Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1220

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES EN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 20 september 2024

Op 23 april 2024 heeft het kabinet de policy brief «Too late to act? Europe's quest for cloud sovereignty» van het Clingendael Institute ontvangen en aan uw Kamer gezonden.[1]

De oproep van het Instituut Clingendael (hierna: Clingendael) luidt dat het voor de digitale veiligheid van Europa van essentieel belang is dat risicovolle strategische afhankelijkheden afgebouwd worden, onder andere door het versterken van de Europese concurrentiekracht. Ook is het onbetwist dat de huidige markt voor clouddiensten niet goed functioneert en wordt gedomineerd door grote niet-Europese aanbieders van clouddiensten.

Zoals ook Clingendael in haar policy brief beschrijft, is het kabinet op de hoogte van het groeiende belang van public clouddiensten. De Rijksoverheid wordt de vraag voorgelegd om het gewenste niveau van cloudsoevereiniteit te bepalen. Het is van belang dat de overheid eigenaarschap van gegevens en controle over systemen houdt. Of en wanneer hierbij public clouddiensten van buiten Nederland of de Europese Unie gebruikt kunnen worden, zal zorgvuldig afgewogen worden. Voor de Rijksoverheid gebeurt dit op grond van het Rijksbreed cloudbeleid 2022, dat momenteel ook geëvalueerd wordt.

Gedurende de procedurevergadering van de vaste commissie voor Digitale Zaken van 13 maart 2024 heeft de commissie verzocht om de Clingendael policy brief aan de Kamer aan te bieden, voorzien van een kabinetsreactie.

[1] Kamerstuk 26 643, nr. 1158 – Clingendael rapport over Cloud | Tweede Kamer der Staten-Generaal

kst-26643-1220
ISSN 0921 - 7371
's-Gravenhage 2024

Met deze kabinetsreactie wordt tevens voldaan aan de toezegging gedaan tijdens het Commissiedebat over digitale infrastructuur en economie van 25 april 2024 om het idee van de «Bijenkorf-cloud» nader te onderzoeken.[2]

Voortbouwend op deze brief alsmede de binnenkort volgende kamerbrieven over de evaluatie van het Rijksbreed cloudbeleid en de quickscan die op basis van de SIDN casus is uitgevoerd, zal het kabinet in zijn reactie op de initiatiefnota «Wolken aan de horizon» later dit jaar met een geïntegreerde aanpak van de problematiek rondom cloud komen.

Public cloud

Clingendael beschrijft in de policy brief allereerst de doorbraak van public clouddiensten in de bredere economie. Het gebruik van clouddiensten brengt organisaties vele voordelen, met name op het vlak van efficiëntie en gebruiksgemak. Cloud is daarmee een belangrijke bouwsteen van onze digitale economie en samenleving geworden en onmisbaar bij de digitale transitie die we doormaken. Tegelijkertijd schetst Clingendael ook uitdagingen bij het gebruik van clouddiensten. Concreet beschrijven de onderzoekers de noodzaak voor afnemers om bij het gebruik van public clouddiensten een balans te vinden tussen efficiëntie, kosten en soevereiniteit, om optimaal van de voordelen van public clouddiensten gebruik te kunnen maken. Gebruikers moeten zich hierbij bewust zijn van de technische, organisatorische en juridische uitdagingen die komen kijken bij de migratie van ICT-diensten naar een public cloudomgeving. Clingendael benadrukt dat, meer nog dan andersoortige organisaties, overheden zich bij de overgang naar (public) cloud van de uitdagingen en risico's voor publieke belangen bewust moeten zijn.

Definitie Public cloud:

In het Rijksbreed Cloudbeleid 2022 wordt de in de sector gangbare terminologie gehanteerd uit de NIST Definition of Cloud Computing. De NIST is de *National Institute for Standards and Technology* uit de Verenigde Staten. In dit technologiedomein heeft «public» een andere betekenis dan bijvoorbeeld «publiek» en «privaat» (bijvoorbeeld over instellingen) in Nederlands recht. Een «publieke» of «public» cloud is een clouddienst bij een dienstverlener waar zowel de hardware als de software met andere organisaties wordt gedeeld, en waarin je (afhankelijk van de behoefte) een stukje capaciteit en verwerking krijgt toebedeeld door de dienstverlener. De verwerkingen worden van elkaar gescheiden door logische beveiligingsmaatregelen.

Logische beveiligingsmaatregelen omvatten het geheel van richtlijnen, procedures, en beheersingsprocessen en faciliteiten die noodzakelijk zijn voor het verschaffen van toegang tot informatiesystemen, besturingssystemen, netwerken, mobiele apparaten en telewerken van een organisatie.

Perspectief huidig kabinet op cloud

De bevindingen van Clingendael in dit hoofdstuk zijn grotendeels in lijn met eerder getrokken conclusies in onder andere de Staat van de Digitale Infrastructuur.[3] We hebben reeds geconstateerd dat een groeiend aantal

[2] Toezegging bij Digitale infrastructuur en economie TZ202405-003 | Tweede Kamer der Staten-Generaal

[3] Staat van de Digitale Infrastructuur – De ruggengraat van onze digitale economie | Rapport | Rijksoverheid.nl

Nederlandse consumenten en bedrijven gebruik maakt van clouddiensten.[4] Voor ons economisch verdienvermogen en onze brede welvaart is dit een positieve zaak. De voordelen van het gebruik van public clouddiensten zijn namelijk legio. Organisaties kunnen door makkelijk schaalbare, *on-demand* clouddiensten leunen op relatief hoogwaardige, veilige en continue ICT-dienstverlening voor hun bedrijfsvoering.

De migratie naar cloud brengt echter ook uitdagingen met zich mee voor gebruikers. Zoals de onderzoekers schetsen, acht het kabinet het inderdaad van belang dat organisaties bewust afwegen welke infrastructuur, data en applicaties ze in eigen beheer willen houden (on-premise) en welke veilig naar public of private clouddiensten gemigreerd kunnen worden. Daarnaast is het van belang dat gebruikers zelf afwegen welke clouddienstaanbieders ze willen gebruiken, hoeveel diensten ze willen afnemen en wat dit betekent voor hun toekomstige ICT-dienstverlening. Dit is niet alleen van belang voor overheden, maar juist ook voor andere afnemers zoals bedrijven, onderwijsinstellingen en consumenten. Voor de Rijksoverheid dienen deze afwegingen plaats te vinden conform het Rijksbreed cloudbeleid 2022.

Dat hier tegenwoordig steeds meer aandacht aan wordt besteed is meer dan terecht. Clingendael benoemt de noodzaak om bij het gebruik van public clouddiensten een balans tussen efficiëntie en soevereiniteit te vinden. Dit sluit aan op de beleidsdoelen in de Agenda Digitale Open Strategische Autonomie (DOSA), die Clingendael zelf ook aanhaalt.[5]

Deze balans is dus ook van belang, maar tegelijkertijd wordt er niet altijd bewust en zorgvuldig een afweging gemaakt door afnemers. Zo constateert de ACM-marktstudie naar clouddiensten[6] dat veel afnemers wel diensten bij verschillende cloudaanbieders afnemen (multi-cloud), maar dat dit zich veelal beperkt tot diensten die niet noodzakelijk met elkaar gekoppeld hoeven te worden. De ACM moedigt gebruikers van clouddiensten aan zich bewust te zijn van de aan afname van clouddiensten gerelateerde padafhankelijkheid[7] en daarom een afweging te maken tussen de meerwaarde van een specifieke clouddienst en de mate van vendor lock-in.

Ook spelen overwegingen op het gebied van DOSA voor gebruikers niet altijd voldoende een rol bij de keuze voor een specifieke clouddienst, aangezien vooral overwegingen rondom kosten, gebruiksgemak en efficiëntie de overhand hebben. Hierdoor ontstaat al gauw een voorkeur voor één van de grote niet-Europese aanbieders van clouddiensten. Dergelijke aanbieders hoeven op de lange termijn niet altijd de beste (makkelijkste of goedkoopste) optie te zijn voor een individuele gebruiker, o.a. vanwege de genoemde padafhankelijkheid en lock-in effecten. Het is daarom van belang dat afnemers van public clouddiensten scherp blijven op de keuzes die ze maken en de effecten daarvan, zoals ook in de policy brief goed wordt beschreven.

De (centrale en decentrale) overheid kent bij de overgang naar public clouddiensten aanvullende unieke afwegingen die meegenomen dienen te worden. Naast het feit dat de overheid graag haar digitale dienstverlening richting de burger continu wil verbeteren, zijn er ook bijzondere aandachtsgebieden. Risico's voor de nationale veiligheid dienen hierbij

---

[4] Zie bijvoorbeeld: https://digital-strategy.ec.europa.eu/en/policies/desi-netherlands
[5] https://open.overheid.nl/documenten/5cb9749c-7efa-40db-9328-5da7fa5fcb7c/file
[6] Autoriteit Consument & Markt (2022) – Marktstudie clouddiensten.
[7] Padafhankelijkheid houdt in dat het in de cloudmarkt veelal lastig is om terug te keren van een eenmaal ingeslagen weg.

meegenomen te worden. Ook dient daarbij in ogenschouw genomen te worden dat diverse landen wet- en regelgeving kennen met extraterritoriale werking die medewerking aan veiligheidsdiensten verplicht, zoals de CLOUD act in de VS[8], wat in bepaalde gevallen mogelijk kan leiden tot ongewenste toegang tot Nederlandse gegevens.

Voor de meeste gevoelige informatie van de overheid, waaronder staatsgeheime informatie en informatie waarbij rekening moet worden gehouden met inbreuken door statelijke actoren, is daarom een standaard uitgangspunt geformuleerd in het Rijksbreed Cloudbeleid: staatsgeheime informatie mag niet worden opgeslagen of verwerkt in de public cloud. Voor Departementaal Vertrouwelijk gerubriceerde informatie dient op case-by-case basis een risicoafweging te worden gemaakt, op basis waarvan de departementaal verantwoordelijk Minister kan besluiten gebruik van public clouddiensten toe te staan. Buiten de Rijksdienst is er wel sprake van (sectorale) wet- en regelgeving op het gebied van informatiebeveiliging, maar is er geen centraal verplichtend kader omtrent het gebruik van clouddiensten. Organisaties zijn zelf verantwoordelijk voor hun keuzes omtrent het gebruik van public clouddiensten, zolang zij maar voldoen aan de wettelijke kaders zoals bijvoorbeeld de Algemene verordening gegevensbescherming (AVG), Wet beveiliging netwerk- en Informatiesystemen (Wbni) en overige wet- en regelgeving.

Bijzondere aandacht daarbij dient gegeven te worden aan het classificeren van data. Uiteindelijk bepaalt, zoals ook Clingendael stelt, de classificering van de data welke technische oplossing gekozen kan en mag worden. Voor de Rijksoverheid bepaalt uiteindelijk de rubricering van de informatie in wat voor systemen de informatie verwerkt mag worden.

Ook is in het cloudbeleid extra aandacht gegeven aan en zijn waarborgen opgenomen voor privacygevoelige informatie en de basisregistraties van de overheid.[9] Indien er het risico is op de dreiging van statelijke actoren, moet er voortijdig dreigings- en beveiligingsadvies ingewonnen worden vanuit de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en/of de Militaire Inlichtingen- en Veiligheidsdienst (MIVD).

Clingendael benoemt ook het concept van community clouds, een hybride vorm van cloud computing tussen public en private clouds in, die vaak sectoraal gericht zijn. Het kabinet ziet community clouds als een geschikt model om schaalgrootte te creëren voor semi-publieke en nutsvoorzienende sectoren, waarvan de dienstverlening vanwege bijvoorbeeld grootschalige verwerking van privacygevoelige informatie of kritieke maatschappelijke dienstverlening een grotere mate van soevereiniteit vragen dan reguliere kantoorautomatisering.

Geopolitieke aspecten

In het hoofdstuk «(Geo)Politicisation of cloud services» van de policy brief beschrijft Clingendael de toenemende politisering van het debat over clouddiensten en de bestaande beleidsinzet hierop. De drie grootste Amerikaanse cloudaanbieders hebben een gezamenlijk marktaandeel van zeventig procent, terwijl de grootste Europese aanbieders gezamenlijk niet meer dan vijftien procent van de opbrengsten in de markt voor clouddiensten genereren.

---

[8] Onder de EU-U.S. Data Privacy Framework zijn, in het kader van de CLOUD act, nadere afspraken gemaakt op welke wijze en onder welke omstandigheden van dergelijke bevoegdheden gebruik gemaakt kan en mag worden.

[9] Rijksbreed Cloudbeleid 2022

Op basis van deze marktverhoudingen en de technische obstakels om over te stappen naar andere aanbieders, concludeert Clingendael dat er risicovolle afhankelijkheden bestaan van een beperkt aantal Amerikaanse cloudaanbieders.

De dominantie van Amerikaanse cloudaanbieders in Europa vormt niet enkel economisch een afhankelijkheid, maar heeft ook impact heeft op onze digitale open strategische autonomie. Het ontwikkelen van een volwaardig Europees cloudaanbod is daarom noodzaak, volgens Clingendael.

Clingendael beziet drie lagen van cloud soevereiniteit, van zwaar naar minder zwaar bezien zijn dit:
1. Cloud soevereiniteit als onderdeel van de nationale veiligheid;
2. Cloud soevereiniteit als datasoevereiniteit; en
3. Cloud soevereiniteit als voldoen aan wet- en regelgeving.

Wordt cloud soevereiniteit bezien als het voldoen aan wet- en regelgeving, houdt dit in feite niets anders in dan dat cloud overeenkomsten onder de jurisdictie vallen van een Europese lidstaat en daarmee tevens voldoen aan Europese wet- en regelgeving. Cloudsoevereiniteit als datasoevereiniteit moet hier gelezen worden als datalokalisatie – gegevens dienen binnen EU-grondgebied opgeslagen te zijn.

Een ingewikkeldere situatie doet zich voor bij cloud soevereiniteit als onderdeel van de nationale veiligheid. Hierbij worden immers ook eisen gesteld aan de herkomst van de clouddienstverlener. Om aan een dergelijk niveau te voldoen is een goed functionerende Nederlandse en Europese cloudmarkt onontbeerlijk.

Clingendael betoogt dat de EU en haar lidstaten op zoek moeten naar manieren om deze afhankelijkheden te beheersen en verkleinen. Daarvoor moet een antwoord gevonden worden op twee vragen:
- (Hoe) kunnen Europese cloudaanbieders de benodigde schaal, breedte van dienstverlening en relevantie realiseren om de digitale economische veiligheid van de EU te verzekeren?
- Of – gezien het aanzienlijke verschil tussen Europese en Amerikaanse cloudaanbieders – kan Europa nog altijd betrouwbare Europese cloud omgevingen ontwikkelen met voldoende en veilige mogelijkheden om de meest gevoelige gegevens van Europese overheden te hosten en verwerken?

Clingendael signaleert dat recent diverse ontwikkelingen en initiatieven in Europa (en specifiek Nederland) van de grond zijn gekomen om invulling te geven aan bovenstaande vragen. Ze delen het bestaand beleid op in twee soorten: initiatieven om Europese consumenten en cloudaanbieders te beschermen en initiatieven om eigen Europees cloudaanbod te stimuleren.

Clingendael merkt op dat in aanvulling op de bestaande initiatieven het inzetten van publieke aanbesteding als mechanisme om Europese cloudaanbieders te stimuleren verder verkend zou kunnen worden. In de Verenigde Staten is overheidsinkoop bij lokale cloudaanbieders een belangrijke aanzet geweest voor het realiseren van een dominant Amerikaanse cloudaanbod.

Perspectief kabinet op geopolitisering clouddiensten

De bevindingen over afhankelijkheden van een beperkt aantal dominante, vooral Amerikaanse partijen in de cloudmarkt staan niet op zichzelf, maar

sluiten aan bij de bevindingen van diverse eerdere gepubliceerde analyses over de cloudmarkt. Zo zet de eerder genoemde cloudmarktstudie van de ACM uit 2022 de economische en technische afhankelijkheden in de sector gedetailleerd uiteen. Ook verschillende andere recente publicaties maken de afhankelijkheden, risico's en kwetsbaarheden op de cloudmarkt helder inzichtelijk.[10]

Op dit moment heeft het Ministerie van Economische Zaken een onderzoek uitgezet dat nader inzicht zal bieden in (de verschillen tussen) het Nederlandse en Europese cloudaanbod enerzijds en dat van de grote Amerikaanse cloudaanbieders anderzijds. Ook zal het mogelijk handelingsperspectief verkennen voor het dichten van mogelijke verschillen tussen lokaal en Amerikaans cloudaanbod[11].

De analyse van de geopolitieke aspecten van clouddiensten volgt dezelfde lijn als door het kabinet uiteengezet in de agenda DOSA: de cloud is niet alleen een economische afhankelijkheid, maar ook van invloed op de digitale open strategische autonomie van Europa. Cloud is daarom opgenomen als één van de beleidsprioriteiten in de agenda DOSA.

De door Clingendael voorgestelde onderverdeling van cloudsoevereiniteit is helder en onderschrijft het belang van diverse niveaus van cloudsoevereiniteit, afhankelijk van het bedrijfsproces waarbij men gebruik wil gaan maken van de cloud. Na de zomer zal hiervoor een nadere uitwerking worden opgenomen in de voortgangrapportage Strategie Digitale Economie. Deze aspecten worden tevens meegenomen in de evaluatie van het Rijksbreed cloudbeleid.

Als gevolg van de potentiële extraterritoriale werking van Amerikaanse wetgeving kunnen Amerikaanse cloudaanbieders in specifieke situaties ertoe gedwongen worden 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.[12] AWS publiceert bijvoorbeeld sinds 2020 twee keer per jaar over informatieverzoeken van de Amerikaanse overheid.[13] Daaruit komt het beeld naar voren dat er in die periode geen verzoeken zijn geweest die hebben geleid tot ontsluiting naar de Amerikaans overheid van data die is opgeslagen buiten de Verenigde Staten.[14] De inzagemogelijkheid van een clouddienst kan worden geblokkeerd door bestanden te versleutelen voordat zij in de cloud worden opgeslagen. Hierbij kan alleen de gebruiker de bestanden ontcijferen en de clouddienst niet. Het versleutelen van bestanden blokkeert echter ook nuttige cloudfuncties zoals indexering of gezamenlijk

---

[10] Onderstaand een selectie van relevante recente publicaties met betrekking tot het functioneren van de cloudmarkt in Nederland en/of Europa:
- https://www.autoritedelaconcurrence.fr/en/press-release/cloud-computing-autorite-de-la-concurrence-issues-its-market-study-competition-cloud
- Berthub.eu (2024) – Cloud Native, Europa, de «Bijenkorf» Megascaler
- Berthub.eu (2024) – The Cloud Gap in Europe
- Ofcom (2023) – Cloud services market study
- Digitale toekomst Europa: meer zeggenschap over technologieën en data – TNO Vector

[11] Het uitzetten van dit onderzoek is mede ingegeven door de recente casus rondom de voorgenomen migratie van het domeinregistratiesysteem van SIDN naar Amazon Web Services. De Tweede Kamer wordt hierover geïnformeerd met een separate Kamerbrief.

[12] Cloud Act requests | Rapport | Nationaal Cyber Security Centrum (ncsc.nl)

[13] Law Enforcement Information Requests – Amazon Customer Service

[14] Onder de EU-U.S. Data Privacy Framework zijn, in het kader van de CLOUD act, nadere afspraken gemaakt op welke wijze en onder welke omstandigheden van dergelijke bevoegdheden gebruik gemaakt kan en mag worden.

editen door een groep. Een dergelijke wijze van versleuteling wordt echter nog niet door alle cloudleveranciers aangeboden.

Het is belangrijk hieraan toe te voegen dat, ongeacht de herkomst van de clouddienstverlener, het voor gebruikers van cloud van belang blijft om van een diversiteit aan clouddienstverleners gebruik te maken. Stapelingsrisico's door te veel afhankelijk te zijn van één dienstverlener kunnen de soevereiniteit en continuïteit schaden. Ook dient voorkomen te worden dat er een ongewenste geografische afhankelijkheid van enkel niet-Europese dienstverleners ontstaat. Mede hierom is in het Rijksbreed cloudbeleid 2022 de noodzaak opgenomen om contractuele afspraken te maken over een exit-strategie.

Daarom heeft het kabinet zich met diverse beleidsinitiatieven in Nederland en Europa ingezet voor een goedwerkende cloudmarkt met aanbod van Europese spelers als alternatieve optie naast de Amerikaanse cloudaanbieders, die aansluit bij de behoeften van de markt, zoals een «alles in één oplossing». Het gros van deze inzet voor de markt wordt door Clingendael samengevat in haar policy brief. De beleidsinzet delen we als kabinet in langs drie pijlers, die ten dele ook aansluit bij de categorisering die Clingendael maakt. Deze pijlers zijn:

– Protect: Met wet- en regelgeving gebruikers beschermen en marktpartijen een eerlijk speelveld bieden.
– Promote: Innovatie en de toetreding van nieuwe cloudaanbieders stimuleren. Door samen te werken en te clusteren met overheidspartijen in binnen- en buitenland is het ook mogelijk om sterker te staan en Europese aanbieders te stimuleren.
– Partner: Regelmatige samenwerking en contact met marktpartijen en expertise & best practices uitwisselen met andere overheden, zowel binnen de EU als daarbuiten.

De volgende acties maken deel uit van de bestaande beleidsinzet:

- EU Cybersecurity Scheme for Cloud Services (EUCS)
- Network and Information Systems Directive revised (NIS2)
- EU Cloud Rulebook
- Guidance on public procurement
- Rijksbreed cloudbeleid
- Gaia-X
- Important Projects of Common European Interest Cloud Infrastructure and Services (IPCEI CIS)
- Dataverordening
- Digitalemarktenverordening
- European Open Science Cloud
- Alliance for Industrial Data, Edge and Cloud

Over de voortgang op deze beleidsinitiatieven bent u op verschillende momenten separaat geïnformeerd middels verschillende Kamerbrieven. In het najaar zal in het kader van de voortgangsrapportage Strategie Digitale Economie ook bij de verschillende acties en aspecten rond cloud worden stilgestaan, ook zal meer uitleg hierover terugkomen in de kabinetsreactie op de initiatiefnota «Wolken aan de horizon».

Aanvullende acties

In aanvulling op de bestaande initiatieven, suggereert Clingendael om Rijksinkoop van clouddiensten in te zetten om Nederlandse of Europese cloudaanbieders te stimuleren. Het is immers van belang om, náást de aanbodkant, ook de vraagkant van de cloudmarkt te stimuleren. Bij inkoop hanteert het kabinet een landenneutraal beleid. Het uitsluiten van

aanbieders uit Europese lidstaten of landen die lid zijn van de Government Procurement Agreement (GPA) is in beginsel niet toegestaan.

Wel kunnen er in voorkomende gevallen redenen zijn om landen uit te sluiten. Hierbij moet men onder meer denken aan risico's voor de nationale veiligheid. Die moeten blijken uit bijvoorbeeld de quickscan en risicoanalyse nationale veiligheid.[15] Tevens onderzoekt het kabinet in het kader van de evaluatie van het Rijksbreed cloudbeleid de mogelijkheden om autonomie c.q. afhankelijkheid mee te nemen bij cloudinkooptrajecten. Daarnaast wordt ingezet op het versterken van concurrentiekracht van het Europees aanbod, kennisontwikkeling en de arbeidsmarkt.

De AIVD participeert vanuit zijn veiligheidsbevorderende taak in werkgroepen waarin (publieke) cloudbeveiligingsnormen voor gerubriceerde informatie van de EU en NAVO worden uitgewerkt. Op deze wijze vindt kennisuitwisseling en afstemming met onze partners en bondgenoten plaats. Naast protect-waarde biedt deze afstemming ook promotewaarde, omdat gelijkgeschakeld beveiligingsbeleid tussen landen schaalgrootte biedt die het voor cloudaanbieders aantrekkelijk maakt dienstverlening met hogere beveiligingsniveaus te ontwikkelen en aan te bieden.

Naast het inzetten van Rijksinkoop oppert Clingendael het idee om tot een zogeheten «Bijenkorf cloud» te komen. Hierover zegt Clingendael het volgende «Een aantrekkelijke Europese propositie vereist een «Alles in-1 pakket» – met onder meer opslag, databases, veiligheid en software ontwikkelings-instrumenten – als alternatief op bestaande Amerikaanse proposities. Alleen door samen te werken kunnen Nederlandse en andere Europese cloudbedrijven komen tot zo'n Europese «Bijenkorf Cloud Megascaler».»[16] Dit voorstel sluit aan bij lopende beleidsinitiatieven om een goed functionerende markt te creëren door middel van een ecosysteem waarin verschillende Europese dienstenaanbieders op een federatieve wijze samenwerken om tot een vraaggestuurd aanbod te komen, zonder dat er daarbij ongezonde machtsposities binnen de markt ontstaan. Hierbij is het zoals Clingendael benoemt wenselijk dat het gebruiksgemak voor afnemers van clouddiensten centraal staat en dus vraag en aanbod goed op elkaar aansluiten, waarmee Europese partijen een aantrekkelijkere keuze worden.

Naast bovengenoemde beleidsinzet zijn mogelijk aanvullende acties wenselijk. De Tweede Kamerleden Kathmann en Six Dijkstra hebben hier al een aanzet voor gedaan in de intiatiefnota «Wolken aan de horizon». Het kabinet zal een voorstel voor een geïntegreerde aanpak ten aanzien van het thema cloud als reactie op deze initiatiefnota in het najaar naar uw Kamer sturen. Deze brief kan als bouwsteen worden beschouwd voor deze geïntegreerde aanpak.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
F. Zsolt Szabó

De Minister van Economische Zaken en Klimaat,
D.S. Beljaarts

---

[15] Quickscan/risicomitigatie nationale veiligheid bij inkoop en aanbesteden | PIANOo – Expertisecentrum Aanbesteden

[16] Clingendael (2024) – Nederland en de EU: Zet in op cloudsoevereiniteit.