeslagen? Wanneer zou dit niet meer het geval zijn?

Antwoord 15
De werkplek-data blijft nu in de eigen datacenters. Naar aanleiding van het nieuwe cloudbeleid kan bij de doorontwikkeling van de werkplek hierin verandering optreden. Maar op dit moment is dat niet aan de orde.

Vraag 16
Met hoeveel zekerheid kunt u zeggen dat er geen gevoelige overheidsinformatie of persoonsgegevens worden verwerkt op de 58.000 digitale werkplekken, als u in uw brief aan de Kamer aangeeft dat hier «gewoonlijk» geen sprake van is?

Antwoord 16
Het blijft de verantwoordelijkheid van de individuele ambtenaar om conform de geldende regelgeving veilig met informatie en gegevens om te gaan. In de nieuwe werkplek is de manier van gegevens verwerken niet anders dan nu het geval is. Via gerichte communicatie en instructies kan dit verder worden ondersteund.

Vraag 17
Kunt u deze vragen afzonderlijk van elkaar en indien mogelijk nog vóór het plenaire debat over de migratie van overheids-ICT naar het buitenland beantwoorden?

Antwoord 17
Zie alle bovenstaande antwoorden op de gestelde vragen.