Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

36 574 Initiatiefnota van de leden Six Dijkstra en Kathmann over «Wolken aan de horizon»

Nr. 2 **INITIATIEFNOTA**

Inhoudsopgave **p.**

1. Inleiding

Nederland digitaliseert in een rap tempo. In alle bedrijven en organisaties liggen ingewikkelde vraagstukken over ICT op tafel. Essentiële infrastructuur is tegenwoordig veel meer dan alleen de snelwegen en bruggen die ons verbinden. Ook de digitale snelwegen waarover we onze data de wereld rond sturen en de opslag van de gevoelige gegevens van Nederlanders zijn een kwestie van nationaal belang. Onze dienstverlening, economie en veiligheid hangen ervan af. Keuzes over technologie zijn daarin allesbepalend en bij uitstek politiek.

Eén van de grootste technologische ontwikkelingen deze afgelopen jaren is de «cloud». Het is een soort digitaal duizenddingendoekje: mailverkeer, applicaties, achtergrondprocessen, opslag of de volledige digitale werkomgeving van een organisatie kunnen draaien op de computers van iemand anders. De ICT-leveranciers verkopen clouddiensten als een snoepwinkel met voor ieder wat wils. Onder één abonnement krijg je de databeheer en diensten voorgeschoteld die prima werken en de organisatie ontzorgen, met allerlei leuke extraatjes voor een afgeprijsd tarief.

kst-36574-2
ISSN 0921 - 7371
's-Gravenhage 2024

Maar wat is die «cloud» nu precies? Om te beginnen bij de basis: de **cloud** is een verzamelnaam voor IT-diensten, waaronder data-opslag en *operations* (het geheel van digitale processen), die worden aangeboden via het internet. De gebruiker hoeft zelf geen hardware of software aan te schaffen. In plaats daarvan betaalt de gebruiker met een abonnement voor de diensten en/of de infrastructuur die de leverancier aanbiedt. Er zijn verschillende modellen voor **clouddiensten**. De drie bekendste modellen zijn *infrastructure-as-a-service* (IaaS), *platform-as-a-service* (PaaS) en *software-as-a-service* (SaaS). SaaS is de meest verstrekkende van de drie, waarbij de gebruiker het beheer van zowel de applicaties, als het digitale platform, als de digitale infrastructuur (servers) waarop deze draaien, uit handen geeft aan de cloudaanbieder.

Er bestaat een **publieke cloud** en een **private cloud**. In het geval van een publieke cloud is er een generieke dienst waar veel mensen gebruik van maken. Voorbeelden hiervan zijn de iCloud, OneDrive, of de diensten van Amazon Web Services (AWS). Zowel individuele internetgebruikers als bedrijven maken hier grootschalig gebruik van. In het geval van een private cloud wordt een dienst speciaal ingericht voor één afnemer, zoals een bedrijf. Daarmee is het IT-personeel van de organisatie aan zet om eisen te stellen aan de dienst, zoals voor aanvullende veiligheidsmaatregelen.

Overstappen naar de publieke cloud blijkt aantrekkelijk. De voordelen – gebruiksgemak en lage kosten – zijn voor de eigen organisatie, de nadelen zijn voor de leverancier, zoals beheer en onderhoud. Uiteraard is dit niet zonder gevolgen. Met de vrijheid die Nederlandse organisaties hebben over het inkopen en inrichten van de eigen ICT, is er een razendsnelle migratie in gang gezet van Rijksorganisaties, Ministeries en lokale overheden die gebruik maken van clouddiensten. Dit kan logisch zijn voor het bedrijfsleven, maar niet voor het Rijk. Het is namelijk wel goed voor het kostenplaatje, maar op grote schaal ook de aanjager van grote nationale veiligheidsrisico's.

De markt van cloudleveranciers wordt namelijk volledig gedomineerd door slechts drie Amerikaanse megabedrijven – de «hyperscalers». Hun dominantie neemt toe. Zo heeft Microsoft 40–45% van de cloudmarkt in handen; Amazon heeft 30–35% veroverd; Google komt daar achteraan met 5–10%.[1] Het aandeel van Europese en Nederlandse leveranciers is zeer mager. Een keuze voor de cloud betekent vrijwel standaard de keuze voor Microsoft, Amazon of Google. Deze bedrijven hebben onder Amerikaanse wet- en regelgeving verplichtingen ten opzichte van de politieke leiding van dat land, waar een stabiele regering in de toekomst allerminst zeker is.

Dat is kwetsbaar. Terwijl per individuele organisatie de keuze om naar een publieke cloud over te stappen goed te volgen is, leidt het bij elkaar opgeteld tot een massale uitstroom van kennis, kunde en gezag over de digitale infrastructuur van Nederland. Gegevens worden opgeslagen en verwerkt door megabedrijven die hun politieke en economische belangen buiten Europa hebben liggen en zo alleenheerser worden over het digitale domein. Door innige samenwerking tussen het Rijk en Microsoft zet Nederland lokale alternatieven buitenspel. Een ICT'er wordt eerder gevraagd naar ervaring met Microsoft, dan om innige systeemkennis.

[1] «Marktstudie clouddiensten», ACM (2022), via https://www.acm.nl/nl/publicaties/marktstudie-clouddiensten

Zonder ingrijpen is het denkbaar dat er op termijn zelfs geen Nederlandse of Europese cloudindustrie overblijft. Dit schaadt onze **nationale veiligheid**, **kennispositie** en **economisch verdienvermogen**.

De initiatiefnemers dienen daarom deze nota in met aanbevelingen om vaker te kiezen voor een cloudleverancier van Nederlandse of Europese bodem. De Nederlandse autonomie kan alleen worden bewaakt als de afhankelijkheid van Amerikaanse megabedrijven afneemt. Zo verbetert de dataveiligheid, groeit de ICT-kenniseconomie in Nederland en bieden we op lange termijn serieus tegenwicht aan de vanzelfsprekende Amerikaanse leveranciers. In onstabiele tijden moet Nederland zich digitaal weerbaar tonen en actief bouwen aan Nederlands-Europese alternatieven.

Dat vraagt om een nieuwe manier van denken: besluitvorming over ICT-systemen, die onze digitale infrastructuur bepalen, hoort thuis in het hart van de politiek in plaats van versnipperd door alle bestuurslagen. Ondanks de erkende onwenselijkheid van de groeiende afhankelijkheid van techleveranciers door de regering, onder andere in de agenda Digitale Open Strategische Autonomie (DOSA), verdwijnen systemen in eigen beheer en de expertkennis die dat mogelijk maakt in rap tempo uit organisaties. Hoewel de risico's groot zijn, zowel maatschappelijk als voor de nationale veiligheid,[2] is het huidige cloudbeleid niet voldoende om deze te mitigeren.

Het langetermijnplan «Wolken aan de horizon» stelt daarom als doel om in 2029 over een volwassen nationale cloudinfrastructuur te beschikken waarmee we essentiële overheidsdiensten in eigen beheer houden. Dit is nodig om digitaal autonoom te zijn en meer zeggenschap te krijgen over kritische ICT-infrastructuur. Dat doen de initiatiefnemers vanuit de gedachte **«Nederlands waar mogelijk, Europees waar noodzakelijk.»**

De initiatiefnemers hanteren de volgende definitie van strategische autonomie: *Strategische autonomie bestaat uit het vermogen, de capaciteiten en de controle om te beslissen over, en te acteren op, essentiële onderdelen van onze economie, samenleving en democratie.*[3]

2. Probleemstelling

Omdat digitale vraagstukken zich vaak achter de schermen afspelen, worden veiligheidsrisico's bij burgers en instanties nog weinig doorleefd. De keuze voor de cloud wordt vaak gezien als slechts een onderdeel van kantoorautomatisering zonder enige bestuurlijke relevantie. Dit maakt dat er tot nu toe relatief weinig media- of maatschappelijke aandacht op gevestigd wordt, waardoor essentiële politieke keuzes over de kritische digitale infrastructuur van de overheid uitblijven. Terwijl de politiek aan zet is om risico's op de lange termijn vóór te zijn, ook als deze nu niet zichtbaar zijn.

Desondanks raakt dit alles de Nederlandse burger. In het kader van hun dienstverlening verzamelen en verwerken de overheid, het bedrijfsleven en het maatschappelijk middenveld steeds meer gegevens van, over en met betrekking tot burgers. Dit heeft tot gevolg dat burgers er niet meer aan ontkomen om bewust en onbewust zeggenschap over hun persoonlijke data aan andere partijen uit handen te geven. Onderhand is het afleveren van data een voorwaarde geworden om volwaardig mee te

---

[2] Kamerstukken 26 643, nr. 1082

[3] Naar: «Sovereignty in the Digital Age», Paul Timmers (2023), via https://link.springer.com/chapter/10.1007/978-3-031-45304-5_36

kunnen doen in de samenleving. Als zodanig moeten burgers er redelijkerwijs op kunnen vertrouwen dat er goed rentmeesterschap over hun data wordt uitgeoefend. Men moet kunnen rekenen op een hoge mate van veiligheid, privacy en controle. Er zijn betrouwbaarheidsmechanismes nodig die ervoor zorgen dat de digitale leefomgeving ook in onzekere omstandigheden in stand blijft en dat gevoelige informatie, zoals de basisregistratie personen of medische gegevens, niet op straat belandt. Het recht op een veilige openbare ruimte moet even goed gelden in het digitale domein.

Zodra een samenleving de vereiste mate van betrouwbaarheid niet meer aan haar burgers kan garanderen, omdat zowel de systemen waarvan de samenleving afhankelijk is, als de kennis óver die systemen, volledig in buitenlands beheer zijn, raken uiteindelijk burgers in de knel. Door de grootschalige verhuizing van persoonsgegevens naar landen waar bedrijven geen loyaliteit hebben richting Nederlanders, raken burgers grip over hun eigen leven kwijt. De initiatiefnemers vinden dat de essentiële dienstverlening waarop de samenleving draait, waaronder de diensten van overheden, ziekenhuizen en universiteiten, te belangrijk zijn om merendeels uit handen te geven aan het buitenland, zelfs als dat een bondgenoot betreft. Hetzelfde geldt voor de verantwoordelijkheid over de confidentialiteit, integriteit en beschikbaarheid van gevoelige informatie van en over burgers.

Om een zo duidelijk mogelijk beeld te geven van de knelpunten in dit dossier, zullen de initiatiefnemers eerst een uitgebreidere situatieschets geven van het Nederlandse cloudlandschap en aangeven welke ontwikkelingen er daarin gaande zijn. Vervolgens beargumenteren ze waarom de situatie zoals hij momenteel is, onwenselijk is en er een noodzaak bestaat voor een hogere mate van strategische autonomie in de cloud. Ten slotte komen ze tot aanbevelingen hoe dit gerealiseerd kan worden.

Overheden

De inbedding van niet-Europese publieke cloudproviders groeit gestaag en raakt alle bestuurslagen. ICT-systemen die voorheen fysiek op locatie aanwezig waren, worden ingeruild voor cloudoplossingen. Een marktstudie van de Autoriteit Consument & Markt (ACM) constateert het volgende: «Ook (publieke) organisaties zoals scholen, zorginstellingen en overheidsinstellingen maken in groeiende mate gebruik van clouddiensten. Nederland staat daarmee in de top 5 van landen waarin er het meest wordt besteed aan clouddiensten als percentage van de totale IT-kosten.»[4]

De Vereniging van Nederlandse Gemeenten (VNG) spreekt van een «verSaaSing» van gemeenten, een trend waarin applicaties én de digitale omgeving waarop zij draaien als een pakket *(software-as-a-service)* worden aangekocht van dezelfde leverancier. De verwachting is dat het aandeel SaaS in het totale applicatielandschap van gemeenten in 2025 toeneemt tot 70%.[5] Grotendeels worden SaaS-oplossingen ingekocht bij Microsoft, daardoor vrezen sommige gemeenten voor een te grote leveranciersafhankelijkheid. Helaas verkennen ze nu enkel de mogelijkheid

[4] «Marktstudie clouddiensten», ACM (2022), via https://www.acm.nl/nl/publicaties/marktstudie-clouddiensten

[5] «Analyse cloudontwikkelingen gemeenten», VNG (2023), via https://vng.nl/projecten/ggi-cloud-expertisecentrum

om uit te breiden naar andere grote providers als Google Cloud en Amazon Web Services.[6] Nederlandse alternatieven blijven uit.

Sinds 2022 is het de Rijksoverheid toegestaan gebruik te maken van commerciële clouddiensten. In het cloudbeleid van het Rijk staat dat er maatregelen moeten worden genomen om afhankelijkheden van buitenlandse technologiebedrijven te beheersen, echter blijkt de keuze in individuele gevallen telkens uit te vallen in het voordeel van commerciële clouddiensten, aangeboden door slechts drie grote Amerikaanse bedrijven. Uit het jaarlijkse overzicht van het Forum Standaardisatie, dat de aanbestedingen van de Rijksoverheid onderzoekt, blijkt dat de keuze voor clouddiensten steeds vanzelfsprekender wordt.[7] De nauwe samenwerking tussen de Rijksoverheid en cloudaanbieders als Microsoft wordt bekrachtigd door samenwerkingen als het «Strategisch Leveranciersmanagement Microsoft Rijk»[8] (later omgedoopt tot «SLM Microsoft, Google Cloud en Amazon Web Services»[9]).

Per individuele casus zijn er meestal uitlegbare voordelen voor het kiezen voor dergelijke grote cloudaanbieders, zoals de beheersbare kosten, lage onderhoudslasten en gebruiksgemak. De gevolgen op de lange termijn worden echter buiten beschouwing gelaten en zijn ook geen onderdeel van het inkoopbeleid.

Recent maakte de Stichting Internet Domeinregistratie Nederland (SIDN) nog bekend dat zij het systeem waarmee nieuwe websites en mailadressen worden toegevoegd aan het .nl-domein, onder willen brengen in de cloud van AWS. De initiatiefnemers zien dit als een ontluisterend voorbeeld van onze afhankelijkheid van buitenlandse leveranciers. Als Nederland het eigen .nl-domein niet meer kan beheren, wat dan nog wel? In Nederland ontbreekt het arbeidsaanbod om de dienst te beheren, zo was het idee. Daarmee verdwijnt er weer een onderdeel van de kritische digitale infrastructuur in Nederland uit ons beheer, terwijl een lokaal alternatief mogelijk is. Voor de initiatiefnemers is dit reden om op te roepen tot een heroverweging van dit besluit en een duidelijke aanleiding dat er maatregelen nodig zijn om de beschikbaarheid en het gebruik van betrouwbare Nederlands-Europese clouddiensten te vergroten.

In de beantwoording van Kamervragen over deze keuze van de SIDN, die onder andere door de initiatiefnemers gesteld zijn, zet de Minister van Economische Zaken en Klimaat ferm in op het behouden van het domeinregistratiesysteem in Nederland mits dit mogelijk blijkt.[10] Sindsdien constateren de leden dat er goed overleg is met de Nederlandse cloudsector,[11] dat het Rijksbrede cloudbeleid wordt herzien met oog op strategische autonomie[12] en dat het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties een strategische verkenning heeft aange-

---

[6] «Behoefteonderzoek cloudondersteuning», VNG (2023), via https://vng.nl/projecten/ggi-cloud-expertisecentrum

[7] «Monitor Open Standaarden 2023», Forum Standaardisatie (2024), via https://www.forumstandaardisatie.nl/metingen/monitor

[8] «Strategisch Leveranciersmanagement Microsoft Rijk (SLM Rijk)», Rijksoverheid (2018), via https://www.rijksoverheid.nl/documenten/publicaties/2018/11/12/strategisch-leveranciersmanagement-microsoft-rijk-slm-microsoft

[9] https://slmmicrosoftrijk.nl/

[10] «Antwoorden op Kamervragen over verhuizing.nl-domein», Minister van Economische Zaken en Klimaat (2024), via https://www.rijksoverheid.nl/documenten/kamerstukken/2024/03/22/beantwoording-kamervragen-verhuizing-nl-domein

[11] Bijdrage Micky Adriaansens op LinkedIn (april 2024)

[12] Kamerstukken 26 643, nr. 1149

kondigd naar digitale soevereiniteit.[13] Toch bereikt Nederland een mate van afhankelijkheid van buitenlandse hyperscalers die de initiatiefnemers grote zorgen baart en niet in lijn is met de uitgesproken ambitie om de strategische autonomie te bevorderen.

Publieke sector

Dit is niet enkel een probleem bij overheden. Ook andere vormen van publieke of semi-publieke organisaties stappen massaal over naar de clouddiensten van Amerikaanse hyperscalers. Uit onderzoek van de TU Delft blijkt dat bij Nederlandse universiteiten het gebruik van Microsoft voor hun mailservers is uitgegroeid van nog slechts een paar procent in 2018 tot wel 50% in 2022.[14]In datzelfde onderzoek wordt aangegeven dat de massale groei sinds 2019 te verklaren is door een Kamerbrief uit juli 2019 van de Minister van Justitie en Veiligheid,[15] waarin staat dat het Ministerie – samen met het Strategisch Leveranciers-management Microsoft – tot een verbeterplan is gekomen om de privacyveiligheid op Microsoft clouddiensten te borgen. Ter illustratie: deze brief is door de TU Eindhoven vervolgens expliciet genoemd als aanleiding om de maildiensten naar Microsoft te verhuizen, omdat de zorgen rondom privacy en veiligheid voldoende waren weggenomen. Als grootste IT-opdrachtgever van Nederland is de Rijksoverheid een toonbeeld voor andere organisaties. In de Kamerbrief staat niets vermeld over de gevolgen van leveranciersafhankelijkheid of autonomie. Het onderzoek belicht de risico's hiervan op o.a. de academische vrijheid, privacy van studenten en docenten, en de «soft power» die de techgiganten in handen hebben door de groeiende afhankelijkheid.

Ook in de zorg, waar een veelvoud aan gevoelige gegevens wordt verwerkt, is er een zorgwekkende centralisatie van data gaande die via leveranciers van medische apparatuur in de cloud van Amazon belandt. In 2023 berichtte Follow the Money[16] over het Navify-platform, door farmacieconcern Roche Diagnostics. Dit platform brengt de diagnose en behandelgeschiedenis van patiënten samen, waarin hun gegevens enkel gepseudonimiseerd zijn. De Autoriteit Persoonsgegevens wijst er herhaaldelijk op dat pseudonimisering vaak een onvoldoende waarborg is van gegevens, gezien deze – vooral in het geval van specialistische en persoonlijke behandelplannen – mogelijk herleidbaar zijn naar individuen.[17] Bovendien is het maar de vraag of de verstrekkers van patiëntgegevens deze voldoende afgeschermd invoeren.

De kwalijkheid van deze situatie lijkt niet doorgedrongen bij veel bestuurders van zorginstellingen. Een citaat van de directeur van Calculus Software, verantwoordelijk voor de opslag van driekwart van de Nederlandse huisartsendossiers, is veelzeggend: «Voor niemand is het een heel

---

[13] «BZK start strategische verkenning naar digitale soevereiniteit», iBestuur (2024), via https://ibestuur.nl/artikel/bzk-start-strategische-verkenning-naar-digitale-soevereiniteit/

[14] «Heads in the Clouds? Measuring Universities» Migration to Public Clouds: Implications for Privacy & Academic Freedom», T. Fiebig et al (2023)

[15] Kamerstukken 32 761 nr. 622

[16] «Medische industrie zet gevoelige data van patiënten bij Amazon in de cloud, zonder dat zij dat weten», Follow the Money (2023), via https://www.ftm.nl/artikelen/medische-industrie-zet-patientendata-in-amerikaanse-cloud

[17] «Gegevens pseudonmiseren», Autoriteit Persoonsgegevens, via https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/beveiliging-van-persoonsgegevens/gegevens-pseudonimiseren

groot probleem als bekend is dat je diabetes hebt.»[18] Ook al deze dossiers staan opgeslagen in de cloud van Amazon.

Met oog op de verstrekkende bevoegdheden van de Amerikaanse overheid, bestaat de mogelijkheid dat zij via Amazon – maar de facto geldt dit voor elke Amerikaanse aanbieder – toegang kan opeisen tot een groot gedeelte van de Nederlandse medische gegevens. Hoewel gegevensdeling met organisaties in de VS sinds 2023 weer geoorloofd is onder bepaalde voorwaarden,[19]blijkt uit de berichtgeving van Follow the Money dat Amazon via een uitzonderingsclausule het recht heeft om data met de overheid te delen. De combinatie van het soort werk dat in de publieke cloud wordt gedaan en de onzekere mate van privacy die deze diensten leveren, is reden tot zorg.

Deze situatie is zoals hij is omdat er momenteel geen goed alternatief voor handen lijkt te zijn die zowel qua schaalbaarheid als functionaliteit kan bieden wat de grote hyperscalers kunnen bieden. Europese spelers hebben in het verleden nagelaten in de cloudmarkt te stappen en noodzakelijke investeringen in de binnenlandse techsector blijven uit. Een belangrijke verklaring hiervoor is het feit dat de Amerikaanse industrie een duidelijk andere financiële structuur heeft dan de Europese, waarbij veelal beduidend meer financiële risico's genomen worden om innovatie en doorgroei te stimuleren. Inmiddels lijkt het spel bepaald, maar dat is allesbehalve een reden om stil te zitten. De initiatiefnemers zien nog altijd een belangrijke rol voor Nederland weggelegd om haar rol als digitaal knooppunt van de wereld te behouden. Dat dit een politieke kentering vraagt, staat echter wel vast.

De initiatiefnemers zullen nader onderbouwen waarom het nodig is om alsnog erop in te zetten de situatie te veranderen.

3. Argumenten

De kern van de zaak is het volgende: er is in de afgelopen tien jaar teveel met een houding van laissez-faire en neoliberale kortzichtigheid naar deze kwestie gekeken. Lokale en landelijke overheidsinstanties maakten, vaak gedwongen door bezuinigingen, de keuze om hun data en *operations* weg te zetten bij een Amerikaanse hyperscaler, omdat op de korte termijn dit vaak goedkoper leek dan om eigen hardware te onderhouden of een kleinere aanbieder in de hand te nemen.

Door pragmatisme hebben we als Nederland iets belangrijks uit handen gegeven wat we tezamen terug moeten veroveren: grip op en eigenaarschap over onze data en onze digitale diensten. Dit is een principiële kwestie. Hieronder zetten we de belangrijkste argumenten onder elkaar.

Met verschuivende geopolitieke verhoudingen is het noodzakelijk dat de Europese Unie op eigen benen kan staan wat betreft vitale infrastructuur, en dat betreft ook belangrijke digitale diensten en gegevensopslag. In dat kader is een soevereine cloud ook een nationale veiligheidsbelang, dat ook raakt aan vraagstukken omtrent economische veiligheid, kennisvei-

[18] «Zonder hun medeweten worden de medische dossiers van miljoenen Nederlanders gekopieerd en «ergens» opgeslagen», NRC (2023), via https://www.nrc.nl/nieuws/2023/07/18/zonder-hun-toestemming-worden-de-medische-dossiers-van-miljoenen-nederlanders-gekopieerd-en-ergens-opgeslagen-a4170063

[19] «Doorgifte persoonsgegevens naar de VS», Autoriteit Persoonsgegevens, via https://www.autoriteitpersoonsgegevens.nl/themas/internationaal/doorgifte-binnen-en-buiten-de-eer/doorgifte-persoonsgegevens-naar-de-vs

ligheid en de stabiliteit en continuïteit van kritieke processen en de bijbehorende toeleveringsketens.[20]

De cloud zou daarnaast in de toekomst als pressiemiddel kunnen worden ingezet door de Verenigde Staten. Het is in zijn geheel beschouwd een onderdeel van onze kritieke infrastructuur, want we hebben een groot probleem als alles tegelijkertijd wegvalt. Er is geen serieuze fall-backoptie.

De Verenigde Staten hebben bovendien aantoonbaar andere normen dan Europa op het gebied van veiligheid en privacy. De CLOUD-Act stelt ze in staat om gegevens uit het buitenland via cloudproviders te verzamelen. Ook het voorliggende amendement Section 702 op de Amerikaanse Foreign Intelligence Surveillance Act (Fisa) geven het land verstrekkende wettelijke handvatten om inlichtingen in het buitenland in te winnen.[21] Uit onder andere de *Snowden leaks* is gebleken dat de Verenigde Staten een programma heeft om Europese bondgenoten te bespioneren. Zo heeft de NSA in het verleden een tap geplaatst op de telefoon van de Duitse bondskanselier Angela Merkel.[22] De lokalisatie van datacentra op Europees grondgebied neemt zorgen omtrent Amerikaanse dataverzameling niet weg, aangezien de ligging van het hoofdkantoor van de dienstaanbieder doorslaggevend is voor de geldende wetgeving omtrent omgang met data. Bovendien liggen de economische en politieke belangen van een Amerikaanse provider bij uitstek in de Verenigde Staten.

Teveel regie in het digitale domein bij grote tech-multinationals houden is verder onwenselijk. Zelfs als mocht blijken dat deze partijen middels Europese wetgeving goed te reguleren zijn, dan nog hebben een select aantal bedrijven *state-level capabilities* die ze in staat stellen om onze digitale leefomgeving sterk naar hun commerciële belangen te vormen. Cruciale *operations* van Nederlandse overheden en bedrijven worden nu bepaald door deze commerciële instanties.

En dat terwijl er genoeg diensten zijn die in Nederland kúnnen draaien. Met name chat- en mailverkeer en langetermijn-opslag kunnen op een veilige en gebruiksvriendelijke manier bij Nederlandse en Europese leveranciers belegd worden. Een dergelijke aanpak voor overheidsdiensten kan in ieder geval betekenen dat communicatie en databeheer onder Nederlandse en Europese regels vallen, die betere bescherming bieden en onderhevig zijn aan democratische controle.

Het veelvuldig uitbesteden van digitale infrastructuur zal leiden tot een negatieve spiraal van het wegvloeien van kennis, middelen en geld. Zolang je namelijk clouddiensten blijft uitbesteden aan partijen buiten Nederland of Europa, moet je op termijn steeds meer clouddiensten gaan uitbesteden, omdat je als land steeds minder kennis en middelen overhoudt voor je cloudinfrastructuur. Uiteindelijk leidt dit ertoe dat Nederland steeds meer digitale autonomie zal verliezen, waarbij een reëel risico is dat Nederland bijvoorbeeld zijn eigen paspoortregistraties en -systemen niet meer zelf kan bijhouden. Een vergelijkbare situatie is al ontstaan bij de Nederlandse onderzeeboten-industrie. Sterke nationale

---

[20] Zie ook: «Too late to act? Europe's quest for cloud sovereignty», Clingendael (2024), via https://www.clingendael.org/publication/too-late-act-europes-quest-cloud-sovereignty

[21] «A Backroom Deal Looms Over a High-Stakes US Surveillance Fight», Wired (2024), via https://www.wired.com/story/section-702-reform-backroom-deal /. Zie ook The US isn't just reauthorizing its surveillance laws – it's vastly expanding them», The Guardian (2024), via https://www.theguardian.com/us-news/2024/apr/16/house-fisa-government-surveillance-senate

[22] «Angela Merkel phone-bugging claims are result of Snowden leaks, MP claims», The Guardian (2013), via https://www.theguardian.com/world/2013/oct/24/angela-merkel-bugging-snowden-leaks-mp

leveranciers dragen juist bij aan het behouden en ontwikkelen van kennis in het digitale domein.

Met een gezonde voedingsbodem voor cloudleveranciers met toekomstperspectief binnen Nederland kunnen we specialistische kennis opbouwen. Het werkveld wordt nu in grote mate opgeleid tot Microsoft 365- of AWS-expert waardoor systeemkennis verloren gaat. Veel experts en betrokkenen hebben bij de initiatiefnemers aangegeven dit te observeren en zich hier grote zorgen om te maken. Het is niet voldoende dat personeel van Microsoft of Amazon in Nederland rondloopt, omdat deze bedrijven hun belangrijkste softwareontwikkelingen in Amerika uit laten voeren. In plaats daarvan moet lokaal geïnvesteerd worden in talent en moeten er strategische langetermijnbesluiten genomen worden.

Het is tot slot van groot belang dat Nederlandse waarden in Europese en internationale context geborgd zijn. Belangrijk hierbij is dat er een incompatibiliteit bestaat tussen het Europees Verdrag voor de Rechten van de Mens (EVRM) en de Grondwet van de Verenigde Staten. Zo geldt de Amerikaanse Grondwet niet voor Nederlandse burgers, maar geldt het EVRM wel voor Amerikaanse burgers. Ook is artikel 10 van het EVRM (recht op vrijheid van meningsuiting) anders dan het First Amendment *(freedom of speech)* en verschillen de opvattingen over het begrip privacy tussen Europa en Amerika. Onze positie als digitaal knooppunt en infrastructurele expertise bieden de unieke kans om toonaangevend te zijn in de standaarden die Nederland hanteert op bijvoorbeeld veiligheid en privacybescherming. Door nationale en Europese leveranciers te laten voldoen aan de door Nederland gestelde kaders en normen, worden deze in de praktijk gebracht.

Vanuit de Tweede Kamer is reeds een motie aangenomen om datadeling met partijen die niet in de EER zitten te heroverwegen en bij voorkeur voor een Europees cloudalternatief te kiezen (Motie-Rajkowski c.s.).[23] De Staatssecretaris Koninkrijksrelaties en Digitalisering heeft in de verzamelbrief Digitalisering maart 2024 in reactie daarop het volgende aangegeven: «Een belangrijk onderdeel van deze toetsing is de Data Transfer Impact Assessment (DTIA), een instrument dat de Rijksoverheid momenteel ontwikkelt om de doorgifte van gegevens zorgvuldig te beoordelen. Dit model, dat nog in de conceptfase zit, zal naar verwachting in het derde kwartaal van 2024 klaar zijn. Het bevat vragen over de beschikbaarheid van alternatieven binnen de EER.»[24]

Hoewel de initiatiefnemers benieuwd zijn naar de DTIA, vinden ze dat bij dergelijke modellen de nadruk nog teveel ligt op de individuele afwegingen van departementen bij de keuze voor een publieke leverancier en het bredere belang van strategische autonomie daarmee onvoldoende geborgd is.

4. Aanpak

De scheefgroei van het cloudlandschap is een belangrijk probleem, maar vooralsnog geen urgent probleem. Zoals eerder gezegd: de effecten zijn nog niet voelbaar. Hoewel dat niet ten gunste komt van de maatschappelijke aandacht, kunnen we hier juist wel ons voordeel mee doen. Dit maakt namelijk dat we de tijd kunnen nemen om de situatie bij te sturen zonder paniekvoetbal te spelen.

[23] Kamerstuk 26 643, nr. 975
[24] Kamerstuk 26 643, nr. 1149

De langetermijnaanpak «Wolken aan de horizon» heeft als einddoel om in 2029 over een volwassen nationale cloudinfrastructuur te beschikken. Dat geeft Nederland vijf jaar vanaf het moment van indienen van deze initiatiefnota om orde op zaken te stellen.

In het kader van strategische autonomie streven de initiatiefnemers ernaar dat er in 2029 een volwassen cloudlandschap bestaat waarin Nederlandse en Europese aanbieders een volwaardig en schaalbaar alternatief op de clouddiensten van niet-Europese hyperscalers kunnen bieden. Dit betekent niet dat de huidige dominante hyperscalers niet meer op de Nederlandse markt hun diensten mogen aanbieden, maar wel dat er een eerlijkere markt komt met meer variëteit aan aanbod.

In het kader van strategische autonomie moet voor ten minste de meest kritieke en gevoelige data en diensten de Nederlandse soevereiniteit in de cloud zijn gewaarborgd. De initiatiefnemers benadrukken dat in ieder geval communicatie, mailarchieven en data-opslag met prioriteit worden meegenomen. Om een stip op de horizon te zetten, worden er doelstellingen geformuleerd over het aandeel binnen het applicatielandschap van Nederlandse overheden dat draait op Nederlands-Europese diensten.

Nederland moet structureel investeren in een economische voedingsbodem waarin Nederlandse mkb-bedrijven op het gebied van de cloud en de digitale infrastructuur kunnen ontstaan en zich kunnen ontwikkelen, zelfstandig dan wel verenigd.

Om de Nederlandse kenniseconomie te beschermen op het gebied van de cloud en digitalisering, moet er structureel geïnvesteerd worden in generieke opleidingen gerelateerd aan cloud computing en digitale infrastructuur. Deze opleidingen dienen mensen op te leiden voor een brede inzet binnen het werkveld in plaats van hen op te leiden om te werken met specifieke (gesloten) software.

Om deze horizon te bereiken, moeten een aantal zaken in gang worden gezet. Deze worden hieronder uiteengezet. Uiteraard zijn er ook een aantal veelgehoorde en serieus te nemen argumenten *tegen* het inzetten op de bouw van een soevereine cloud, bijvoorbeeld dat het probleem niet reëel is of dat de oplossing niet haalbaar is. De initiatiefnemers hebben de belangrijkste tegenargumenten opgesomd en geven voor elk daarvan een weerlegging. Dit is opgenomen in de appendix.

Levensvatbare alternatieven

Er moeten vruchtbare omstandigheden gecreëerd worden zodat (deels) Nederlandse cloudaanbieders hun diensten van de grond kunnen krijgen. Het is onvoldoende om enkel naar Duitsland en Frankrijk te kijken, in de ideale situatie is Nederland ook volwaardig betrokken bij initiatieven.

Allereerst moet in kaart worden gebracht wat het Nederlandse, Europese of open source aanbod momenteel is, welke beperkingen in kwaliteit, betrouwbaarheid of beschikbaarheid deze clouddiensten nog hebben, hoe deze beperkingen verholpen zouden kunnen worden, en welke verdere belemmeringen er zijn om deze diensten door te laten groeien in schaal en volwassenheid. Volgens techexpert Bert Hubert zullen de huidige kwaliteitsbeperkingen hoofdzakelijk zitten in de facetten van schaalbare objectopslag (functionaliteit à la Amazon S3, Google Cloud Storage of

Azure Blob Storage), *managed Kubernetes*, *Infrastructure as Code* (IaC), *Identity and Access Management* (IAM) en *managed databases*.[25]

Vervolgens moet er door Nederland een regierol genomen worden om zo Nederlandse telecommunicatie-, hosting- en cloudaanbieders, waar nodig in samenwerking met gelijkgezinde landen zoals Duitsland, België en Scandinavische landen, in een positie te brengen om deze beperkingen te kunnen overbruggen en toekomstbestendige clouddiensten te realiseren. Hierbij wordt bij voorkeur toegewerkt naar een «Bijenkorf Cloud Megascaler» naar het model van Clingendael.[26] In de gesprekken moeten bij voorkeur ook overheidspartijen aan tafel zitten die zelf kennis hebben over het inrichten van cloudinfrastructuur, zoals ODC Noord, DICTU, DUO en RDW.

Beseft moet worden dat het cloudvraagstuk verder gaat dan enkel waar externe digitale infrastructuur beschikbaar is. De eerder genoemde verSaaSing maakt juist dat het in de cloud draaien van applicaties een belangrijke vereiste is voor veel afnemers. In de uitvoering kan inspiratie worden opgedaan uit de wijze waarop de Duitse overheid bezig is met het uitrollen van de open-source cloudoplossing Nextcloud voor haar dataopslag en *operations*. Afstappen van de commerciële cloud betekent dat in sommige gevallen alternatieven gezocht moeten worden voor de momenteel door de Nederlandse overheid gebruikte Amerikaanse *cloud-only* applicaties. Voor de veelgebruikte videovergaderapp Microsoft Teams kan bijvoorbeeld naar het open-source Jitsi als alternatief gekeken worden.

De *Important Project of Common European Interest* (IPCEI)-regeling staat toe dat overheden ingrijpen in de markt voor specifieke doeleinden. Nu er ook vanuit Nederland IPCEI-gelden zijn vrijgemaakt voor cloudtechnologie, moeten die nuttig ingezet worden. Deze en eventuele additionele gelden kunnen helpen om clouddienstverlening van de grond te krijgen waar de markt dit niet eigenstandig kan. De Nederlandse positie op cloudtechnologie kan actief bevorderd worden door deze technologie op te laten nemen in de Nationale Technologiestrategie (NTS)[27] en een prominenter thema te laten zijn in de agenda Digitale Open Strategische Autonomie (DOSA).[28]

Overheidsbeleid

De overheid moet als launching customer deze diensten afnemen en in het beginstadium actief participeren in het opzetten van de diensten. Het beleid, waaronder het Rijkscloudbeleid en het aanbestedingsbeleid, moet worden bijgesteld zodat strategische (digitale) autonomie een belangrijk uitgangspunt wordt en een clouddienst van Nederlands-Europese bodem daarmee de voorkeur geniet boven een van buiten de EU. Aanbestedingen van de Rijksoverheid mogen niet langer «toegeschreven» worden naar een Amerikaanse hyperscaler, maar moeten eerlijke, open en transparante eisen bevatten waardoor ook Nederlands-Europese partijen

---

[25] «Cloud Native, Europa, de «Bijenkorf» Megascaler», Bert Hubert (2024), via https://berthub.eu/articles/posts/cloud-native-europa/

[26] «Nederland en de EU: Zet in op cloudsoevereiniteit», Clingendael (2024), via https://www.clingendael.org/publication/nederland-en-de-eu-zet-op-cloudsoevereiniteit

[27] «De Nationale Technologiestrategie», Rijksoverheid (2024), via https://www.rijksoverheid.nl/documenten/beleidsnotas/2024/01/19/de-nationale-technologiestrategie

[28] «Agenda Digitale Open Strategische Autonomie», Rijksoverheid (2023), via https://www.rijksoverheid.nl/documenten/kamerstukken/2023/10/17/kamerbrief-aanbieden-agenda-digitale-open-strategische-autonomie-coco-5-oktober

een kans maken om een aanbestedingstraject te winnen.[29] De initiatiefnemers vinden het vreemd dat er een Nederlands overheidsonderdeel is dat vernoemd is naar private partijen en dat zich enkel richt op het leveranciersmanagement van Microsoft 365 en Azure, Google Cloud en AWS. In het buitenland wordt SLM Rijk wel eens gekscherend het «Ministerie van Microsoft» genoemd.[30] Een dergelijk overheidsonderdeel zou zich in plaats daarvan moeten richten op leveranciersmanagement van clouddiensten die de Nederlandse strategische autonomie versterken. Naast dat dit binnen de Rijksoverheid geborgd moet zijn, zou de bewindspersoon die toeziet op Digitalisering ook het gesprek aan moeten gaan met lokale overheden en vitale sectoren om hen mee te nemen in deze beweging richting een soevereine cloud.

Hierbij geldt de volgordelijkheid dat de Nederlands-Europese cloudmarkt eerst zodanig gevormd moet zijn dat dit aan de aanbodkant mogelijk is, voordat deze eisen in werking treden. Ook moet er rekening gehouden worden met de eventuele contractduur tussen de overheid en clouddienstverleners die een snelle overstap zou kunnen bemoeilijken, evenals enige *vendor lock-in*. Er zou dan sprake zijn van een *warm-up*-periode. Als harde deadline voor het uitfaseren van de niet-Nederlandse cloud wordt het jaar 2029 vastgesteld.

Overheidsdepartementen moeten werk maken van een strakke exitstrategie waardoor ze, het liefst binnen drie maanden, in staat zijn hun gehele omgeving in rap tempo te migreren tussen clouddiensten. De Havenstandaard voor platformonafhankelijke cloudinfrastructuur van de VNG, een generieke laag tussen applicaties en infrastructuur, is een mooi voorbeeld van hoe geborgd kan worden dat migratie altijd tijdig mogelijk is.[31] Een dergelijke standaard zou er ook voor bredere cloudoplossingen moeten komen.

De initiatiefnemers stellen voor dat CIO Rijk onder verantwoordelijkheid van de Staatssecretaris (of toekomstige bewindspersoon die toeziet op Digitale Zaken) eigenaarschap krijgt over de uitvoering van het langetermijnplan cloud, door in het Besluit CIO-stelsel Rijksdienst op te nemen dat deze verantwoordelijk is voor de borging van strategische (digitale) autonomie op de lange termijn. Dit uiteraard in nauwe samenwerking met het Ministerie van Economische Zaken en Klimaat, vanwege de raakvlakken met de agenda's DOSA en NTS.

Strategische kennisborging

De overheid moet verder in gesprek gaan met technische opleidingsinstituten om gezamenlijk de software en applicaties binnen dit curriculum zo open mogelijk in te richten. Al vele decennia zien we een sterke lobby van grote internationale techbedrijven bij opleidingen om gebruik te maken van hun specifieke en gesloten software. Dit kan er uiteindelijk toe leiden dat het gros van het werkveld alleen nog bekend is met de applicaties van deze bedrijven, waardoor er een grote mate van afhankelijkheid gecreëerd wordt. Daarom dienen de software en applicaties binnen technische opleidingen zoveel mogelijk gebaseerd te zijn op open software en standaarden.

---

[29] Zie voor voorbeelden van toeschrijven naar Amerikaanse hyperscalers het Zwartboek Aanbestedingen ICT, via https://mastodon.nl/@zwartboekaanbesteden

[30] «De hele overheid naar de cloud? Dat is een politiek besluit.», Bert Hubert (2024), via https://berthub.eu/articles/posts/de-hele-overheid-naar-de-cloud-dat-is-een-politiek-besluit/

[31] https://haven.commonground.nl/

De overheid dient zelf zo veel mogelijk over te stappen op het gebruik van op open standaarden gebaseerde Nederlandse of Europese software en applicaties. Nederlandse overheden zijn namelijk te afhankelijk geworden van de software en applicaties van grote internationale bedrijven. Dit betekent bijvoorbeeld dat de overheid geen alternatieven heeft in de situatie dat deze bedrijven vervelende voorwaarden stellen op het gebied van data-gebruik en overige clouddienstverlening. Dat is extra onwenselijk in combinatie met het eerder benoemde aspect van het wegvloeien van kennis en middelen door deze steeds groter wordende afhankelijkheid. Hierdoor moeten er namelijk steeds gevoeligere systemen aan deze bedrijven worden overgedragen.

Datacentra

Er is tot slot regie nodig op datacentrumcapaciteit zodat schaalbaarheid voldoende geborgd is. Het wordt de uitdaging om een volwassen Nederlandse cloudlandschap te bewerkstelligen, waarbij gezien de bredere afwegingen rondom ruimtelijke ordening en netcapaciteit zo min mogelijk datacentra bijgebouwd moeten worden. De instrumenten om op de inzetbaarheid te sturen moeten duidelijk zijn en op het juiste moment ingezet worden. Hieraan moet in de Nota Ruimte expliciet aandacht worden besteed.

Het is aan te raden dat de overheid ook een eenduidige meerjarenstrategie voor de ontwikkeling van nieuwe datacenters opstelt. Waar er in de samenleving begrijpelijkerwijs grote weerstand tegen mega-datacentra is, kan met strategisch geplaatste kleinere datacentra voldoende capaciteit voor eigen gebruik worden gerealiseerd en kunnen de reststromen zoals warmte in bijvoorbeeld woonwijken effectief worden hergebruikt.

5. Aanbevelingen

De initiatiefnemers komen tot de volgende aanbevelingen:

1. **Pak de regie over digitale soevereiniteit.** De versnippering over verschillende departementen, dienstverleners en afdelingen leidt ertoe dat strategische autonomie niet voldoende wordt bewaakt bij keuzes over Rijks-ICT. De Kamer is aan zet om richting te geven aan keuzes over digitale infrastructuur. Dit vergt een beter inzicht op de staat van de ICT bij de overheid en een stip aan de horizon waar men naartoe werkt.
    - **Richt een Rijksmaildienst en een Rijkschatdienst op.** Enkele departementen binnen de overheid, zoals Algemene Zaken en Defensie, beheren hun eigen communicatiekanalen. Schaal deze voorbeelden op tot één algemene Rijksmaildienst, waar op termijn breed gebruik van wordt gemaakt zodat communicatie en de bijbehorende archieven in eigen beheer zijn. Met een betrouwbaar alternatief kan e-mailcommunicatie binnen en met de Rijksoverheid snel uit de publieke cloud verdwijnen en in eigen beheer komen. Neem parallel aan de ontwikkeling van de maildienst ook de uitkomsten mee van de verkenning naar een eigen chatapplicatie voor Ministers en ambtenaren (motie-Palmen)[32] om ook te komen tot een soevereine Rijkschatdienst.
    - **Stel normen.** Normeer het minimumaandeel cloudopslagdiensten en cloudapplicaties dat door Nederlands-Europese leveranciers aan de Rijksoverheid wordt aangeboden op 30% voor 2029.
    - **Centraliseer de kennis.** Er moet een centraal overzicht komen van het applicatielandschap van de brede Rijksoverheid, inclusief uitvoeringsorganisaties, zodat de Kamer de vinger aan de pols kan

[32] Kamerstuk 36 410 III, nr. 11

houden over de eigen ICT. Vergroot, in lijn met de I-strategie Rijk 2021–2025, de transparantie en het inzicht in informatievoorziening, specifiek daar waar het betreft de licenties en kosten van (cloud)infrastructuur. Onderzoek of de huidige departementale ICT-budgetten toereikend zullen zijn om de benodigde soevereine clouddiensten te kunnen afnemen. Zo niet, breng in kaart welk financieel tekort er zou ontstaan en rapporteer dit aan de Tweede Kamer.
    - **Verkrijg inzicht in cloudmigraties.** Onderzoek waarom overheidsinstanties genegen zijn te kiezen voor een commerciële Amerikaanse cloudoplossing voor hun dataopslag en *operations*, ondanks de tegenstrijdigheid van deze beslissingen met Nederlandse ambities op het gebied van autonomie. Neem in het onderzoek mee welke specifieke besluiten, uitspraken en onderzoeken hebben bijgedragen aan de snelle migratie naar buitenlandse leveranciers.
    - **Trek nauw op met medeoverheden.** Ook op decentraal niveau is er sprake van een vergaande afhankelijkheid van buitenlandse techbedrijven. Ga in gesprek met het Interprovinciaal Overleg (IPO) en de Vereniging van Nederlandse Gemeenten (VNG) om inzichtelijk te maken strategische (digitale) autonomie versterkt kan worden op lokaal niveau.
    - **Stimuleer autonomie bij vitale bedrijven.** Ga in gesprek met NIS2-doelgroepen buiten de overheid, zijnde bedrijven in de vitale-sector, om te bespreken hoe strategische (digitale) autonomie bij deze doelgroepen versterkt kan worden.
    - **Reserveer ruimte voor de nodige datacapaciteit.** Besteed expliciet aandacht aan datacentrumcapaciteit voor Nederlandse cloudoplossingen in de Nota Ruimte. Datacentra op Nederlands grondgebied zijn duurzaam en komen ten goede van de strategische autonomie.
2. **Zorg voor een gezonde voedingsbodem en eerlijke concurrentie.** De Rijksoverheid is de grootste ICT-afnemer van Nederland en heeft een enorme marktmacht die onvoldoende wordt benut. Aanbestedingen bij Nederlandse bedrijven moeten zorgen voor een gezonde voedingsbodem voor de binnenlandse techindustrie. Maak als overheid afspraken om als *launching customer* op te treden voor een Nederlands-Europese clouddiensten.
    - **Kom de Nederlandse cloudsector tegemoet.** Breng in kaart op welke onderdelen Nederlandse cloudaanbieders momenteel tekortschieten om een adequate clouddienstverlening aan te kunnen bieden aan grote overheidsdepartementen of bedrijven.
    - **Leg duurzame contacten en stimuleer samenwerking.** Faciliteer als overheid gesprekken tussen Nederlandse telecommunicatie-, hosting- en cloudaanbieders, Overheidsdatacenters (ODCs) en spelers in bijvoorbeeld Duitsland, België of Scandinavische landen om te komen tot een gezamenlijke volwaardige cloudoplossing, zoals de «Bijenkorf Cloud Megascaler» naar het model van Clingendael.
    - **Hef het «Ministerie van Microsoft» op.** Het rijksdepartement SLM Microsoft, Google Cloud en Amazon Web Services bevoordeelt in de huidige vorm buitenlandse techgiganten. Het is een symptoom van de doorgeslagen afhankelijkheid van technologische grootmachten, wederom mogelijk gemaakt door het gebrek aan samenhang tussen afnemende organisaties. Breng de aanwezige expertise onder in een departement verantwoordelijk voor strategisch leveranciersmanagement voor cloudomgevingen die de Nederlandse strategische autonomie juist versterken.
    - **Hervorm het aanbestedingsbeleid van de Rijksoverheid.** Niet langer mag door departementen naar leveranciers «toegeschre-

ven» worden en terminologie specifiek voor aanbieders als Microsoft 365 of AWS moet uit aanbestedingen blijven. In plaats daarvan moeten er eerlijke, transparante aanbestedingseisen komen waarbij ook alternatieve aanbieders mee kunnen doen.
    - **Licht de huidige voorrangspositie van publieke cloudleveranciers goed door.** Laat de Audit Dienst Rijk (ADR) actief onderzoeken of departementen hun aanbestedingen naar Amerikaanse hyperscalers «toeschrijven», breng de ADR in stelling om op te treden als dit het geval is en laat de ADR hier in de toekomst blijvend toezicht op houden.
    - **Ondersteun nationale partijen in aanbestedingen.** Speel een faciliterende rol in het partijen op weg helpen om te kunnen voldoen aan aanbestedingen, door proactief met aanbieders samen te werken naar Zweeds voorbeeld.
    - **Laat Europese financiering ten goede komen van de Nederlandse industrie.** Zet een gedeelte van de aan Nederland toegekende € 71,2 mln *Important Project of Common European Interest Cloud Infrastructure and Services* (IPCEI-CIS)-gelden strategisch in om deze initiatieven te versterken en actief te participeren. Help organisaties om het budget uit het *Digital Europe Programma* optimaal te benutten bij de keuze voor Nederlands-Europese leveranciers.
    - **Stimuleer cloudtechnologie in bestaande trajecten.** Neem cloudtechnologie bijvoorbeeld op als sleuteltechnologie in de Nationale Technologiestrategie (NTS).
    - **Maak het onderwijs technologieneutraal.** ICT'ers verdienen een opleiding tot meer dan een Microsoft- of Amazon-expert. Stimuleer technische opleidingsinstituten om tot een curriculum gericht op open standaarden voor software en applicaties te komen. Sluit Nederlandse cloudpartijen aan bij bestaande publiek-private samenwerkingen die gericht zijn op ICT-opleidingen.
3. **Handhaaf het eigen beleid.** Het Nederlandse beleid maakt van autonomie en privacy een hoofdpunt. Een gebrek aan regie maakt dit beleid echter boterzacht, waardoor het over de breedte van het Rijk niet wordt nageleefd. Het bevorderen van de Nederlandse autonomie wordt een harde eis en de verantwoordelijkheid over dit punt wordt duidelijker belegd.
    - **Maak van strategische autonomie een doel op zich.** Neem in de herziening van het Rijks Cloudbeleid op dat strategische autonomie een belangrijk uitgangspunt is voor de overheid als geheel. Stel daarbij vast dat soevereine cloud een voorwaardelijkheid is voor o.a. kritieke en gevoelige overheidsonderdelen en neem 2029 als harde deadline voor de uitfasering van niet-Nederlandse cloudaanbieders. Dit kan op getrapte wijze, waarin diensten met een lage eisendrempel als eerst worden omgeschakeld zodat Nederlandse partijen via die weg hun entree maken.
    - **Veranker strategische autonomie in aanhangige wetgeving.** Neem in de herziening van de Baseline Informatiebeveiliging Overheid (BIO) op dat strategische (digitale) autonomie en soevereiniteit in de cloud voor BBN2 een vereiste is.
    - **Stel de CIO Rijk verantwoordelijk.** Door een gebrekkige rolverdeling voelt niemand zich écht verantwoordelijk voor het handhaven van de strategische autonomie. Kom met een wijziging van het Besluit CIO-stelsel Rijksdienst zodanig dat de CIO Rijk in zijn taakstelling verantwoordelijk wordt voor het waarborgen van de Nederlandse langetermijnbelangen op strategische (digitale) autonomie binnen de Rijksoverheid. Door de verantwoordelijkheid voor besluiten over (grote) ICT-aanbestedingen te beleggen bij de

CIO Rijk, monitort deze de rijksbrede langetermijndoelen op het gebied van strategische autonomie.

- **Maak duidelijk hoe bestaande kaders worden nageleefd.** Er bestaat een implementatiekader risicoafweging cloudgebruik.[33] Het is bij individuele migraties nu onduidelijk hoe invulling wordt gegeven aan deze regels en welke punten leidend zijn bij het maken van een afweging. De onderbouwing bij keuzes over ICT-migraties worden transparant en centraal bijgehouden, zodat beslissingen over de digitale infrastructuur van de overheid controleerbaar zijn.
- **Stel vlotte exitstrategieën als randvoorwaarde.** Verplicht NIS2-doelgroepen (overheid en vitale sectoren) om een exitstrategie en bijbehorende budgetten te hebben voor hun clouddiensten, waarbij gehanteerd moet worden dat een migratietijd maximaal drie maanden mag duren. Stimuleer gebruik van een platformonafhankelijke standaard voor cloudinfrastructuur met het «pas-toe-of-leg-uit»-principe, analoog met de Haven-standaard van de VNG. Dit om *vendor lock-in* te voorkomen.
- **Maak open standaarden de norm.** Neem in afstemming met Forum Standaardisatie in het digitaliseringsbeleid van de Rijksoverheid op dat open standaarden voor software en applicaties de norm worden. Zo worden ICT-diensten schaalbaar en kan er beter tussen departementen en overheden worden samengewerkt.

6. Financieel kader

Deze initiatiefnota voorziet geen verschuivingen op de begroting.

De initiatiefnemers gaan uit van een kostenplaat vergelijkbaar met de huidige. Er is echter zeer beperkt inzicht in de huidige cijfers omtrent door departementen afgenomen clouddiensten en onderhoud van eigen infrastructuur binnen de overheid, evenals of een Nederlands-Europese cloudaanbieder voor een vergelijkbaar bedrag de benodigde alternatieve diensten zou kunnen leveren. Mocht de afname van soevereine clouddiensten echter significant duurder blijken, dan moet de Tweede Kamer hierover door de regering geïnformeerd worden en moet besloten worden hoe het tekort gefinancierd kan worden.

Overheidsinvesteringen in de vorming van een Nederlands cloudlandschap kunnen gefinancierd worden uit de reeds gereserveerde € 71,2 mln van IPCEI-CIS. Er wordt zo veel mogelijk met Europese subsidieprogramma's gericht op het versterken van infrastructuur, autonomie en industrie.

7. Beslispunt

De Kamer wordt gevraagd om in te stemmen met de aanbevelingen en de regering te verzoeken deze over te nemen.

Six Dijkstra
Kathmann

[33] Implementatiekader risicoafweging cloudgebruik | Rapport | Rijksoverheid.nl

8. Bronvermelding en raadpleging

De volgende experts en belanghebbenden zijn geraadpleegd bij het opstellen van deze initiatiefnota:
- Bert Hubert, persoonlijke titel
- Ron Roozendaal, persoonlijke titel
- Brenno de Winter, persoonlijke titel
- Dr. Corinne Cath, TU Delft
- Maaike Okano-Heijmans, Instituut Clingendael
- Alexandre Ferreira Gomes, Instituut Clingendael
- Ludo Baauw, Intermax
- Simon Besteman, Dutch Cloud Community
- Wido den Hollander, Your.Online

9. Appendix

Er zijn een aantal veelgehoorde tegenargumenten waarom het niet verstandig zou zijn strategische autonomie in het clouddomein na te streven. De initiatiefnemers zetten hieronder de prominentste op een rij en geven een weerlegging.

1. Het haalbaarheidsargument
«Nederlandse cloudaanbieders kunnen nooit de schaalbaarheid en functionaliteit bieden die hyperscalers bieden.»

Nederlandse en Europese leveranciers zullen op korte termijn nog niet in staat zijn om de buitenlandse cloudaanbieders volwaardig te vervangen. Dit betekent ook dat als Nederland hier nu niet in investeert, we ook op de lange termijn afhankelijk blijven van *big tech* hyperscalers. Juist daarom vinden de initiatiefnemers het van belang om de voedingsbodem voor nationale en Europese alternatieven te verbeteren, zodat er op termijn voldoende kennis, kunde en schaal wordt opgebouwd om steeds meer diensten dichterbij huis te kunnen vestigen. Voor diensten met bijzondere specificaties die op maat moeten worden ontwikkeld, zoals paspoortregistraties of vitale infrastructuur, kunnen nationale en Europese partijen dan ook in de toekomst een uitkomst blijven bieden. Bovendien heeft de Nederland juist aangetoond dat ze een aantal zaken al wél kan. Zie bijvoorbeeld de platforms die ontwikkeld en beheerd worden door partijen als ODC Noord, DICTU, RDW en DUO. Ook tijdens de coronacrisis heeft de overheid, na enige opstartproblemen, voor miljoenen burgers ondersteunende ICT-faciliteiten kunnen bieden.

2. Het «boot gemist»-argument
«We lopen al teveel achter op de hyperscalers om hun niveau ooit bij te kunnen benen.»

Achterlopen zou nooit een reden moeten zijn om af te haken. We meten juist tegengewicht bieden, anders zal de kennis van cloudinfrastructuur en -diensten in de toekomst helemaal uit Nederland en Europa verdwijnen. Daarom moet Nederland brede kennis behouden over clouddiensten, waarbij dit niet alleen gaat over bekend zijn met de Microsoft, Google en Amazon-omgevingen. Daardoor zullen we namelijk de afhankelijkheid in stand houden. Dus zelfs als volwaardige alternatieven op de hyperscalers uitblijven, moet Nederland lokale alternatieven, zeker voor bijzondere en kritische infrastructuur, op peil brengen.

3. Het cybersecurity-argument
«De cloudpakketten van hyperscalers bieden betere digitale bescherming dan bedrijven zelf zouden kunnen realiseren wanneer ze data in eigen beheer hebben.»

De razendsnelle toename en de complexiteit van cyberveiligheidsrisico's maken het eigen beheer van data en digitale diensten steeds minder aantrekkelijk. Het is echter veel te gemakkelijk om te zeggen dat commerciële clouddiensten een totaaloplossing bieden. Ten eerste, serieuze cyberveiligheidsrisico's hangen meestal af van menselijk handelen. Juist het idee dat commerciële clouddiensten waterdicht zijn kan leiden tot schijnveiligheid en het bewustzijn verminderen. Ten tweede, ook grote Amerikaanse aanbieders kunnen kwetsbaarheden bevatten, zoals kritieke *zero days*. Dit hebben we in de afgelopen jaren ook voldoende gezien. De impact van deze digitale achilleshielen is bij wereldwijde aanbieders vele malen groter dan bij kleinere partijen. Bovendien vormen deze partijen een aantrekkelijk strategisch doelwit voor statelijke cyberactoren, zoals de Chinese hackersgroep Storm-0558 die in 2023 clouddiensten van Microsoft succesvol heeft aangevallen en tienduizenden overheidsmails heeft buitgemaakt. Het Amerikaanse Department of Homeland Security identificeerde naar aanleiding van dit incident «een reeks operationele en strategische keuzes van Microsoft die tezamen wezen op een bedrijfscultuur waarin investeringen in bedrijfsbeveiliging en rigoureus risicomanagement geen prioriteit kregen,wat strijdig is met de centrale positie van het bedrijf in het technologie-ecosysteem en het niveau van vertrouwen dat klanten in het bedrijf stellen om hun gegevens en bedrijfsvoering te beschermen».[34] Ten slotte willen de initiatiefnemers benadrukken dat de afhankelijkheid van buitenlandse clouddiensten en de daarmee verdwijnende kennis van de eigen systemen op zichzelf ook een veiligheidsrisico is.

4. Het encryptie-argument
«Via DPIA's en andere assessments kan al worden vastgesteld dat hyperscalers hun klanten middels encryptie voldoende privacy bieden.»

Door cloudaanbieders kunnen cryptografische maatregelen zoals *confidential computing* getroffen worden om klantdata te beveiligen op een manier dat ook de aanbieder zelf technisch niet bij deze data kan. Deze diensten worden vaak aangeboden als «cloud for sovereignty»-pakketten. Hier moet wel de kanttekening bij geplaatst worden dat ook dit systeem nooit waterdicht is, omdat het uiteindelijk de aanbieder is die de maatregel implementeert, en Amerikaanse aanbieders onder Amerikaanse wetgeving gedwongen kunnen worden om heimelijk dit soort maatregelen ongedaan te maken.[35] Omdat de geopolitieke situatie een hoge mate van onvoorspelbaarheid kent, is lastig vast te stellen hoe robuust de waarborgen van Amerikaanse aanbieders zullen blijken. Door een te grote afhankelijkheid in te bouwen van enkele niet-Europese leveranciers, ontnemen we onszelf ook de mogelijkheid om over te stappen op een alternatief, mocht dit onverwacht toch nodig zijn. Dit kan je alleen bereiken door alternatieve diensten te hebben. Bovendien zijn de hyperscalers van een dusdanig grote omvang dat boetes bij niet-naleving van privacywetgeving niet voldoende toereikend zijn. Ten slotte verengt dit argument het vraagstuk van digitale strategische autonomie onterecht tot een kwestie van vertrouwelijkheid, waarbij voorbij gegaan wordt aan

[34] «Cyber Safety Review Board Releases Report on Microsoft Online Exchange Incident from Summer 2023», Department of Homeland Security (2024), via https://www.dhs.gov/news/2024/04/02/cyber-safety-review-board-releases-report-microsoft-online-exchange-incident-summer
[35] «Bijeenkomst Cloud en Digitale Open Strategische Autonomie», Bert Hubert (2024), via https://berthub.eu/articles/posts/bzk-ezk-overheid-cloud-europa/

de cruciale aspecten onafhankelijkheid (c.q. als land zelf keuzes kunnen maken), zelfstandigheid en kennisborging.[36]

5. Het lokalisatie-argument
«Er is al wettelijk bepaald dat data fysiek in Nederland wordt opgeslagen. Dat is waarborg voldoende.»

Het opslaan van Europese data op eigen grondgebied biedt juridisch gezien onvoldoende waarborgen dat deze data niet inzichtelijk zijn voor niet-Europese mogendheden. De eerder genoemde Amerikaanse CLOUD-Act biedt de Amerikaanse regering namelijk al verstrekkende bevoegdheden, ook voor data die is opgeslagen op Europees grondgebied. Het in de Verenigde Staten voorliggende amendement Section 702 op de Amerikaanse Foreign Intelligence Surveillance Act (Fisa) geeft het land ook verstrekkende wettelijke handvatten om inlichtingen in het buitenland in te winnen. Bovendien kan blijken dat de aanbieder als gevolg van capaciteitsissues ook buiten Nederland data opslaat. Dit is niet altijd volledig transparant voor de gebruiker. Ook hier geldt dat dit argument het vraagstuk van digitale strategische autonomie onterecht tot een kwestie van vertrouwelijkheid verengt.

6. Het verdragsargument
«Er zijn verdragen tussen Europa en de Verenigde Staten die garanderen dat de VS niet zomaar bij Europese data komt.»

Ook hier kan wederom worden aangegeven dat de verstrekkende bevoegdheden van de Verenigde Staten vanuit de CLOUD-act en het voorliggende amendement Section 702 op de Fisa niet moet worden onderschat. Bovendien moet ook worden benoemd dat de economische en politieke belangen van niet-Europese leveranciers waarschijnlijk niet altijd primair op de privacy van Europese burgers gericht zijn. De geldende verdragen laten namelijk onverlet dat de Verenigde Staten ook buiten verdragen om druk kan uitoefenen op de Europese markt wegens haar dominantie.[37] De VS is eerder bereid én in staat gebleken om Europese belangen indirect aan te tasten, door sancties op te leggen die nadelig zijn voor ons continent. De onvoorspelbaarheid van het Amerikaanse politieke leiderschap moet extra aanzetten tot stevige Europese alternatieven.

7. Het «niets te verbergen»-argument
«Ik heb als burger geen geheimen. Het maakt mij niet uit wie mijn data inziet.»

Ten eerste heeft iedereen iets te verbergen. Het is van groot belang dat niet alleen burgers zelf zorgvuldig met hun gegevens omgaan, maar ook dat overheden en bedrijven hier verantwoord mee omgaan. Het belang hiervan komt voort uit de noodzaak om zowel privacygevoelige informatie van burgers af te schermen (denk aan vertrouwelijkheid van medische gegevens), als om burgers te beschermen tegen identiteitsfraude (denk aan vertrouwelijkheid van het BSN). Het is bovendien met een goede reden dat doxing, het online delen van persoonsgegevens met als doel onder andere intimidatie of activisme, strafbaar is. Mensen kunnen er ongelofelijk veel last aan ondervinden als hun persoonsgegevens lekken en het is bovendien een nagenoeg onomkeerbare handeling. Ten tweede

---

[36] «Hoe soeverein wil je zijn?», Bert Hubert (2024), via https://berthub.eu/tmp/hoe-soeverein-wil-je-zijn.html

[37] «2020: The year of economic coercion under Trump», European Council on Foreign Relations (2020), via https://ecfr.eu/article/commentary_2020_the_year_of_economic_coercion_under_trump

is het soeverein kunnen borgen van de vertrouwelijkheid van data niet alleen een kwestie van privacybescherming voor burgers, maar ook een groter vraagstuk van nationale veiligheid. De overheid draagt verantwoordelijkheid voor een grote hoeveelheid online gegevens én *operations*, die als geheel van belang zijn voor het functioneren van de overheid, de Nederlandse economische en kennisveiligheid, en kritieke processen in de samenleving.

8. Het Europa-argument
«In de EU doen andere landen voldoende via bijvoorbeeld GAIA-X, dus we hoeven als Nederland niet een te actieve rol te spelen.»

Nederland is trots op haar rol binnen Europa en op haar rol als internationaal digitaal knooppunt. Deze positie heeft Nederland natuurlijk niet zomaar gekregen. Als we ons hier niet voor blijven inzetten zal deze belangrijke rol vervallen. Daarom past het Nederland om toonaangevend te zijn op het gebied van digitalisering op basis van Nederlands-Europese waarden. Door de voedingsbodem voor nationale cloudleveranciers te verbeteren, stelt Nederland zichzelf daarbij in staat om invulling te geven aan haar ambitie op dit gebied. Dit versterkt bovendien de digitale kennis- en diensteneconomie waar Nederland bekend om staat.

9. Het francoscepsis-argument
«Met een Europese cloud worden we afhankelijk een land als Frankrijk, dat we ook niet blind kunnen vertrouwen.»

Het is inderdaad onwenselijk dat blind gevaren wordt op diensten uit andere EU-landen waarbij Nederland zelf niet betrokken is. Voor dataopslag en digitale diensten is het van belang dat Nederland zelf kennis en capaciteiten in huis heeft. Derhalve dient de soevereine cloud een sterke Nederlandse component te hebben, zodanig dat Nederland een duidelijke mate van strategische autonomie over de diensten heeft. Het aandeel uit Nederland hoeft niet volledig te zijn, maar er moet tenminste sprake zijn van een gelijkwaardig partnerschap tussen Nederlandse partijen en die uit andere landen.

10. Het datacentrumargument
«We hebben niet genoeg datacentrumcapaciteit om zelf onze data te hosten.»

Datacentra maken een razendsnelle efficiëntie- en verduurzamingsslag door. Het is van groot belang om een eenduidige nationale visie op te stellen over de waardevolle plaatsing van datacentra in de geringe ruimte die wij in Nederland beschikbaar hebben. Daarin bestaat een wezenlijk verschil tussen bijvoorbeeld een datacentrum van een big tech-bedrijf gebouwd voor eigen gebruik en een datacentrum dat gedragen en behuisd wordt door Nederlands-Europese belanghebbenden. Het is voorstelbaar dat de al beschikbare ruimte efficiënter gebruikt zal worden, maar de vraag naar serverruimte neemt eveneens toe. Hiervoor moet de samenwerking met Europese bondgenoten worden opgezocht om datacentra ruimtelijk inpasbaar te houden en ook te laten passen in het Nederlandse waardenraamwerk.