Ministerie van Economische Zaken

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Prinses Irenestraat 6
2595 BD DEN HAAG

Datum 17 januari 2025
Betreft Initiatiefnota ‘Wolken aan de horizon’

Geachte Voorzitter,

Op 18 juni 2024 heeft het kabinet de Initiatiefnota 'Wolken aan de horizon' van de leden Six Dijkstra (NSC) en Kathmann (GL-PvdA) ontvangen. Allereerst willen we de opstellers van de initiatiefnota bedanken dat zij aandacht vragen en aanbevelingen doen voor dit belangrijke onderwerp. We delen de stelling dat essentiële infrastructuur veel meer is dan de snelwegen en bruggen die ons verbinden. Tegenwoordig spelen de digitale snelwegen waarover data bewegen en de omgang met en opslag van gevoelige gegevens van Nederlandse burgers en bedrijven een cruciale rol in onze economie en samenleving.

Middels deze brief ontvangt u een reactie op de initiatiefnota van het kabinet. De initiatiefnota roept op tot het terugdringen en voorkomen van afhankelijkheden van grote cloudaanbieders bij de overheid. Cloud is in korte tijd een onmisbare bouwsteen in onze digitale economie en samenleving geworden, met grote voordelen op het vlak van gebruiksgemak en efficiëntie voor afnemende organisaties. Brede adoptie van de technologie kent dan ook economische en maatschappelijke baten, maar de grote mate van afhankelijkheid van een klein aantal cloudaanbieders zorgt tegelijkertijd voor risico’s op het vlak van o.a. concurrentiepositie, digitale open strategische autonomie en continuïteit.

Ook voor de Rijksoverheid is cloud inmiddels van groot belang, zoals ook is onderschreven in het Rijksbreed cloudbeleid uit 2022. Naar aanleiding van de huidige ontwikkelingen zal er een herzien cloudbeleid opgesteld worden. Daarnaast zullen de (uitkomsten van de) onderzoeken van de Auditdienst Rijk (ADR) en de Algemene Rekenkamer (AR) meegenomen worden in het herziene cloudbeleid.[1] Cloud is tevens een thema in de Nederlandse Digitaliseringstrategie (NDS).

In het herziene cloudbeleid zal het gebruik van public cloud door de Rijksoverheid aangescherpt worden, met inbegrip van kaders voor digitale autonomie. Dit heeft als consequentie dat er mogelijk minder digitale diensten van de Rijksoverheid in de public cloud kunnen worden ontwikkeld, afhankelijk van de te beschermen belangen bij desbetreffende diensten. Voor dergelijke diensten zal dan ook onderzocht moeten worden of er een soevereine overheidscloud opgezet kan worden.

[1] Bevindingen onderzoeksopdracht 'Evaluatie public cloudbeleid Rijksoverheid' | Rapport | Rijksoverheid.nl

We presenteren aan het eind van deze kabinetsreactie een geïntegreerde aanpak voor het stimuleren van verantwoord gebruik van clouddienstverlening door organisaties in Nederland. Deze aanpak bestaat uit een set beleidsacties aanvullend op de huidige inzet, waarmee we de ambities op het vlak van het verminderen van afhankelijkheden meer kracht bij zetten. Ze schetsen actielijnen voor het kabinet op Europees en nationaal niveau, gericht op het verbeteren van de positie van zowel Nederlandse cloudgebruikers als -aanbieders.

De probleemstellingen en aanbevelingen in de initiatiefnota zijn breed en diepgaand. Daarom is het belangrijk om eerst aandacht te besteden aan de problemen en het huidige beleid voordat we de contouren schetsen van een geïntegreerde aanvullende aanpak voor het gebruik van public cloud. In deze kabinetsreactie wordt toegewerkt naar de geïntegreerde aanpak door allereerst in te gaan op enkele definitiekwesties. Aansluitend zal dieper op de hierboven aangestipte risico's en problemen op de cloudmarkt worden ingegaan, zoals ook geschetst door de initiatiefnemers. Daarna volgt een beschrijving van de huidige beleidsinzet op deze problematiek. Tot slot worden de contouren van een aanvullende aanpak geschetst, en in de bijlage reageren we op alle individuele aanbevelingen uit de initiatiefnota.

Deze brief bouwt voort op verschillende eerdere Kamerstukken die de afgelopen tijd naar de kamer zijn gestuurd, namelijk de kabinetsreactie op de policy brief van Instituut Clingendael "Too late to act – Europe's quest for cloud sovereignty", de Kamerbrief met betrekking tot de evaluatie van het Rijksbreed Cloudbeleid en de Kamerbrief met betrekking tot de voorgenomen en geplande migraties van overheids-ICT naar het buitenland.[2]

Definities
In de initiatiefnota worden de begrippen soevereiniteit en autonomie op een andere wijze gebruikt dan dat het kabinet deze hanteert. Hieronder wordt kort aangegeven hoe het kabinet de begrippen 'soevereiniteit' en 'autonomie' interpreteert binnen het digitale domein, om vervolgens in te gaan op het binnen de rijksoverheid gehanteerde begrip '(digitale) open strategische autonomie'.[3]

Soevereiniteit
Soevereiniteit is een politiek begrip waarvoor geen eenduidige algemeen geaccepteerde definitie bestaat. Soevereiniteit wordt algemeen geassocieerd met territorialiteit, grondgebied (inclusief natuurlijke hulpbronnen), jurisdictie, een bevolking en gezag met zowel interne als externe erkenning (legitimiteit). Interne legitimiteit betreft de effectiviteit van de staat als uitvoerder van overheidstaken (bijvoorbeeld het beheren en controleren van het verkiezingsproces en de strafrechtketen) en ook de erkenning door burgers van de staat (het hebben van vertrouwen in de rechtstaat). Externe legitimiteit betreft in eerste instantie vooral de erkenning door buitenlandse staten en de handelingsautonomie van een staat jegens vreemde staten.[4]

[2] Kamerstuk 26643, nr. 1220; Kamerstuk 26643 nr. 1225; Kamerstuk 26643 nr. 1243
[3] Agenda Digitale Open Strategische Autonomie (overheid.nl)
[4] Rebo- Reflecties over Digitale Soevereiniteit - FINAL 1 december 2020.pdf (uu.nl)

In de context van cloud definieert het Instituut Clingendael de term ‘soevereiniteit’ in de policy brief ‘Too late to act? Europe’s quest for cloud sovereignty’ ook wel als “sovereignty, or ownership and the ability to manage the system and the data that run on it.”[5] Vanwege het ontbreken van een rijksbreed afgestemde definitie van de term soevereiniteit in het kader van cloud hanteert het kabinet in voorliggende kabinetsreactie de term autonomie in plaats van soevereiniteit.

Autonomie
In de initiatiefnota wordt de term autonomie meerdere keren gebruikt, waardoor het van belang is om helder te hebben waar dit begrip op ziet en wat de relatie is met het begrip soevereiniteit. In dit kader wordt vaak de term strategische autonomie genoemd: “het vermogen om autonoom te kunnen beslissen en handelen aangaande essentiële aspecten van de langere-termijn toekomst in economie, maatschappij en democratie.”[6]

Vanwege het belang van een open economie en van internationale partnerschappen voor het waarborgen van onze belangen wordt er in Europees verband, mede op aandringen van Nederland, gesproken over ‘open’ strategische autonomie. Voor Nederland gaat het versterken van de weerbaarheid van de EU hand in hand met – en niet ten koste van – het behoud van een open economie.

Het kabinet hanteert daarom de volgende definitie, zoals beschreven in de Kamerbrief[7], omtrent Open Strategische Autonomie (OSA): *het vermogen van de EU om als mondiale speler, in samenwerking met internationale partners, op basis van eigen inzichten en keuzes publieke belangen te borgen en weerbaar te zijn in een onderling verbonden wereld.* Die belangen zijn onder meer de nationale veiligheid, het lange termijn verdienvermogen, het vinden van oplossingen voor maatschappelijke uitdagingen, en de borging van de democratische rechtsstaat en fundamentele waarden.

Met de agenda Digitale Open Strategische Autonomie (DOSA)[8] heeft het destijds demissionaire kabinet in een integraal beleidskader voor open strategische autonomie binnen het digitale domein voorzien. In lijn met de Kamerbrief OSA en kabinetsbrede aanpak strategische afhankelijkheden wil Nederland hiermee een gebalanceerd narratief uitdragen op Europees en internationaal niveau.[9] We willen open zijn naar de buitenwereld waar het kan, en beschermend waar dat moet, ook in het digitale domein. In deze reactie ziet het kabinet de bovenstaande definities van OSA en DOSA als leidend, waar het refereert aan gebruik van de term autonomie in de initiatiefnota.

[5] Policy_brief_Cloud_sovereignty.pdf (clingendael.org)
[6] Rebo- Reflecties over Digitale Soevereiniteit - FINAL 1 december 2020.pdf (uu.nl)
[7] Staat van de Europese Unie 2022 | Tweede Kamer der Staten-Generaal
[8] Staat van de Europese Unie 2023 | Tweede Kamer der Staten-Generaal
[9] Kamerstuk 30 821, nr. 181

Public, private, multi- en hybride 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 domein heeft «public» een andere betekenis dan bijvoorbeeld «publiek» en «privaat» (bijvoorbeeld over instellingen) in Nederlands recht. Een «publieke» of «public» cloud is een commerciële clouddienst bij een dienstverlener waar zowel de hardware als de software met andere organisaties wordt gedeeld, en waarin je (afhankelijk van de behoefte) capaciteit en verwerking krijgt toebedeeld door de dienstverlener. De commerciële clouddienst is verantwoordelijk voor de scheiding van de processen en data van de verschillende gebruikers.

Naast de public cloud onderscheidt de NIST ook andere vormen van cloud. «Private» of een «privé» cloud, waarbij gebruik gemaakt wordt van cloud technieken en infrastructuur, al dan niet uitbesteed, ingericht voor een enkele afnemer. Een private cloudoplossing stelt door de aard van deze techniek hogere eisen aan kennis bij zowel uitbestedende als inbestedende partijen. Dit onder meer omdat er geen gedeelde resources gebruikt kunnen worden, maar deze specifiek voor de oplossing moeten worden ingezet. Hiermee zullen initiële kosten voor de afnemer hoger kunnen zijn. Tot slot bestaat ook community (of gemeenschappelijke) cloud, waarbij de cloud technieken en/of infrastructuur ingericht worden voor een specifieke “community” van afnemers met gemeenschappelijke eisen aan een cloudomgeving, en hybride cloud, een combinatie van een van deze modellen. Een hybride cloud omgeving combineert cloudtechnieken met andere ICT aanbiedingsvormen zoals on-premise oplossingen. Multi-cloud houdt in dat afnemende organisaties gebruik maken van een combinatie van verschillende al dan niet public clouddiensten.

Hiernaast kan cloud opgedeeld worden in verschillende servicemodellen, zoals Software as a Service (SaaS), Platform as a Service (PaaS) en, Infrastructure as a Service (IaaS). IaaS betekent dat cloudaanbieder de hardware beheert en de gebruiker de rest. Bij een PaaS model voorziet de aanbieder in hardware en een besturingsysteem, en de gebruiker regelt de rest. SaaS houdt in dat de gebruiker meestal online inlogt in een omgeving en vervolgens kan werken in die omgeving. De aanbieder is verantwoordelijk voor het beheer van de applicatie en alle onderliggende infrastructuur. Afhankelijk van het gebruikte servicemodel worden er méér diensten aan de cloudleverancier uitbesteed, waardoor er minder eigen inrichtingseisen kunnen worden opgelegd aan de omgeving.

Problematiek op de cloudmarkt

Net als de opstellers van de initiatiefnota signaleert het kabinet dat er diverse problemen spelen op de markt voor clouddiensten. Deze problemen zorgen ervoor dat Europese cloudaanbieders niet eerlijk en effectief kunnen concurreren met de

grote cloudaanbieders en dat gebruikers onvoldoende keuzevrijheid ervaren in het gebruik van clouddiensten. De problemen zijn het gevolg van oorzaken die deels uniek zijn en deels overlappen. Eerder zijn in diverse analyses, zoals onder andere de agenda DOSA, de marktstudie naar clouddiensten van de ACM[10] en een recente CPB studie over economische afhankelijkheden[11], uitgebreid de onderliggende oorzaken voor het huidige functioneren van de markt voor clouddiensten uiteengezet. In deze sectie zetten we de vier voornaamste problemen en onderliggende oorzaken kernachtig op een rij. Een gedetailleerdere beschrijving van de huidige problematiek op de cloudmarkt is opgenomen in een bijlage bij deze brief.

1. Concurrentiepositie Europese bedrijven op de markt voor clouddiensten

Een voorname oorzaak voor de slecht functionerende cloudmarkt is de verregaande concentratie aan de aanbodzijde van de markt. Vier grote niet-Europese bedrijven domineren de wereldwijde markt voor public cloudinfrastructuur: de zogenoemde Amerikaanse hyperscalers Amazon, Microsoft, Google en het Chinese Alibaba.[12] In Nederland en de rest van Europa beschikken met name Amazon en Microsoft over grote geconsolideerde marktaandelen. De ACM verwacht dat de marktconsolidatie verder doorzet als gevolg van onder meer schaalvoordelen en netwerkeffecten.[13]

De overweldigende schaal die Amerikaanse partijen hebben voor investeringen in innovatie en uitbreiding van hun clouddienstverlening en infrastructuur is een belangrijke reden waarom Europese aanbieders niet in staat zijn om te concurreren. Als gevolg van deze schaal bieden de hyperscalers een dienstenaanbod dat qua integraliteit en kwaliteit op dit moment superieur is. Hyperscalers profiteren dus sterk van hun wereldwijde aanwezigheid en technologische voorsprong.

De omvang van de problematiek verschilt per cloudlaag: de markt voor SaaS-diensten is relatief heterogeen met veel productdifferentiatie en meer ruimte voor specialistisch aanbod van kleinere aanbieders. PaaS- en IaaS-diensten hebben een homogenere aard, waardoor de dominante marktpartijen hier op schaal kunnen concurreren. In haar rapport stelt ACM dat met name op deze twee sub-markten de grote cloudaanbieders een sterke marktpositie hebben, die voorlopig niet in te halen is.[14] Al met al is het voor kleinere partijen met een minder omvangrijk dienstenaanbod moeilijk om effectief te concurreren met hyperscalers met een geïntegreerd aanbod over alle cloudlagen. Het is te verwachten dat de consolidatie in de markt voor clouddiensten verder doorzet.

Het sterk geconcentreerde marktaanbod is op zichzelf problematisch voor onze concurrentiepositie en digitale open strategische autonomie, maar heeft daarnaast diverse negatieve afgeleide effecten:

- Zo kan het op den duur negatieve effecten hebben op het innovatievermogen van de lokale cloudsector. Kennis en technologie in Europa worden in grote

[10] Marktstudie clouddiensten | ACM.nl
[11] Kansen en kwetsbaarheden: economische verwevenheid met de VS (cpb.nl)
[12] Staat van de Europese Unie 2023 | Tweede Kamer der Staten-Generaal
[13] Marktstudie clouddiensten | ACM.nl
[14] Marktstudie clouddiensten | ACM.nl

mate benut door niet-Europese bedrijven, vanwege hun grotere financiële armkracht. Op termijn kan een tekort aan gekwalificeerd personeel ontstaan in eigen cloudinfrastructuur binnen Europa.[15]

- Daarnaast hebben lokale cloudaanbieders vaak geen eigen geïntegreerd aanbod van cloudinfrastructuurdiensten tot cloudapplicaties, waardoor ze hun cloudaanbod doorgaans aanbieden via de infrastructuur van een van de hyperscalers moeten leveren. Hierdoor zijn de partijen verbonden aan en afhankelijk van de infrastructuur van een hyperscaler, waardoor de innovaties van uitdagers worden geabsorbeerd in het aanbod van de hyperscaler.[16] Als gevolg hiervan zijn deze kleinere partijen ook aantrekkelijke kandidaten voor overname door een hyperscaler.
- Hyperscalers zijn in diverse sectoren van de digitale economie in staat geweest hun leidende marktpositie in te zetten voor het creëren van een sterke positie in aanpalende of nieuwe digitale markten. Hun leidende positie in de cloudmarkt, geeft hyperscalers bij uitstek een goede uitgangspositie om ook op de AI-markt dominant te worden. Schaalbare rekenkracht en dataopslag zijn elementen die de cloud een belangrijke bouwsteen maken voor ontwikkelaars, aanbieders en gebruikers van AI-modellen en systemen. Alternatieven voor de hyperscalers ontbreken namelijk veelal door de hoge investeringen die gepaard gaan met de infrastructuur die nodig is voor het trainen van (generatieve) AI-modellen. Er lopen daarom diverse onderzoeken op Europees niveau naar exclusieve partnerships tussen hyperscalers en aanbieders van generatieve AI.

2. Gebrek aan keuzevrijheid voor eindgebruikers

Waar het vorige probleem voornamelijk voortkomt uit oorzaken aan de aanbodzijde van de markt voor clouddiensten, spelen er ook problemen aan de vraagzijde van de markt: afnemers hebben beperkte keuzevrijheid op de markt voor clouddiensten. Voor een deel zijn is dit het gevolg van de hoge mate van concentratie op de markt: organisaties die een geïntegreerd pakket aan clouddiensten op de SaaS, PaaS en IaaS lagen willen afnemen, zijn grotendeels afhankelijk van het aanbod van grote niet-Europese technologiebedrijven.

Een ander belangrijk obstakel voor keuzevrijheid is de *vendor lock-in* die afnemers kunnen ervaren. Er is sprake van lock-in als cloudaanbieders door middel van belemmeringen de mogelijkheden van afnemers beperken om over te stappen naar een andere cloudaanbieder. Aan deze lock-in liggen verschillende oorzaken ten grondslag, zoals ook ACM in haar marktstudie gedetailleerd heeft uitgewerkt.[17] Overstapbelemmeringen kunnen technisch, organisatorisch en financieel van aard zijn. De technische en organisatorische belemmeringen zijn in grote mate gerelateerd aan beperkte dataportabiliteit en interoperabiliteit.

Dataportabiliteit betreft de mogelijkheid om gegevens over te zetten van één clouddienst naar een ander. Door sterke verwevenheid tussen de clouddiensten en bedrijfsprocessen van een organisatie kost het veel tijd en werk om (alle) diensten te ontvlechten en opnieuw in te richten. Ook is het technisch niet altijd mogelijk

[15] The Future of European Competitiveness, Part B
[16] Marktstudie clouddiensten | ACM.nl
[17] Marktstudie clouddiensten | ACM.nl

gegevens over te zetten. Als gevolg hiervan is het niet altijd vooraf duidelijk voor een gebruiker of het mogelijk is hun data volledig en met behoud van functionaliteit te porteren van de ene cloudaanbieder naar de andere.

Interoperabiliteit is de mogelijkheid om gelijktijdig verschillende clouddiensten te gebruiken en met elkaar te verbinden. Een vaak genoemde oplossing om lock-in te voorkomen is de inzet van multi-cloud, waarbij een gebruiker interoperabele clouddiensten afneemt van verschillende aanbieders en deze met elkaar verbindt. In de praktijk zijn de mogelijkheden om lock-in te voorkomen met multi-cloud echter beperkt, vanwege beperkte interoperabiliteit tussen clouddiensten van verschillende aanbieders.[18] De clouddiensten kunnen daardoor niet effectief met elkaar communiceren en samenwerken. Als gevolg hiervan zijn gebruikers bij het kiezen van nieuwe diensten in de praktijk vaak beperkt tot dezelfde aanbieder of een derde partij die gebruik maakt van een compatibele cloudinfrastructuur. Gebrekkige interoperabiliteit versterkt zo vendor lock-in.

Financiële overstapbelemmeringen ontstaan met name door de tariefstructuur die veel cloudaanbieders hanteren. De schaalbaarheid van gebruik van clouddiensten zorgt voor een tariefstructuur die complex, en zorgt voor onvoorspelbaarheid over de uiteindelijke totale kosten van gebruik van clouddiensten. Verder kan een overstap ook leiden tot onvoorspelbare kosten. Zo kan data in veel gevallen kosteloos in de cloud worden geplaatst (ingress fees), maar worden er wel kosten gerekend voor het verplaatsen van data uit de cloud, bijvoorbeeld naar een andere aanbieder (egress fees).[19]

Al met al wordt de marktconcentratie aan de aanbodzijde door vendor lock-in verder versterkt: financiële overstapdrempels en technische barrières zoals gebrekkige dataportabiliteit en interoperabiliteit versterken het concurrentievoordeel van leidende marktpartijen.

3. Publieke belangen, databescherming en rechtsmachtconflicten

Data zijn een waardevolle bron in de digitale economie, die strategisch moeten worden beheerd, beschermd en benut. Cloud is in dat opzicht niet alleen een technische efficiëntiemaatregel: het kan impact hebben op de manier waarop publieke waarden als privacy, transparantie en keuzevrijheid worden gehandhaafd. Zo is het ten allen tijde van belang dat de juiste afwegingen worden gemaakt bij het inzetten van public cloud, met name daar waar het op data betrekking heeft op het vlak van de nationale veiligheid of gevoelige gegevens van en over Nederlandse burgers. Ook toegang tot data in de cloud die nodig zijn voor het uitvoeren van overheidstaken en dienstverlening aan burgers en bedrijven moet worden geborgd. Door beperkte keuze op de cloudmarkt is het niet altijd mogelijk voor datahouders om een clouddienst af te nemen die enerzijds passend is bij het benodigde veiligheidsniveau voor de data, en anderzijds de gewenste functionaliteit biedt om deze data ook optimaal te kunnen benutten.

[18] Marktstudie clouddiensten | ACM.nl, zie paragraaf 2.5 en 6.2.
[19] De problematiek op het vlak van egress fees lijkt recentelijk al te worden geadresseerd door de drie grootste marktpartijen, door deze kosten niet langer door te berekenen. Zie bijvoorbeeld: Amazon AWS Joins Google Cloud In Removing Egress Costs (forrester.com)

Een belangrijke oorzaak voor zorgen over databescherming in de cloud zijn rechtsmachtconflicten tussen staten/machtsblokken. Diverse landen kennen wet- en regelgeving met extraterritoriale werking die medewerking aan veiligheidsdiensten verplicht, zoals de CLOUD Act in de Verenigde Staten (V.S.).[20] Dergelijke wet- en regelgeving kan in bepaalde gevallen mogelijk leiden tot ongewenste toegang tot Nederlandse gegevens wanneer dit conflicteert met regelgeving als de AVG. Hier is uw Kamer eerder over geïnformeerd.[21]

Op verzoek van het Nationaal Cyber Security Centrum (NCSC) heeft advocatenkantoor 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.

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

4. Cloudtechnologie kan worden ingezet als geopolitiek pressiemiddel.

Een grote afhankelijkheid van een klein aantal leveranciers uit één land zorgt er tevens voor dat de toegang tot cloudtechnologie mogelijk als geopolitiek pressiemiddel ingezet zou kunnen worden, wanneer dit door een dergelijk land opportuun wordt geacht en mogelijk is binnen juridische kaders. Op dit moment is er geen concrete aanleiding dat dit risico daadwerkelijk tot stand komt, maar de gevolgen van de verwezenlijking van een dergelijk risico zijn zeer groot voor o.a. de nationale veiligheid en autonomie van de Nederlandse overheid en samenleving. Hierdoor is het van belang om risico's van dergelijke strategische afhankelijkheden te mitigeren.

Huidig beleid aangaande de cloudmarkt

Het kabinet zet zich met diverse beleidsinitiatieven op nationaal en Europees niveau in om de hierboven geschetste problematiek te adresseren en zodoende te komen tot een goedwerkende cloudmarkt, waarin Europese cloudaanbieders eerlijk kunnen concurreren met de hyperscalers en gebruikers voldoende keuzevrijheid ervaren in de clouddiensten die zij gebruiken.

[20] 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. Er ligt een adequaatheidsbesluit onderschreven door Nederland.
[21] JBZ-Raad | Tweede Kamer der Staten-Generaal

De problemen op de markt voor clouddiensten doen zich voor aan de vraag- en aanbodzijde van de markt. Het is daarom belangrijk om beleid te richten op het versterken van beide onderdelen van onze cloud-economie.

Aan de *aanbodkant* kunnen overheden maatregelen nemen om de toetredingsdrempels voor nieuwe aanbieders te verlagen, zoals het bevorderen van open standaarden, het bieden van subsidies of investeringsprogramma's, en het faciliteren van een eerlijke toegang tot cloudinfrastructuren.

Aan de *vraagkant* kan de overheid optreden als een strategische klant, waarbij zij innovatieve oplossingen bevordert door vraagontwikkeling van nieuwe Europese clouddiensten te stimuleren. Dit kan door het stimuleren van interoperabiliteit, het ondersteunen van multi-cloudstrategieën en door overheidsopdrachten toegankelijker te maken (open inkoop). Gezien het feit dat het huidige kabinetsbeleid zich vooral op de aanbodzijde richt, legt de initiatiefnota terecht ook de nadruk op de vraagzijde van de markt voor clouddiensten.

De beleidsinzet delen we als kabinet in langs de drie pijlers uit de Agenda DOSA:
- 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 schaal te creëren en hiermee Europese aanbieders te stimuleren;
- Partnership: samenwerking en contact met marktpartijen en overheden, zowel decentraal als Europees, voor het uitwisselen van expertise en best practices.

Door het kabinet ingezette beleidsinstrumenten kunnen niet op alle hierboven benoemde problemen tegelijk worden gericht, daarvoor is een gecombineerde aanpak nodig. Zo vragen zorgen met betrekking tot nationale veiligheid om een ander perspectief en een ander handelingskader dan zorgen over keuzevrijheid voor consumenten. Dit betekent dat er een veelheid aan beleidsinstrumenten op het gebied van cloud wordt ingezet, één one-size-fits-all oplossing bestaat niet. De volgende beleidsinitiatieven maken deel uit van de bestaande beleidsinzet van het kabinet. Een deel wordt ook in de initiatiefnota benoemd maar voor de volledigheid benoemen we hier kort de lopende inzet op verschillende beleidsterreinen:

Protect
<u>Cyberveiligheid en digitale weerbaarheid</u>
- EU Cybersecurity Certification Scheme for Cloud Services (EUCS)

In het kader van de Europese Cyber Security Verordening wordt door de Europese Commissie samen met het Europese cyberagentschap ENISA een EU cybersecurity certificeringsschema voor cloud services (EUCS) uitgewerkt als uitvoeringshandeling. Het doel van de EUCS is om zowel het beveiligingsniveau tegen cyberdreigingen te verhogen, als om ervoor te zorgen dat clouddienstverleners schaalvoordelen biedt omdat zij niet in elke lidstaat afzonderlijk een certificaat hoeven te behalen. De Europese regeling vervangt daarmee vergelijkbare nationale certificeringen. Tegelijkertijd kan het EUCS

cloudgebruikers helpen de veiligheid van de clouddiensten van hun leveranciers te beoordelen en aan te tonen. Naar verwachting zal de EUCS begin 2025 worden gefinaliseerd zodat het EUCS-schema volgend jaar kan worden gepubliceerd.

- Network and Information Security Directive revised (NIS2-richtlijn)

De NIS2 (Network and Information Security Directive) is een nieuwe Europese richtlijn gericht op het vergroten van digitale weerbaarheid en het beperken van de gevolgen van cyberincidenten in de Europese Unie (EU). In Nederland wordt de NIS2-richtlijn geïmplementeerd in de vorm van de Cyberbeveiligingswet. Op het moment dat de Cyberbeveiligingswet wordt aangenomen, vervangt deze de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni).

Met de komst van de NIS2 gaan meer sectoren onder deze wetgeving vallen – waaronder ook digitale dienstverleners, zoals aanbieders van clouddiensten. Deze bedrijven moeten voldoen aan o.a. een zorgplicht om risico's op netwerk- en informatiesystemen te beheersen en een meldplicht met betrekking tot mogelijke significante incidenten. Dit met als doel om de digitale weerbaarheid te verhogen.

Zowel het EUCS als de NIS-2-richtlijn richten zich op het geconstateerde probleem van databescherming, en bieden zowel praktisch als juridisch oplossingen. Daarnaast maakt deze wetgeving het voor eindgebruikers inzichtelijker om te zien aan welke veiligheidsnormen aanbieders voldoen.

- Baseline Informatiebeveiliging Overheid 2.0 (BIO 2.0)

De Baseline Informatiebeveiliging Overheid (BIO)[22] wordt momenteel herzien. In de BIO 2.0 is ook meer inzet op cloud. Hoewel de huidige teksten nog in concept zijn, omvatten de nieuwe maatregelen onder meer:

- Verplicht een inventaris van alle bedrijfsmiddelen die van belang zijn voor informatieverwerking, met alle eigenschappen die nodig zijn voor beheer en onderhoud. In de inventaris zijn ook cloud-omgevingen opgenomen.
- Een beheersmaatregel omtrent informatiebeveiliging voor het gebruik van clouddiensten. Er moet beleid zijn – en geïmplementeerd zijn – dat toeziet op het inventariseren, classificeren, selecteren, beoordelen en managen van clouddienst aanbieders, waaronder het beëindigen van dienstverlening door aanbieders van clouddiensten.

- Herziening Rijksbreed Cloudbeleid

Zoals destijds in het beleid zelf al werd aangekondigd zou het Rijksbreed cloudbeleid 2022 geëvalueerd en waar nodig herzien worden. In het kader van deze evaluatie hebben CIO Rijk[23], de Auditdienst Rijk (ADR)[24] en de Algemene Rekenkamer (AR)[25] onderzoeken uitgevoerd op welke punten het beleid herzien moet worden.

[22] Verplichte maatregelen en richtlijnen - Baseline Informatiebeveiliging Overheid 2 (BIO2) [concept]. NB: Dit zijn conceptteksten. Deze teksten kunnen nog aan wijzigingen onderhavig zijn.
[23] Kamerbrief evaluatie Rijksbreed cloudbeleid | Kamerstuk | Rijksoverheid.nl
[24] Bevindingen onderzoeksopdracht 'Evaluatie public cloudbeleid Rijksoverheid' | Rapport | Rijksoverheid.nl
[25] Publicatie verwacht in Q1 '25.

Op hoofdlijnen zijn de aandachtspunten vanuit de evaluatie primair gericht op de volgende punten:

- De implementatie van het Rijksbreed Cloudbeleid 2022, met bijzondere aandacht voor:
    - Departementaal cloudbeleid en -strategie; en
    - Advisering m.b.t. de basisregistraties. Basisregistraties worden veelal beheerd door ZBO's en vallen buiten de reikwijdte van het cloudbeleid.
- Het voorkomen van ongewenste afhankelijkheden op het gebied van marktconcentratie, digitale autonomie, de implementatie van exit-strategieën en continuïteit;
- Het gebruik van AI, algoritmes en nieuwe technologieën;
- Rapportage en registratie. De rapportage over het cloudgebruik blijft achter;
- Inkoopvoorwaarden en doorverkopers. Door SLM Rijk aangescherpte voorwaarden bij hyperscalers worden niet altijd overgenomen indien het cloudgebruik via doorverkopers plaatsvindt;
- Inhoud, effectiviteit en efficiënte risicoafweging;
- Inhoud en doelgroep cloudbeleid en -strategie. Er zijn momenteel geen afspraken over de inhoud van departementaal cloudbeleid en -strategie, waaronder bijvoorbeeld aandacht voor samenwerkingsverbanden en ketenregie; en
- Het verhelderen van termen en begrippen, waaronder 'materieel cloudgebruik'.

In het herziene cloudbeleid zal het gebruik van public cloud door de Rijksoverheid aangescherpt worden, met inbegrip van kaders voor digitale autonomie. Dit heeft als consequentie dat er mogelijk minder digitale diensten van de Rijksoverheid in de public cloud kunnen worden ontwikkeld, afhankelijk van de te beschermen belangen bij desbetreffende diensten. Voor dergelijke diensten zal dan ook onderzocht moeten worden of er een soevereine overheidscloud opgezet kan worden.

<u>Marktwerking</u>

- Dataverordening

Deze wetgeving bevat bepalingen die aanbieders van clouddiensten verplichten overstapbelemmeringen weg te nemen. Ze dienen mee te werken om overstappen tussen clouddiensten technisch mogelijk te maken en mogen geen contractuele belemmeringen opwerpen. Ook mogen ze geen egress fees meer heffen – vooruitlopend op de inwerkingtreding van de Dataverordening hebben verschillende cloudaanbieders hun egress fees recent al uitgefaseerd. Aanbieders moeten er daarnaast voor zorgen dat de gebruiker verschillende diensten tegelijk kan gebruiken. Dat vergroot de keuzevrijheid. Ook verplicht de dataverordening aanbieders van clouddiensten om transparant te zijn richting gebruikers over de jurisdictie waar de aangeboden diensten onder vallen.

De dataverordening treedt 12 september 2025 in werking, de uitvoeringswet wordt naar verwachting begin 2025 naar het Parlement gestuurd. De komende tijd zullen ook nog verschillende standaardisatie trajecten in het kader van deze

verordening plaatsvinden, waarbij ook Nederlandse stakeholders invloed kunnen uitoefenen op de implementatie. De implementatie zal verder de komende jaren van de ACM als beoogd coördinerend toezichthouder en het Ministerie van Economische Zaken het nodige werk vergen, onder andere op het terrein van voorlichting en communicatie.

- Digitalemarktenverordening

De digitalemarktenverordening bevat regels voor aanbieders van kernplatformdiensten die door de Europese Commissie als poortwachter worden aangewezen vanwege hun marktpositie. De verordening bevat ook interoperabiliteit- en dataportabiliteitverplichtingen voor deze poortwachtersplatforms. Tot nu toe is er nog geen poortwachter aangewezen op het terrein van clouddiensten. Dat betekent dat de betreffende verplichtingen nog niet van toepassing zijn op de grote aanbieders van clouddiensten. Op termijn kan deze verordening echter wel bijdragen aan het vergroten van keuzemogelijkheden voor gebruikers. Het kabinet zet zich ervoor in om de aanpak van problematiek op cloudmarkten onderdeel te maken van de evaluatie van de digitalemarktenverordening, die is voorzien voor 2026.

De hierboven genoemde dataverordening en digitalemarktenverordening dienen niet alleen om bescherming te bieden. Door het eerlijke speelveld worden ook kansen voor Europese bedrijven gecreëerd. Daarmee zorgen deze lopende beleidsmaatregelen ervoor dat problematiek op het terrein van de Europese concurrentiepositie en het gebrek aan keuzevrijheid worden geadresseerd. De komende jaren zullen deze verordeningen ook worden geëvalueerd. Hieruit kunnen mogelijke wijzigingen in de regelgeving of nieuwe beleidsopties voortkomen. Het is echter nog te vroeg om hierop vooruit te lopen.

Promote

- Gaia-X

Gaia-X is een samenwerkingsverband van honderden bedrijven dat een gemeenschappelijke set van regels en afspraken over cloudinfrastructuur en datadeling heeft ontwikkeld.[26] Het biedt standaarden die zorgen voor veilige gegevensuitwisseling en bevorderen interoperabiliteit binnen het cloudlandschap. Dit maakt het mogelijk om bestaande diensten te verbinden en nieuwe innovatieve toepassingen te ontwikkelen. Het initiatief is erop gericht een alternatief te ontwikkelen voor de deels gesloten ecosystemen van bestaande grote cloudspelers. Diverse Nederlandse bedrijven en organisaties zijn de drijvende kracht achter Gaia-X. Ook niet-Europese partijen kunnen aansluiten bij het initiatief: het is immers de bedoeling dat die partijen zich ook houden aan Europese wetten en waarden. Ze hebben echter geen stemrecht.

Het kabinet zet zich actief in om Nederlandse belangen binnen het initiatief te borgen en is betrokken bij het oprichten van de Nederlandse Gaia-X hub (ondergebracht bij TNO) en financiert deze. De hub functioneert als centraal punt voor ontwikkelingen in Nederland en voor het ontwikkelen en uitwerken van use cases. Ook is het kabinet vertegenwoordigd in de Governmental Advisory Board

[26] Home - Gaia-X: A Federated Secure Data Infrastructure

van Gaia-X die het initiatief gevraagd en ongevraagd adviseert. Over de voortgang van het Gaia-X initiatief wordt u separaat geïnformeerd[27].

- Important Projects of Common European Interest Cloud Infrastructure and Services (IPCEI CIS)

IPCEI CIS betreft een belangrijk digitaal initiatief voor Europa, waar meer dan 100 bedrijven en onderzoeksorganisaties uit 12 EU-lidstaten met hulp van staatssteun gaan samenwerken om een volledig nieuwe Europese gedecentraliseerde software-infrastructuur voor het geavanceerde gebruik van computerbronnen op het gebied van cloud en edge te bouwen.[28] Het geheel wordt gebouwd in een nieuw type open ecosysteem, waarin meerdere aanbieders samen een infrastructuur opzetten en beheren. Door de opzet van dit ecosysteem worden de technologische afhankelijkheden en ongewenste lock-in-effecten verminderd. IPCEI CIS is eind 2023 van start gegaan, en resultaten worden in de komende jaren verwacht. U bent hierover eind 2023 in een Kamerbrief geïnformeerd.[29] Op het moment van het versturen van deze brief werken de drie Nederlandse consortia met daarin 13 Nederlandse bedrijven en kennisinstellingen nog aan de uitvoering van hun projectplannen. U wordt hier separaat verder over geïnformeerd[30].

De komende jaren worden verschillende resultaten verwacht, die zullen worden gedeeld met de relevante sectoren. Dergelijke resultaten van investeringsprogramma's kunnen bijdragen aan een sterkere concurrentiepositie van het Europees bedrijfsleven en vergroten de keuzevrijheid van eindgebruikers. In de reactie op aanbeveling 2g wordt hier ook nader op ingegaan.

Partnership
Op Europees en nationaal is Nederland betrokken in verschillende samenwerkingsinitiatieven. Zo zijn de Nederlandse overheid en verschillende bedrijven deelnemer van de Europese Alliantie voor industriële data, edge en cloud. Deze alliantie heeft tot doel de ontwikkeling en uitrol van edge- en cloudtechnologieën van de volgende generatie te bevorderen. De alliantie brengt bedrijven, vertegenwoordigers van lidstaten en relevante deskundigen samen. In Nederland financiert het Ministerie van Economische Zaken het *Centre of Excellence voor Data Sharing en Cloud* opgericht (bij TNO), waarmee het Nederlandse bedrijfsleven wordt geïnformeerd over datadelen en cloud. Ook de Nederlandse Gaia-X hub is ondergebracht in dit centrum.

Over de voortgang op deze (Europese) protect, promote en partner initiatieven bent u op verschillende momenten separaat geïnformeerd middels verschillende Kamerbrieven, zoals benoemd in de inleiding van deze brief. Ook in de nabije toekomst zult u worden geïnformeerd over de voortgang van deze trajecten. Hierbij wordt ook ingegaan op de financiële consequenties van de verschillende beleidsinstrumenten. Zo zijn er al middelen beschikbaar gesteld voor de lopende

[27] De voortgang wordt beschreven in de Kamerbrief Voortgangsupdate IPCEI CIS en Gaia-X, die 17 januari 2025 naar de Tweede Kamer is verzonden.
[28] IPCEI Cloud Infrastructuur en Services (CIS) | RVO.nl
[29] Kamerstuk 26643, nr. 1114.
[30] De voortgang wordt beschreven in de Kamerbrief Voortgangsupdate IPCEI CIS en Gaia-X, die 17 januari 2025 naar de Tweede Kamer is verzonden.

subsidietrajecten en vereisen de verschillende genoemde wetgevingsinitiatieven capaciteit bij de toezichthouders.

Geïntegreerde aanvullende aanpak voor cloud

Cloud is in relatief kort tijdsbestek een onmisbare bouwsteen in onze digitale economie en samenleving geworden. Het gebruik van clouddiensten brengt organisaties vele voordelen, met name op het vlak van gebruiksgemak en efficiëntie. Grote en kleine organisaties kunnen door makkelijk schaalbare, on-demand clouddiensten leunen op relatief hoogwaardige, veilige en continue ICT-dienstverlening voor hun bedrijfsvoering, bijvoorbeeld voor het optimaliseren van interne processen en dienstverlening. Voor ons economisch verdienvermogen en onze brede welvaart is de brede adoptie van cloudtechnologie in het bedrijfsleven en de overheid daarom een positieve zaak, en een ontwikkeling die we met concreet beleid nastreven.

Nederland is mede hierdoor in Europees verband een voorloper in de migratie van overheid en bedrijfsleven richting de cloud. De grootschalige cloudmigratie brengt echter ook uitdagingen met zich mee, die in de voorgaande secties uitgebreid zijn toegelicht. Centraal in deze uitdagingen staat de noodzaak om afhankelijkheden af te bouwen teneinde onze nationale veiligheid en digitale open strategische autonomie te waarborgen.

Ook de overheid maakt gebruik van clouddiensten om voorgenoemde voordelen. Recente ontwikkelingen laten echter zien dat een ongebreidelde cloudadoptie van veelal ‘big-tech’-spelers ook risico’s met zich meebrengt. Om deze risico’s te mitigeren wordt in het kader van de NDS en de vernieuwing van het cloudbeleid voor de (rijks)overheid gekeken naar mogelijkheden om cloudtechnologie op verantwoorde wijze in te zetten.

Om de ambities op het vlak van strategische autonomie, in het licht van toenemende geopolitieke spanning, meer kracht bij te zetten komen we in dit deel van de kabinetsreactie tot aanvullende beleidsacties voor het stimuleren van verantwoord gebruik van clouddienstverlening door organisaties in Nederland. We zetten in deze *geïntegreerde aanvullende aanpak voor cloud* dus de acties uiteen die het kabinet in aanvulling op het reeds lopende beleid zal uitwerken om afhankelijkheden op het gebied van cloud tegen te gaan.

Uniforme beleidsinzet op Europees niveau

De complexe en veelzijdige problematiek op de Nederlandse cloudmarkt is niet uniek, andere lidstaten ervaren problemen van gelijke aard. Het clouddossier staat dan ook bij diverse andere lidstaten en de Europese Commissie hoog op de agenda. Vanwege de internationale aard van de marktproblematiek is het van essentieel belang om problemen waar mogelijk in Europees verband beleidsmatig aan te pakken. De lidstaten van de Europese Unie lopen tegen dezelfde problemen aan en kunnen deze niet zelfstandig oplossen. Gezamenlijke oplossingen dragen daarnaast bij aan een effectief functionerende Europese interne markt.

In dat verband verwelkomt het kabinet de toegenomen Europese inzet op het dossier (zie o.a. de sectie 'Huidig beleid aangaande de cloudmarkt'). Op basis van de expliciete aandacht voor cloud in het Draghi-rapport en in de mission letter voor de nieuwe Eurocommissaris Virkkunen is de verwachting dat in de aankomende periode aanvullende Europese beleidsinitiatieven voor het verbeteren van het functioneren van de cloudmarkt te verwachten zijn.

Hierbij heeft Nederland specifieke aandacht voor mogelijk nieuw EU-cloudbeleid dat in de mission letter voor nieuwe Eurocommissaris Virkkunen is aangekondigd.[31] Zo wordt hierin de ambitie uiteengezet om een *EU Cloud and AI Development Act* uit te werken, gericht op het stimuleren van onze competitiviteit door middel van het beschikbaar stellen van financiering voor expansie en innovatie van de Europese cloud en AI infrastructuur. Ook wordt de wens voor het ontwikkelen van een *single EU-wide cloud policy for public administrations and public procurement* aangekondigd. Dit beleid zou een herziening moeten gaan vormen van bestaande aanbestedingsrichtlijnen, welke ertoe zou moeten bijdragen dat in cloud aanbestedingen meer rekening met de Europese sector gehouden kan worden. Ook mogelijke aanvullende investeringen via nieuwe *Important Projects of Common European Interest* worden op dit moment onderzocht, waarbij het kabinet op dit moment nog niet vooruit kan lopen op mogelijk Nederlandse deelname.

Deze voorstellen vinden hun oorsprong in het Draghi-rapport over de toekomst van de Europese concurrentiepositie en adresseren (in potentie) veel van de problematiek die geschetst is in de initiatiefnota, zowel aan de vraagkant (zoals op het vlak van aanbestedingsregels) als aan de aanbodkant (bijvoorbeeld met betrekking tot innovatie en investeringsbehoefte).[32] Het samenspel van stimulering, wetgeving en een vernieuwde rol van overheidsaanbestedingen in deze voorstellen kan zeer effectief zijn om problemen te adresseren, zeker als deze beleidsinzet samen met het bedrijfsleven wordt vormgegeven. De kabinetsinzet zal er dan ook op gericht zijn een actief betrokken rol te hebben in de vormgeving en totstandkoming van effectief Europees beleid. Uiteraard wordt ieder nieuw voorstel van de Commissie individueel op haar wenselijkheid beoordeeld, maar het kabinet onderschrijft de redenering dat problematiek van internationale aard, voor zover mogelijk, gezamenlijk binnen de EU geadresseerd dient te worden. Daarnaast wordt de komende jaren ook verder ingezet op de uitwerking van lopende beleidsacties op Europees niveau, waarover u eerder in deze brief al hebt kunnen lezen.

Aanvullende nationale beleidsacties
Het kabinet ontwikkelt in aanvulling op de Europese plannen additionele nationale beleidsacties, bijvoorbeeld waar het problematiek betreft die nationaal is van aard, die onvoldoende wordt geadresseerd door EU-beleid of waar het kabinet zelf nadere beleidsintensivering op nastreeft. Uitgangspunt hierbij is om nationale acties in ieder geval niet contrair of redundant te laten zijn ten opzichte van de hierboven beschreven Europese beleidsplannen.

[31] European Commission (2024) – Mission Letter Henna Virkkunen, Executive Vice-President-designate for Tech Sovereignty, Security and Democracy.
[32] The Future of European Competitiveness, Part B

Onze voorgenomen inzet hebben we hieronder uitgesplitst naar beleid gericht op de aanbod- en de vraagzijde van de markt. Bij de vraagzijde staan we ook expliciet stil bij beleid voor de overheid als cloudgebruiker. In de volgende paragrafen wordt hier kort bij stilgestaan.

Cloudaanbieders

Recent is in opdracht van het Ministerie van Economische Zaken een quickscan uitgevoerd door KPMG om inzichtelijk te maken hoe het aanbod van Europese cloudproviders zich verhoudt tot dat van de grote Amerikaanse cloudaanbieders, bijvoorbeeld in termen van technische functionaliteit en organisatorische aspecten.[33] Hoewel de quickscan aanzienlijk beperkt was in omvang en diepgang, bood het interessante eerste inzichten in de verhoudingen tussen de twee groepen cloudaanbieders. Zo bleek dat de grote cloudaanbieders meer, sneller en geïntegreerder innovatieve diensten aanbieden aan hun afnemers dan lokale cloudaanbieders. Ook hadden de grote cloudaanbieders publiek toegankelijke informatievoorziening en communicatie over hun dienstenaanbod beter op orde richting potentiële afnemers.

Het kabinet wil diepgaander onderzoeken wat de achtergronden van dergelijke bevindingen zijn. Daarvoor is gedetailleerder inzicht nodig in de positie en uitdagingen van de Nederlandse cloudsector, door middel van onderzoek en dialoog. Het is voor het kabinet met name van belang om op een regelmatige en gestructureerde manier in contact te staan met de Nederlandse cloudsector en andere relevante belanghebbenden. Dit vergroot het begrip van de uitdagingen en kansen waar zowel aanbieders als afnemers van clouddiensten mee worden geconfronteerd. Het kabinet zal het initiatief nemen om hiervoor een vaste overlegstructuur in het leven te roepen. Op deze manier kan aanvullend nationaal beleid in samenspraak met de sector worden opgesteld.

Cloudgebruikers

Het kabinet hecht er vanzelfsprekend waarde aan dat individuele organisaties die cloudtechnologie gebruiken dat niet enkel doen op een manier die vanuit bedrijfsmatig opzicht effectief en efficiënt is, maar dat organisaties ook afwegen of de technologie wordt ingezet op een wijze die veilig en verantwoord omspringt met mogelijke technische, juridische of operationele risico's.[34] Veilig en verantwoord cloudgebruik is organisatieafhankelijk en wordt bepaald door het risicoprofiel van een organisatie, bijvoorbeeld op basis van welke processen en gegevens kritiek zijn voor het functioneren van de organisatie.

[33] Het eindrapport van het quickscan-onderzoek naar technische, organisatorische en juridische gaps tussen Europese/Nederlandse cloudproviders en Amerikaanse hyperscalers is een bijlage van de Kamerbrief Uitkomst onderzoekstrajecten SIDN migratie .nl domeinregistratiesysteem naar AWS, die 17 januari 2025 naar de Tweede Kamer is verzonden.

[34] Zoals eerder in de kabinetsreactie op het rapport van Clingendael is gedeeld 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. (…) Dit is niet alleen van belang voor overheden, maar juist ook voor andere afnemers zoals bedrijven, onderwijsinstellingen en consumenten." Zie: Kabinetsreactie Policy Brief van het Clingendael Institute 'Too late to act? Europe's quest for cloud sovereignty | Tweede Kamer der Staten-Generaal

Individuele private en publieke organisaties maken een dergelijke inschatting zelfstandig. Daarbij hebben organisaties met een publieke taak of kritieke functie in de economie logischerwijs veelal een ander risicoprofiel dan kleine ondernemers. Voor bepaalde categorieën cloudgebruikers, zoals vitale bedrijven en overheden, gelden al kaders voor cloudgebruik, maar voor de meeste organisaties is het een afweging die ze zelfstandig zullen moeten maken op basis van hun specifieke situatie.

We constateren dat deze overwegingen nog niet altijd voldoende worden meegewogen bij het kiezen voor clouddienstverlening, zoals ook staat beschreven in een recente studie van Clingendael.[35] Door het maken van bewustere afwegingen kunnen organisaties bijvoorbeeld strategischer inzetten op multi-cloud en gefedereerde of open source cloudoplossingen. Ook kan er, waar passend, meer gebruik worden gemaakt van het innovatieve aanbod van dienstverleners uit Nederland en de rest van de EU.

Om nadere ondersteuning te bieden aan organisaties die voor een cloudmigratie staan, is het kabinet van plan om te komen tot een afwegingskader dat organisaties zelfstandig kunnen toepassen op hun organisatie. Dit kader stellen we op in afstemming met de sector.

Individuele organisaties die cloud (gaan) gebruiken behouden tegelijkertijd een eigen verantwoordelijkheid in het voorkomen of terugdringen van afhankelijkheden. Zo is een belangrijke afweging voor bedrijfsmatige cloudgebruikers het voorkomen van afhankelijkheid van één cloudleverancier, bijvoorbeeld door een exit strategie uit te werken of een cloudarchitectuur te ontwerpen met diensten van meerdere cloudaanbieders. Het is daarbij overigens geen doel op zich dat specifieke partijen worden uitgesloten van de markt. Zo wordt het gebruik van clouddienstverlening van grote niet-Europese dienstverleners niet bij voorbaat ontraden. Wel verdient het, in lijn met de Agenda DOSA, aanbeveling dat afnemers bij het selecteren van clouddiensten afwegen of ongewenste afhankelijkheid van één enkele niet-Europese clouddienstverleners wordt voorkomen. Hoewel het in individuele gevallen niet problematisch hoeft te zijn wanneer organisaties clouddiensten bij één hyperscaler afnemen, kan het op het niveau van onze economie en maatschappij problematisch zijn als de meerderheid van de publieke en private organisatiepopulatie voor haar IT-processen afhankelijk is van één niet-Europese dienstverleners. Ook geldt hierbij natuurlijk dat voor bepaalde categorieën organisaties met een publieke missie of taak, zoals overheden, zorginstellingen of vitale bedrijven er additionele regelgeving kan gelden die het onwenselijk maakt om gebruik te maken van public clouddiensten.

Oplossingen in de zorg en het onderwijs

Ook in de sectoren van zorg en onderwijs wordt gewerkt aan verschillende oplossingen:

- SURF biedt in haar cloud strategie verschillende aanknopingspunten voor een gesprek over de wijze waarop clouddiensten worden afgenomen in het onderwijs.
- Op de website AVG-helpdesk voor Zorg, Welzijn en Sport biedt VWS informatie aan over waar zorgaanbieders rekening mee moeten houden als ze persoonsgegevens in de cloud willen brengen. Het dreigingsbeeld van het expertisecentrum voor de cybersecurity in de zorg Z-CERT geeft voorbeelden van incidenten bij cloudleveranciers. Bijvoorbeeld de cyberinbraak op het portaal Carenzorgt of de alarmknoppen van Tungsten. Hierin is het belangrijk om de risico's in kaart te brengen van zowel buitenlandse als Nederlandse partijen die cloudapplicaties aanbieden. Het ministerie van VWS zal in gesprek gaan met de zorginstellingen over de in de initiatiefnota geschetste problematiek en nagaan of en welke mitigerende maatregelen nodig zijn.

Directoraat-generaal
Economie en Digitalisering
Directie Digitale Economie

Ons kenmerk
DGED-DE / 95898883

Overheid als cloudgebruiker

Cloudgebruik binnen de Rijksoverheid is een belangrijke invalshoek in de initiatiefnota. Naar aanleiding van de huidige ontwikkelingen en de suggesties in de initiatiefnota zal er een herzien cloudbeleid opgesteld worden. Hierin zal het gebruik van public cloud door de Rijksoverheid aangescherpt worden. Dit heeft als consequentie dat er mogelijk minder digitale diensten van de Rijksoverheid in de public cloud kunnen worden ontwikkeld, afhankelijk van de te beschermen belangen bij desbetreffende diensten. Voor dergelijke diensten zal onderzocht worden of er een soevereine overheidscloud opgezet kan worden. Dit wordt verder uitgewerkt in de NDS voor de overheid, onder de verantwoordelijkheid van de staatssecretaris van Digitalisering en Koninkrijksrelaties. Hiermee gaat ingezet worden op de volgende vier pijlers:

1. We maken een overheidsbreed beleid voor het inzetten van clouddiensten. Dit doen we in samenwerking met de medeoverheden. Als gevolg van het overheidsbreed beleid zal op uniforme wijze gebruik gemaakt gaan worden van clouddiensten door de overheid, met bijzondere aandacht voor het bevorderen van de digitale open strategische autonomie van Nederland;
2. We stimuleren de vraag vanuit de overheid en zodoende verstevigen we het aanbod van Europese en Nederlandse clouddiensten. Dit doen we mede door het bundelen van inkoopkracht en -eisen, internationale samenwerking en onderzoek naar het inrichten van (autonome) overheidsbrede cloudvoorzieningen op basis van bestaande structuren;
3. We dragen bij aan advies, monitoring en inzicht vanuit bijvoorbeeld CIO Rijk in gebruikte clouddiensten; en
4. We onderzoeken nieuwe open source oplossingen en autonomie bevorderende technische oplossingen. Dit doen we in aanvulling op de reeds genoemde (Europese) investerings- en onderzoeksprogramma’s zoals IPCEI en DEP. Hiermee kunnen overheidsbrede cloudvoorzieningen opgezet worden.

De NDS wordt naar verwachting gepubliceerd in Q2 2025. Hierin zullen deze acties nader uitgewerkt zijn.

Afsluiting

We kijken er naar uit om deze brief met u te bespreken in een nog te plannen nota-overleg. Hierbij kunnen we ook met elkaar in gesprek gaan over nodige aanvullende acties. In de tussentijd zullen de betrokken departementen in overleg met de betrokken sectoren ook proberen om nog bij te dragen aan verdere kennis- en beleidsontwikkeling.

Dirk Beljaarts
Minister van Economische Zaken

Directoraat-generaal
Economie en Digitalisering
Directie Digitale Economie

Ons kenmerk
DGED-DE / 95898883

Zsolt Szabó
Staatssecretaris Digitalisering en Koninkrijksrelaties

Bijlage I - Opvolging aanbevelingen initiatiefnota

Hieronder wordt per aanbeveling ingegaan op de suggesties van de Tweede Kamer. Daarbij is alleen de titel van de specifieke aanbevelingen aangehaald, niet de volledige tekst waarop wordt gereageerd door het kabinet.

Aanbeveling 1: “Pak de regie over digitale soevereiniteit.”

a) Richt een Rijksmaildienst en een Rijkschatdienst op.

Het kabinet onderschrijft dat het uitgangspunt dat de inzet van open source de autonomie van de overheid kan versterken. Onder meer hierom heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties onlangs het programma Beter Samen Werken (BSW) in het leven geroepen. Er is hiervoor een Proof of Concept (PoC) gestart om te beoordelen of er naast de huidig gebruikte middelen open source alternatieven zijn voor de digitale middelen, zowel voor de dienstinrichting als voor de digitale werkomgeving van ambtenaren en voor centrale diensten zoals een maildienst, agendabeheer en chatdiensten. Hiervoor worden open source oplossingen, zoals die al door Frankrijk en Duitsland worden ingezet en doorontwikkeld, in een Nederlandse digitale werkomgeving hergebruikt.

Door dit in een beperkte PoC onder te brengen kan op korte termijn onderzocht worden of, en zo ja welke, alternatieven gebruikt kunnen worden voor diensten die nu veelal zijn ondergebracht bij een hyperscaler. Hiernaast geeft dit een mogelijkheid om te bepalen of hiermee een strategisch uitwerk scenario mogelijk is waarmee (indien nodig) op korte termijn een oplossing kan worden geboden als er vanuit strategische of technische overwegingen op korte termijn voor specifieke onderdelen van de rijksoverheid meer soevereine ondersteuning moet worden ingericht.

b) Stel normen

De basis van informatie management is om per geval (case-by-case) te beoordelen welke dienst, applicatie of leverancier het meest geschikt en passend is om de ondersteuning te bieden voor de gestelde bedrijfsvraag. Hierbij wordt gestreefd naar een evenwichtige aanpak die openheid combineert met bescherming van publieke belangen. Een quotum voor de inzet van Nederlandse en Europese diensten past niet in die aanpak.

Specifiek voor de inzet van public clouddiensten binnen de rijksoverheid wordt de risicoafweging gemaakt op basis van het Rijksbreed cloudbeleid en het bijbehorende implementatiekader. Het Rijksbreed cloudbeleid zal worden herzien, waarbij een uitgebreide risicoanalyse op proces/systeem/dienstniveau een centrale rol heeft. Het reeds geldende uitgangspunt dat Staatsgeheim-gerubriceerde informatie niet in de public cloud verwerkt mag worden staat in de herziening niet ter discussie. Hiernaast zal er in 2025 worden gewerkt aan een IT-sourcingstrategie waarmee richtsnoeren worden opgesteld voor het maken van een keuze voor de optimale invulling van ondersteuning (zelf doen, uitbesteden of clouddiensten). Deze aanpak waarborgt dat de Rijksoverheid een passende dienst, applicatie of leverancier kiest, waarbij ook Europese aanbieders diensten kunnen leveren.

c) Centraliseer de kennis

CIO Rijk is opdrachtgever en eigenaar van zogenaamde Rijksbrede voorzieningen. Hieronder valt een aantal ICT systemen die Rijksbreed worden ingezet. Als eigenaar heeft CIO-Rijk een centrale, aansturende rol in de beheersing van die voorzieningen. CIO Rijk heeft een kaderstellende rol ten aanzien van onder andere ICT systemen en infrastructuur. De ministeries zijn zelfstandig verantwoordelijk voor de binnen hun domein gebruikte middelen. Zij leggen hierover ook zelf verantwoording af aan de Tweede Kamer. Zoals ook aangegeven in de Kamerbrief evaluatie Rijksbreed cloudbeleid zal in het hernieuwde cloudbeleid meer aandacht worden gevraagd voor centraal inzicht en monitoring op organisatie overstijgende afhankelijkheden van aangekochte diensten. Hiernaast zal er inzicht worden geboden in materiële diensten die zijn ondergebracht bij public cloudproviders, conform het huidige Rijksbreed cloudbeleid.

d) Verkrijg inzicht in cloudmigraties

Deze aanbeveling is in lijn met eerdere verzoeken van uw Kamer om inzicht te krijgen in deze ontwikkeling.[36] Hiertoe is Rijksbreed een inventarisatie verricht. Uw Kamer is hier recent over geïnformeerd in een Kamerbrief.[37]

e) Trek op met mede-overheden

De beschreven problematiek van cloudmarkt heeft betrekking op zowel de Rijksoverheid als medeoverheden. We onderschrijven het belang van samenwerkende overheden om deze problematiek breed aan te pakken en hanteren in de NDS daarom ook de één-overheidsgedachte. We zijn in gesprek met de medeoverheden om te inventariseren welke mogelijkheden er liggen voor samenwerking. Zo betrekken we bij de doorontwikkeling van het Rijksbreed cloudbeleid ook de medeoverheden. Deze gesprekken zijn reeds gestart en zullen in 2025 vervolgd worden.

Medeoverheden werken ook zelfstandig aan het verminderen van afhankelijkheden. Zo heeft de Vereniging van Nederlandse Gemeenten (VNG) een standaard ontwikkeld voor de inzet van platform-onafhankelijke cloud hosting van applicaties en websites, de zogenaamde Haven-standaard. Deze Haven-standaard is in samenwerking tussen de VNG en de brede cloudsector tot stand gekomen. Gemeenten en leveranciers kunnen op basis van de standaard een omgeving inrichten die gecontroleerd aan de standaard voldoet. Als kabinet omarmen we deze initiatieven, en nemen dit ook mee in de herziening van het Rijksbreed cloudbeleid in het kader van de uitvoering van de NDS.

f) Stimuleer autonomie bij vitale bedrijven

In deze aanbeveling wordt verzocht om in gesprek te gaan met NIS2-organisaties buiten de overheid, waarbij gedoeld wordt op bedrijven in de vitale sectoren. Bij deze afbakening is het belangrijk dat twee soorten reikwijdtes uit elkaar worden gehouden. De reikwijdte van de implementatie van de NIS2-richtlijn binnen het bedrijfsleven is namelijk niet gelijk aan de bedrijven in de vitale sectoren. Het is

[36] https://www.tweedekamer.nl/kamerstukken/plenaire_verslagen/detail/2023-2024/82
[37] Kamerstuk 26643, nr. 1243

belangrijk het onderscheid tussen deze twee kaders te hanteren bij het overwegen van dergelijke maatregelen.

Een partij is pas vitaal als op basis van een vitaal beoordeling blijkt dat deze, op grond van een of meerdere nationale veiligheidsbelang(en), als zodanig kan worden aangemerkt. Bij deze vitaal beoordeling wordt gekeken naar de gevolgen voor de nationale veiligheid bij verstoring, uitval of manipulatie van een proces of dienst.
De scope van de implementatie van de NIS2-richtlijn betreft partijen die overwegend van rechtswege onder deze richtlijn vallen. Hierbij worden andere criteria gehanteerd. Naar schatting zijn dat circa 8.000 entiteiten verdeeld over 15 sectoren.

De NIS2-richtlijn heeft als doel om de digitale en economische weerbaarheid van Europese lidstaten te versterken. En is niet primair bedoeld om de digitale open strategische autonomie bij entiteiten te versterken. Het is van belang om de weerbaarheid van organisaties als uitgangspunt te nemen bij het, indien van toepassing, bevorderen van autonomie. Aangezien de NIS2-richtlijn risicomanagement en -beheersing als een uitgangsprincipe hanteert, dient het onderdeel te zijn van de risicoanalyse die een organisatie zelf uitvoert. Op basis van de onder de NIS2-richtlijn geldende uitgangsprincipes van risicomanagement en -beheersing moeten NIS2-organisaties als onderdeel van hun zorgplicht passende en evenredige maatregelen nemen om de risico’s, voortvloeiend uit door henzelf gedane risicoanalyses, voor de beveiliging van hun netwerk- en informatiesystemen te beheersen.

In dat perspectief dient ook rekening gehouden te worden met het aanbod van hyperscalers van verschillende goed geïntegreerde diensten en producten die kunnen bijdragen aan het verhogen van de cybersecurity van organisaties. Als een organisatie in de huidige markt autonomie wil nastreven en toch een vergelijkbaar serviceniveau wil behouden, is het belangrijk om alle factoren, waaronder ook kosten, zorgvuldig af te wegen. De organisatie dient zelf deze afweging te maken. Daarnaast kan autonomie een belang dienen dat verder reikt dan dat van de organisatie zelf. Uiteindelijk moet een (overheids)organisatie kiezen voor de aanpak die het beste bij zowel haar eigen doelen als bij bredere maatschappelijke of economische belangen aansluit.

Het NCSC publiceert doorlopend adviezen die organisaties, zoals entiteiten binnen de vitale sectoren en NIS2-doelgroepen, kunnen gebruiken om hun eigen weerbaarheid te vergroten. In dat kader hebben het NCSC en ENISA[38] eerder advies uitgebracht over het omgaan met risico’s in de toeleveringsketen, waarbij ook wordt opgeroepen tot het voorkomen van een te grote afhankelijkheid van specifieke toeleveranciers. In deze publicatie wordt onder meer geadviseerd om leveranciers waar een grote afhankelijkheid bestaat goed in kaart te brengen. Ook wordt de aanbeveling gedaan om te inventariseren welke risico’s voortkomen uit geopolitieke ontwikkelingen. Maatregelen die hierbij van belang zijn worden ook genoemd, zoals het maken van worstcasescenario’s en goede afspraken met deze leveranciers.

[38] Good Practices for Supply Chain Cybersecurity | ENISA (europa.eu)

Zoals eerder benoemd is de Tweede Kamer met betrekking tot autonomie en het beperken van afhankelijkheden op het gebied van cloud reeds op 17 oktober 2023 geïnformeerd over de eerder genoemde Agenda DOSA. Zoals in deze agenda is aangegeven, is het overhevelen van activiteiten naar een cloudleverancier buiten de EU in algemene zin niet strijdig met het beleid rond DOSA. Tegelijkertijd is het belangrijk om te kijken naar de omvang van de risico's die dit oplevert, in hoeverre deze risico's (kunnen) worden gemitigeerd door huidig of aanvullend instrumentarium, en wat de mogelijkheid tot substitutie is. In aanvulling hierop is in de Agenda DOSA al een breder onderzoek voorzien waarin mitigerende maatregelen voor de vermindering van cloudafhankelijkheid van Nederland worden verkend.

g) Reserveer ruimte voor datacapaciteit

In de initiatiefnota wordt het dilemma geschetst tussen enerzijds de noodzaak van de beschikbaarheid van voldoende datacentrumcapaciteit zodat groei van het datagebruik geborgd is, terwijl anderzijds bredere afwegingen noodzakelijk zijn rondom ruimtelijke ordening en netcapaciteit waardoor de groei van datacentra juist beperkt zou moeten worden. Tevens wordt aangegeven dat de datacentra op Nederlands grondgebied relatief duurzaam opereren en dat ze een bijdrage kunnen leveren aan de autonomie van cloudgerelateerde vragen zoals het opslaan van gevoelige data. In de aanbeveling wordt opgeroepen om in de Nota Ruimte expliciet aandacht te besteden aan datacentrumcapaciteit voor Nederlandse cloudoplossingen.

Het kabinet herkent het dilemma dat geschetst wordt en waardeert het dat de initiatiefnemers oog hebben voor de onvermijdelijke groei van het datagebruik en de strategische implicatie van het voorhanden zijn van dataverwerkingscapaciteit op het Nederlandse grondgebied. Om grenzen te stellen aan de groei van datacentra heeft het kabinet reeds kaders gesteld door maatregelen te nemen.[39] Zo is per 1 januari 2024 wetgeving van kracht die verbiedt om in Nederland nieuwe hyperscale datacentra te realiseren, met uitzondering van twee locaties.[40] Voor alle andere datacentra gelden geen bindende ruimtelijke regels vanuit het Rijk. Medeoverheden kunnen in hun ruimtelijk beleid ook regels stellen ten aanzien van nieuwvestiging van datacentra. Dit is bijvoorbeeld het geval in de gemeente Amsterdam, de gemeente Haarlemmermeer en de provincie Noord-Holland.

Het kabinet werkt aan een nieuwe Nota Ruimte waarin afwegingen rondom digitale infrastructuur worden meegenomen. Onze digitale infrastructuur is essentieel voor onze gedigitaliseerde samenleving en cruciaal voor het huidige en toekomstige economische verdienvermogen van ons land. Datacenters zijn een onlosmakelijk onderdeel van de digitale infrastructuur, die functioneert als een ecosysteem, waarin elke schakel (zoals zeekabels, glasvezelnetwerken, internetknooppunten, hosting- en clouddienstverleners en datacentra) noodzakelijk is voor het functioneren van het geheel. Nederland is echter een dichtbevolkt en strak ingericht land en niet alles kan zomaar overal. De capaciteit

[39] Kamerstuk 26643, nr. 1242.
[40] Staatsblad 2023, 492

van het energienet heeft op een aantal plaatsen de grens al bereikt (netcongestie) en de beschikbaarheid van zoetwater komt de komende decennia steeds verder onder druk te staan. Tegelijkertijd biedt het benutten van de restwarmte geproduceerd door datacenters kansen voor de warmtetransitie. Omdat datacentra veel energie verbruiken ligt het op korte termijn voor de hand dat datacentra zich bij voorkeur vestigen op plekken met ruimte op het energienet. Op middellange termijn zal de huidige netcongestie naar verwachting afnemen, waardoor dit aspect minder relevant wordt. Ook zullen innovatieve toepassingen naar verwachting leiden tot een vermindering of efficiënter gebruik van zoetwater voor koelingsdoeleinden. Verder spelen ook vraagstukken als ruimtelijke kwaliteit en beschikbaarheid van ruimte een rol in de locatiekeuze voor nieuwe datacentra.
Het kabinet zal onder coördinatie van de Minister van Volkshuisvesting en Ruimtelijke Ordening nog voor de zomer de ontwerp Nota Ruimte presenteren, waarin integraal wordt gekeken naar de ruimtelijke keuzes die we vanuit het Rijk moeten maken en expliciet aandacht zal worden besteed aan de benodigde infrastructuur voor de digitale samenleving.

Aanbeveling 2: “Zorg voor een gezonde voedingsbodem en eerlijke concurrentie”

a) Kom cloud tegemoet

Het is goed dat u benoemt dat we het dienstenaanbod van de Nederlandse cloudsector beter in kaart moeten brengen. Recent is in opdracht van het Ministerie van Economische Zaken een quickscan uitgevoerd door KPMG om inzichtelijk te maken hoe het aanbod van Europese cloudproviders zich verhoudt tot dat van de hyperscalers, bijvoorbeeld in termen van technische functionaliteit en organisatorische aspecten.[41] De omvang van dit onderzoek was beperkt; om een volledig(er) overzicht te verkrijgen is nader onderzoek vereist. Daarnaast wil het kabinet zich ook inzetten voor een gestructureerde en regelmatige dialoog met de sector en werkt hiervoor op korte termijn een concrete aanpak uit.

Zoals in de reactie op aanbeveling 1.e. al genoemd is, vinden we het belangrijk dat overheden met de Nederlandse en Europese sector om de tafel gaan. Zo is bijvoorbeeld de VNG al in gesprek met vertegenwoordigers van het Nederlandse bedrijfsleven over toepassingen van en voor de Haven-standaard.[42] In de reactie op aanbeveling 2.c. wordt ingegaan op de juridische aspecten die een rol spelen bij het Rijksinkoop en aanbestedingsbeleid.

b) Leg duurzame contacten en stimuleer samenwerking

De overheid zal in gesprek blijven met aanbieders van ICT voorzieningen, zowel nationaal als internationaal. Het faciliteren van gesprekken tussen deze leveranciers of andere marktpartijen en het stimuleren van samenwerking zal via de bestaande structuren van de Nationale Technologiestrategie (NTS) worden

[41] Het eindrapport van het quickscan-onderzoek naar technische, organisatorische en juridische gaps tussen Europese/Nederlandse cloudproviders en Amerikaanse hyperscalers is een bijlage van de Kamerbrief Uitkomst onderzoekstrajecten SIDN migratie .nl domeinregistratiesysteem naar AWS, die in januari 2025 naar de Tweede Kamer is verzonden.
[42] Haven, een standaard voor platform-onafhankelijke cloud hosting | VNG

ingericht. In de NTS is cloud meegenomen als onderdeel van de sleuteltechnologie Artificial Intelligence en Data.

c) Hef het 'Ministerie van Microsoft' op

Om de context van SLM Microsoft, Google Cloud en Amazon Web Services te verduidelijken is het noodzakelijk om uiteen te zetten welk belang er wordt gediend met het organiseren van Strategisch Leveranciersmanagement (SLM) binnen de Rijksoverheid. SLM opereert overigens niet als een 'departement', maar is georganiseerd binnen verschillende organisaties van de Rijksoverheid.

In 2014 heeft de Tijdelijke Commissie ICT-projecten onderzoek verricht naar de problemen bij ICT-projecten bij de overheid. In reactie op het eindrapport Tijdelijke Commissie ICT-projecten ('Commissie Elias') geeft het kabinet aan de analyse van de Commissie omtrent de oorzaken van de ICT problemen bij het Rijk te herkennen.[43] Ook zag het kabinet in de aanbevelingen waardevolle maatregelen om de ICT aanpak te verbeteren.

Een van de concrete aanbevelingen was door te gaan met de centralisatie van ICT-inkoop en Rijksbrede ICT-voorzieningen. Deze lijn was in 2013 al ingezet door het kabinet door onder meer het vormgeven van SLM op Microsoft. Het kabinet gaf daarbij aan dat Rijksbreed strategisch leveranciers- en categoriemanagement ICT moest zorgen voor het verbeteren van de aansturing van de ICT leveranciers, voor het creëren van meer toegevoegde waarde voor de organisatie en voor het reduceren van kosten door het beter organiseren van de vraag vanuit het Rijk aan de markt. SLM zou op die manier bijdragen aan het vergroten van de bijdrage van leveranciers aan de strategische doelen van het Rijk en de optimale benutting van contracten waardoor Rijksbrede voordelen kunnen worden behaald.

Om te voorkomen dat alleen met Microsoft goede contractafspraken zouden worden bereikt, is in 2019 door de CIO Rijk aan SLM gevraagd om zich naast Microsoft ook te richten op Google Cloud en Amazon Web Services. Dit heeft ertoe geleid dat in 2023 met AWS een contract tot stand is gekomen, waardoor ook het compliant gebruik van AWS-diensten mogelijk is. Hetzelfde geldt voor Google Workspace. Het is belangrijk om te vermelden dat SLM geen aankopen doet van Microsoft, Google of AWS-(cloud)diensten. SLM schept de contractuele voorwaarden waaronder gebruik van diensten bij deze leveranciers mogelijk is. Het is aan Rijksorganisaties zelf om de afweging te maken of zij diensten van deze partijen willen aankopen en gebruiken. Daarnaast is het aan de Rijksorganisaties zelf om te bepalen of zij additionele impact assessments moeten uitvoeren om het benodigde niveau van compliance te bereiken, rekening houdend met de specifieke context waarin zij de clouddiensten wensen te gebruiken.

In de loop van de tijd zijn er door SLM Microsoft, Google Cloud en Amazon Web Services veel resultaten bereikt, zoals de totstandkoming van essentiële contractuele privacy-amendementen. Dit heeft de contractuele positie van de Rijksoverheid substantieel verbeterd ten opzichte van (de toenmalige) standaardvoorwaarden van Microsoft. Als gevolg van de onderhandelde SLM-voorwaarden is een aanzienlijke verbetering gerealiseerd van de bescherming van

[43] Kamerstuk 33326 nr. 13

grondrechten van de gebruikers van Microsoft, en van compliance in het algemeen. Deze resultaten zijn tevens erkend door andere lidstaten, (EU) toezichthouders en de Europese Commissie.

De AP heeft in het kader van het EDPB-onderzoek[44] drie SLM-functies binnen het Rijk aangeschreven. Naar aanleiding van dit onderzoek concludeert de AP dat het bundelen van kennis en kunde binnen een SLM-functie inspanning en kosten vergt, maar het grote voordelen met zich meebrengt. De AP stelt dat Nederland met de SLM-functie Europees voorop lijkt te lopen en dat de uitgevoerde DPIA's die SLM publiceert internationaal worden benut.[45] Tot slot concludeert de AP dat de SLM-functie op een professionele en vooruitstrevende wijze invulling geeft aan een deel van de rol die rijksoverheidsorganisaties hebben ten aanzien van de bescherming van persoonsgegevens bij de inzet van een CSP.

Het effectief managen van leveranciers is een continu proces dat vereist dat SLM voortdurend alert blijft op wijzigingen in het productaanbod en veranderende wetgeving, bijvoorbeeld op het gebied van AI. Door het regelmatig uitvoeren van paraplu Data Protection Impact Assessments (DPIA's) over de diensten van de diensten en laten uitvoeren van audits, onderhoudt SLM een constante dialoog met de leveranciers. Dit zorgt niet alleen voor het waarborgen van compliance, maar het zorgt er ook voor dat SLM proactief kan inspelen op veranderingen en daardoor Rijkorganisaties tijdig kan adviseren.

De opdracht aan SLM ligt initieel op Microsoft, Google Cloud en AWS. Nederlandse en Europese partijen hebben de DPIA's daarom nog niet doorlopen en hebben nog geen structurele dialoog met SLM. De door SLM opgebouwde kennis en ervaring wordt nu tevens ingezet voor het opbouwen van duurzame relaties met Nederlandse en Europese partijen. Het is daarbij belangrijk te benadrukken dat Nederlandse of Europese partijen niet automatisch compliant zijn met alle EU wet- en regelgeving, en daardoor niet vanzelfsprekend volwaardige alternatieven vormen. Uit een korte voorstudie van de voorwaarden van een grote Europese partij blijkt dat er op dit vlak diverse aandachtspunten zijn. Bovendien is het essentieel dat Nederlandse en Europese cloudaanbieders partijen de benodigde capaciteit en informatie beschikbaar stellen om te kunnen beoordelen in hoeverre hun diensten geschikt zijn voor de Rijksoverheid.

d) Hervorm het aanbestedingsbeleid van de Rijksoverheid

De aanbestedingsregelgeving zorgt voor eerlijke en transparante aanbestedingen, dit betekent dus dat in de basis ook de aanbestedingseisen eerlijk en transparant moeten zijn. Een groot deel van de aanbestedingen waar in de initiatiefnota over gesproken wordt, gaan niet over aankopen van de producten of zogenaamde integrators maar over inkoop van licenties. De inkoop van softwarelicenties wordt vaak zelfstandig in de markt uitgezet. Doordat deze licenties moeten aansluiten bij eerder aangekochte producten, kunnen deze licenties niet anders worden afgenomen dan toegeschreven naar de leverancier van het product.

[44] Launch of coordinated enforcement on use of cloud by public sector | European Data Protection Board (europa.eu)
[45] Brief over Inzet van Cloud Service Providers 10 november 2022 van de Autoriteit Persoonsgegevens over_inzet_cloud_service_providers.pdf (autoriteitpersoonsgegevens.nl) p.3.

Momenteel wordt in Europa steeds meer opgeroepen om strategischer aan te besteden in sectoren, zoals de cloudsector, om ongewenste strategische afhankelijkheden te voorkomen. Zo wordt in zowel het Draghi-rapport als in de mission letter voor de nieuwe Eurocommissaris Virkkunen opgeroepen om het aanbestedingsbeleid voor cloud te herzien. Als Nederland zullen we deze ontwikkeling in Europa ondersteunen en kijken we graag samen met de andere lidstaten en de Europese Commissie hoe een strategischer aanbestedingsbeleid voor de cloudsector te ontwikkelen.

e) Licht de huidige voorrangspositie van publieke cloudleveranciers goed door

Het is een strategische keuze van een systeem- en proceseigenaar of er gekozen wordt voor een cloudoplossing. Voor het inzetten van cloudoplossingen is het Rijksbreed cloudbeleid 2022 van toepassing. Onlangs heeft de Auditdienst Rijk (ADR) het Rijksbreed cloudbeleid geëvalueerd in opdracht van CIO Rijk. Daarnaast voert de Algemene Rekenkamer op dit moment een meerjarig onderzoek uit naar cloudgebruik. Aanvullend daarop zal het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties met de ADR verkennen of in 2025 wederom nader onderzoek naar de naleving van het cloudbeleid uitgevoerd kan worden.

Bij deze aanbeveling dient sowieso opgemerkt te worden dat het Rijksbreed cloudbeleid herzien wordt. In het herziene Rijksbreed cloudbeleid zal het gebruik van public clouddiensten beperkt worden. Tevens zal onderzocht worden of een soevereine overheidscloud opgezet moet worden voor diensten die, gezien de te beschermen belangen, niet in de public cloud verwerkt moeten worden.

De ADR beoordeelt vanuit haar wettelijke taak de naleving van Europese en nationale aanbestedingsregelgeving. Onderdeel van de toets op de comptabele rechtmatigheid is geen eigenstandige kwalitatieve beoordeling van het programma van eisen.

f) Ondersteun nationale partijen bij aanbestedingen

De Aanbestedingswet, de Europese kaders (Richtlijnen 2014/23, 2014/24, 2014/25) en regels zoals die opgenomen zijn in het Government Procurement Agreement (GPA) geven geen ruimte om actief voorkeur te geven aan nationale of Europese aanbieders. Ondernemers uit de EU, GPA-landen en landen waarmee een bilaterale handelsovereenkomst is gesloten, mogen niet minder gunstig behandeld worden dan Nederlandse ondernemers. Alleen inschrijvingen van ondernemers uit landen die geen partij zijn in de GPA kunnen terzijde worden gelegd, deze afweging is aan de aanbestedende dienst. Het is dus niet mogelijk om integraal via aanbestedingen ondersteuning te bieden aan nationale partijen, dit zou namelijk een discriminerende werking hebben naar ondernemers uit de EU, GPA-landen en landen waarmee een bilaterale handelsovereenkomst is gesloten.

Aanbestedende diensten hebben autonomie om hun eigen criteria te stellen voor een aanbesteding. Volgens het Aanbestedingsrecht moeten deze criteria neutraal gesteld worden en niet naar specifieke leveranciers worden toegeschreven. Indien een aanbesteding binnen het toepassingsbereik van de Aanbestedingswet op

defensie- en veiligheidsgebied (ADV) valt[46], zijn er binnen deze ADV mogelijkheden om inschrijvingen van buiten de EU terzijde te leggen. Volgens de ADV (Art. 1.7) kunnen ondernemers die niet binnen de Europese Unie gevestigd zijn, uitgesloten worden van deelname aan een aanbestedingsprocedure, tenzij dit niet is toegestaan op grond van een voor Nederland verbindend verdrag of besluit. Deze mogelijkheid is conform de GPA (Art. 3).

We begrijpen dat het mee kunnen doen in aanbestedingstrajecten van belang is voor de Nederlandse en Europese cloudsector. De Rijksinkoopstrategie geeft richting aan de samenwerking met leveranciers. Daarnaast gaan we ook met deze partijen in gesprek, bijvoorbeeld over voorlichting. We blijven verder ook op Europees niveau betrokken bij het adresseren van problematiek rondom cloud in sectorspecifieke regelgeving. Binnenkort zal de Minister van Economische Zaken u informeren over het aanbestedingsbeleid in relatie tot open strategische autonomie, dit naar aanleiding van de motie Van Strien.[47]

g) Laat Europese financiering ten goede komen van de Nederlandse industrie

In de initiatiefnota wordt gesproken over “de aan Nederland toegekende € 71,2 mln. Important Project of Common European Interest Cloud Infrastructure and Services (IPCEI-CIS)-gelden”. Het is belangrijk om te benoemen dat de staatssteun in het kader van een IPCEI door lidstaten zelf aan bedrijven ter beschikking wordt gesteld. Daar staatssteun in beginsel niet is toegestaan, moet hiervoor goedkeuring op basis van de IPCEI-mededeling van de Europese Commissie worden verkregen. Het gaat dus om een goedkeuring die is toegekend, niet om gelden.

De middelen die Nederland in de IPCEI CIS investeert zijn al juridisch vastgelegd in beschikkingen aan de deelnemende Nederlandse cloudconsortia. Deze zijn gealloceerd en komen daarmee ten goede aan de bedrijven en kennisinstellingen in de deelnemende consortia, met als doel om innovatie te bevorderen en zo onze afhankelijkheden te verminderen.

Daarnaast stelt het Ministerie van Economische Zaken (EZ) voor een aantal Digital Europe-calls budget beschikbaar voor nationale cofinanciering. Ook ondersteunt de Rijksdienst voor Ondernemend Nederland (RVO) bedrijven die een Europees projectvoorstel willen indienen of nodig hebben over geschikte calls binnen het Digital Europe-programma. Daarnaast biedt RVO ondersteuning aan bij aanvragen voor nationale cofinanciering. Het Ministerie van Economische Zaken heeft in totaal € 75 miljoen budget beschikbaar om cofinanciering voor Nederlandse deelnemers aan Digital Europe-projecten beschikbaar te stellen voor de jaren 2021-2029.[48]

In Europees verband wordt momenteel tevens gewerkt aan de oprichting van een European Digital Infrastructure Consortium (EDIC), om Europese samenwerking op

[46] De ADV is van toepassing op overheidsopdrachten waarbij sprake is van gerubriceerde gegevens en daarmee gevoelig materiaal, diensten of werken bestemd voor veiligheidsdoeleinden die a) betrekking hebben op gerubriceerde gegevens, b) gerubriceerde gegevens bevatten of c) gerubriceerde gegevens noodzakelijk maken.
[47] Motie van het lid Van Strien 36410-XIII-45
[48] Dit budget is beschikbaar voor de door het Ministerie van Economische Zaken geselecteerde projecten uit het Digital Europe Programma, waaronder ook projecten rondom cloud.

het terrein van digitale gemeenschapsgoederen te bevorderen. Doel is tot meer grensoverschrijdende diensten te komen die interoperabel, herbruikbaar en transparant zijn. Een van de projecten waar in dit kader aan gewerkt gaat worden is een werkplekomgeving, in samenwerking met Duitsland, Frankrijk en Estland.

h) Stimuleer cloudtechnologie in bestaande trajecten

In de agenda AI en Data van de NTS is cloudtechnologie genoemd als belangrijke basis voor de ontwikkeling en het gebruik van deze sleuteltechnologieën. Momenteel wordt deze NTS agenda uitgewerkt en hierbij zal ook de stimulering van cloudtechnologie worden meegenomen. Daarnaast wordt rekening gehouden met een ambitieuze inzet van de nieuwe Europese Commissie op het gebied van cloudtechnologie. Het kabinet zal hierbij aansluiten waar mogelijk.

i) Maak het onderwijs technologieneutraal

In de initiatiefnota wordt gesproken over de strategische kennisborging en het belang om het curriculum zo open mogelijk in te richten en technologieneutraal te maken. Ook wordt de aanbeveling gedaan om Nederlandse cloudpartijen aan te sluiten op bestaande publiek-private samenwerkingen (PPS) voor ICT opleidingen. Voor technologieneutraal onderwijs is zowel een goedwerkende leermiddelenmarkt, een divers curriculum en aansluiting van cloudpartijen van belang.

Zoals bovenstaand beschreven is de cloud problematiek binnen het onderwijs vergelijkbaar met de bredere problematiek. Wanneer er binnen de leermiddelenmarkt sprake is van samensmelting en toetreding van infrastructuur en samenwerkingsdiensten in de leermiddelenmarkt kan het ook zijn dat het curriculum wordt gerealiseerd op basis van software en applicaties van deze enkele aanbieders. Het is wenselijk dat curriculum wordt ingevuld op een manier die ICT’ers het beste voorbereid op de hun toekomstig beroep. ICT opleidingen leiden op om concepten te begrijpen en toe te passen, dit betekent dat zowel gesloten als open software gebruikt wordt als middel om te leren en niet zozeer als doel. Studenten zijn in staat om zelf een afweging te maken welke middelen zij gebruiken, op deze wijze worden ze cloud agnostisch opgeleid.

Tegelijkertijd verandert de ICT sector constant en daarmee ook de vraag van werknemers. Dit vergt van ICT opleidingen dus een combinatie van fundamentele kennis die ongeacht de technologie relevant is en adaptieve kennis die aansluit op de ontwikkelingen binnen de ICT sector. Een hoogwaardige leeromgeving en divers curriculum inrichten kost daarom ook veel middelen en inspanningen. Hierdoor specialiseren hogescholen zich meer in onderdelen van het IT domein om elkaar vervolgens op te zoeken en kennis te delen. Hoewel het gebruik van open standaarden voor software en applicaties helpt om de afhankelijkheid van enkele cloudpartijen te reduceren, is het belangrijk om de invulling van het curriculum af te wegen tegen de vaardigheidseisen van werkgevers. Deze afweging vergt een nauwe strategische samenwerking tussen cloudpartijen en opleidingsinstituten om een meer volledig aanbod van Nederlandse en Europese cloudvoorzieningen beschikbaar te maken voor ICT opleidingen.

Wegens het chronisch en toenemende tekort aan ICT'ers zijn er verschillende initiatieven ontstaan die de ICT opleidingen en cloudbedrijven stimuleren samen te werken. De Human Capital Agenda ICT (HCA ICT) zet zich in om PPS tussen het onderwijs en bedrijfsleven te realiseren. Om de eerder beschreven uitdagingen het hoofd te bieden en krapte op de ICT-arbeidsmarkt aan te pakken, zet HCA ICT zich in voor strategische samenwerkingen op nationaal, regionaal en lokaal niveau. Er bestaan 180 publiek-private samenwerkingen binnen het HCA ICT netwerk. Een voorbeeld is de Stichting Cloud IT Academy (CITA), een initiatief van cloudpartijen om samen met opleiders een duale HBO 'Cyber security & Cloud' opleiding vorm te geven in samenwerking met het bedrijfsleven. Een andere PPS is House of Digital', waarin bedrijven in de regio Amsterdam samenwerken met onderwijspartijen om opleidingen rond het thema hosting/cloud te vernieuwen. Verder werkt 'Make IT work' met bedrijven als SAP Nederland of Ultimo om werknemers om te scholen tot ICT professional, met baangarantie bij een aangesloten bedrijf.

Om onze strategische kennispositie te waarborgen is het van belang dat Nederlandse cloudpartijen nauw samenwerken met opleidingsinstituten om systeemkennis te behouden en curricula te ontwikkelen die ten goede komen aan de academische en professionele ontwikkeling van studenten. Hiervoor is niet alleen een divers curriculum nodig, maar ook juist de opschaling van succesvolle PPS, die tevens kunnen bijdragen aan het ontwikkelen van dat diverse curriculum. Binnen het 'actieplan groene en digitale banen' van het Ministerie van Economische Zaken, het Ministerie van Onderwijs, Cultuur en Wetenschap, en het Ministerie van Sociale Zaken en Werkgelegenheid wordt er binnen pijler 1 en 2 gewerkt aan de aansluiting van het onderwijs en arbeidsmarkt en het opschalen van succesvolle PPS'en.

Aanbeveling 3: "Handhaaf het eigen beleid"

a) Maak van strategische autonomie een doel op zich

Digitale open strategische autonomie is van toenemend belang. Dit geldt niet specifiek voor cloud maar is van toepassing op elke vorm van uitbesteding van processen, diensten en producten door de overheid. CIO Rijk zal het initiatief nemen te komen tot een Rijksbreed beleid voor het opnemen van autonomie bij aanbesteding. Bij dit beleid zal worden ingegaan op de risicoafweging met betrekking tot uitbestedingen. Daarnaast zal in samenwerking met vertrouwde partners in EU- en NAVO- verband onderzocht worden of de digitale risico's die we als samenleving lopen autonome digitale voorzieningen vereisen, en zo ja welke.

b) Veranker strategische autonomie in aanhangige wetgeving

In de BIO 2.0 is er geen maatregel specifiek gericht op autonomie voorzien. Wel wordt er een risicoanalyse verplicht, waarbij de aspecten informatieveiligheid, waaronder afhankelijkheden van ketenpartners, moeten worden afgewogen. Of autonomie onderdeel kan zijn van de inkoopeisen die volgen uit de BIO 2.0, de Inkoopeisen Cybersecurity Overheid (ICO), zal worden afgewogen in het proces voor opname van nieuwe normen in het aankomende jaar.

c) Stel de CIO Rijk verantwoordelijk

Er wordt momenteel gewerkt aan een herziening van het besluit CIO-stelsel. Onderdeel van de herziening is het versterken van de coördinerende rol van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en de positie van de CIO Rijk. De aanbeveling zal worden meegenomen in deze herziening. Hierbij zal worden bepaald welke bevoegdheden passend zijn om de CIO Rijk een stevigere rol te geven met betrekking tot het sturen op nakomen van beleid, kaders en richtlijnen waarvan is afgesproken dat deze noodzakelijk zijn om de digitale autonomie van de Rijksoverheid te versterken.

d) Maak duidelijk hoe bestaande kaders worden nageleefd

Door de Rekenkamer, de Auditdienst Rijk en CIO Rijk zijn onderzoeken uitgevoerd naar het Rijksbreed Cloudbeleid en de naleving hiervan. De rapportage van de ADR en de evaluatie uitgevoerd door CIO Rijk is aan u toegestuurd.[49] De AR zal haar rapport naar verwachting begin 2025 publiceren.

e) Stel vlotte exitstrategieën als randvoorwaarde

Het is voor een organisatie essentieel om vóór een cloudmigratie een exitstrategie te ontwikkelen bij het gebruik van een cloudleverancier, als onderdeel van een robuust risicomanagement en bedrijfscontinuïteitsbeheer. Bedrijfscontinuïteit is van cruciaal belang voor alle entiteiten en sectoren, ongeacht of zij onder de reikwijdte van de NIS2-doelgroepen vallen. Een entiteit dient, op basis van een zorgvuldige risicoanalyse en een kostenafweging, zelf te bepalen in welke mate zij gebruik wenst te maken van een clouddiensten. Het opstellen van een exitstrategie kan tevens van belang zijn bij het gebruik van andere producten en diensten waarop de entiteit afhankelijk is. Dit is noodzakelijk aangezien elke door een derde partij geleverde dienst op enig moment kan worden beëindigd, kosten kunnen worden verhoogd, of leveranciers failliet kunnen gaan.

De implementatie van de Dataverordening faciliteert de migratie tussen clouddiensten, waarbij gestreefd wordt naar een verhoogde interoperabiliteit van deze diensten. Daarnaast biedt de verordening betere bescherming voor afnemers tegen contractuele onevenwichtigheden. In de eerdergenoemde publicatie van het NCSC wordt ook een advies gegeven over het opstellen van een exit-plan.

f) Maak open standaarden de norm

De Nederlandse overheid hanteert reeds beleid voor het gebruik van open standaarden in haar ICT-systemen. Het gebruik van open standaarden is verplicht voor ICT-diensten of ICT-producten waarbij de aanschaf een waarde vertegenwoordigt van ten minste € 50.000. Voor sommige standaarden duurt het moment van een volgende aanschaf echter te lang, waardoor de publieke dienstverlening te veel risico loopt. Er worden dan streefbeeldafspraken gemaakt om de adoptie te versnellen. Indien dat tot onvoldoende resultaat leidt, dan kan een standaard in aanmerking komen voor wettelijke verplichting op grond van de Wet digitale overheid (Wdo).

Open standaarden kunnen door iedereen gebruikt worden waardoor de overheid leveranciersonafhankelijk kan bevorderen. Het Forum Standaardisatie, het

[49] Kamerbrief evaluatie Rijksbreed cloudbeleid | Kamerstuk | Rijksoverheid.nl en Bevindingen onderzoeksopdracht 'Evaluatie public cloudbeleid Rijksoverheid' | Rapport | Rijksoverheid.nl

standaardisatie adviesorgaan van en voor de overheid, hanteert een lijst van open standaarden zoals de aanbevolen standaarden, standaarden met een “Pas toe of leg uit’- verplichting en in sommige gevallen worden open standaarden ook wettelijk verplicht.

Directoraat-generaal
Economie en Digitalisering
Directie Digitale Economie

Ons kenmerk
DGED-DE / 95898883

Bijlage II – Beschrijving van de problematiek op de cloudmarkt

Net als de opstellers van de initiatiefnota signaleert het kabinet het dilemma dat er diverse problemen spelen op de markt voor clouddiensten. Deze problemen zorgen ervoor dat Europese cloudaanbieders niet eerlijk en effectief kunnen concurreren met de hyperscalers en dat gebruikers onvoldoende keuzevrijheid ervaren in het gebruik van clouddiensten. De problemen zijn het gevolg van oorzaken die deels uniek zijn en deels overlappen.

Eerder zijn in diverse analyses, zoals onder andere de agenda DOSA en de marktstudie naar clouddiensten van de ACM[50], uitgebreid de onderliggende oorzaken voor het huidige functioneren van de markt voor clouddiensten uiteengezet. In deze bijlage presenteren we een gedetailleerdere beschrijving van de huidige problematiek op de cloudmarkt is opgenomen in een bijlage bij deze brief.

1. Concurrentiepositie Europese bedrijven op markt voor clouddiensten

Een voorname oorzaak voor de slecht functionerende cloudmarkt is de verregaande concentratie aan de aanbodzijde van de markt. Vier grote niet-Europese bedrijven domineren op dit moment wereldwijd de markt voor public cloudinfrastructuur: Amazon, Microsoft, Google en het Chinese Alibaba (vooral actief op de Chinese markt).[51] Deze bedrijven worden vaak als hyperscalers aangeduid.

In de Nederlandse markt beschikken met name de aanbieders Amazon en Microsoft over grote geconsolideerde marktaandelen, zoals ook in andere Europese markten het geval is. De ACM verwacht dat de consolidatie in de markt voor clouddiensten verder doorzet als gevolg van onder meer schaalvoordelen en netwerkeffecten.[52] Een belangrijke reden waarom Europese aanbieders niet in staat zijn om op gelijke voet te concurreren is de overweldigende schaal die de hyperscalers hebben voor investeringen in het vernieuwen van hun clouddienstverlening en onderliggende infrastructuur. Als gevolg van deze schaal kunnen hyperscalers een dienstenaanbod leveren dat qua integraliteit op dit moment superieur is. De grote aanbieders profiteren dus sterk van hun wereldwijde aanwezigheid en technologische voorsprong.

Zoals ook in de initiatiefnota wordt geschetst is het in een dergelijke situatie voor kleinere spelers moeilijk om effectief met grote geïntegreerde aanbieders te concurreren. Nederlandse bedrijven en consumenten die de volledigheid van diensten zoals aangeboden door de hyperscalers wensen, zijn als afnemers van clouddiensten grotendeels afhankelijk van grote niet-Europese hyperscalers.

De beschreven marktproblematiek verschilt per cloudlaag: de markt voor SaaS-diensten is relatief heterogeen met veel productdifferentiatie en daarmee meer ruimte voor diversificatie en specialistisch aanbod van kleinere aanbieders. PaaS- en IaaS-diensten hebben een homogenere aard, waardoor de dominante

[50] Marktstudie clouddiensten | ACM.nl
[51] Staat van de Europese Unie 2023 | Tweede Kamer der Staten-Generaal
[52] Marktstudie clouddiensten | ACM.nl

marktpartijen hier op schaal kunnen concurreren door hun netwerkvoordelen. In haar rapport stelt ACM dat met name op deze twee sub-markten de grote cloudaanbieders een sterke marktpositie hebben.[53] Er is hier sprake van een hoge afhankelijkheid van keuzes van de leverancier met weinig invloed van de vragende partij. In dit segment hebben de eerder genoemde hyperscalers een (voorlopig) niet in te halen voorsprong met uitzondering van enkele maatwerkdiensten. Gebruikers van dergelijke clouddiensten kunnen daarom niet of nauwelijks de afweging maken op basis van afhankelijkheid of autonomie, omdat de sterke positie van de hyperscalers hen weinig alternatieven biedt.

Het sterk geconcentreerde marktaanbod is op zichzelf problematisch voor onze concurrentiepositie en digitale open strategische autonomie, maar heeft daarnaast diverse negatieve afgeleide effecten, bijvoorbeeld met betrekking tot het innovatievermogen van de Europese cloudaanbieders en risico's voor de concurrentie in opkomende digitale markten, zoals AI.

Innovatievermogen cloud
Het is te verwachten dat de consolidatie in de markt voor clouddiensten verder doorzet als gevolg van onder meer schaalvoordelen en netwerkeffecten. Dit kan op den duur negatieve effecten hebben op het innovatievermogen van de bredere cloudsector.

Hoewel kennis en technologie in Europa aanwezig zijn, worden deze in grote mate benut door niet-Europese bedrijven. Het is voor kleinere spelers namelijk moeilijk om effectief met grote geïntegreerde aanbieders te concurreren.[54] Zo kunnen Europese cloudaanbieders, mede als gevolg van de gebrekkige marktwerking, niet altijd meegaan in het groei- en investeringstempo van de grote cloudaanbieders. Hierdoor worden afhankelijkheden op het gebied van innovatie versterkt.

Daarnaast hebben relatief kleine aanbieders vaak geen eigen geïntegreerd aanbod van cloudinfrastructuurdiensten tot cloudapplicaties, waardoor ze hun innovatieve clouddiensten doorgaans aanbieden via de infrastructuur van een van de grote cloudaanbieders. Hierdoor zijn de kleinere partijen verknoopt aan en afhankelijk van de infrastructuur van die grote partij. Als gevolg hiervan zijn deze kleinere partijen ook aantrekkelijke kandidaten om over te nemen voor de grote geïntegreerde cloudaanbieders. Bijkomend effect is dat de innovaties van potentieel concurrerende uitdagers dan worden geabsorbeerd in het geïntegreerde aanbod van de grote cloudaanbieders.[55] Ook kan dit resulteren in een tekort aan gekwalificeerd personeel in eigen cloudinfrastructuur binnen Europa.[56] De marktproblematiek belemmert dus innovatie door kleinere aanbieders van clouddiensten.

Het lijkt echter zo te zijn dat de genoemde barrières voor een optimaal werkende cloudmarkt negatief bijdragen aan de concurrentie op de markt, wat de innovatieprikkel voor de leidende clouddiensten beperkt. Het beschikbare aanbod

[53] Marktstudie clouddiensten | ACM.nl
[54] Marktstudie clouddiensten | ACM.nl
[55] Marktstudie clouddiensten | ACM.nl
[56] The Future of European Competitiveness, Part B

van clouddiensten is zeker innovatief te noemen, maar de kwaliteit van innovatie is optimaal wanneer er sterke concurrentie tussen aanbieders zou zijn op een gelijk speelveld. De innovatie en marketing dient in de huidige marktsituatie met name om klanten te werven die nog geen gebruik maken van clouddiensten, niet concurrentiedoeleinden. Ook in de huidige situatie met vendor lock-in hebben cloudproviders nog steeds een prikkel om te innoveren, namelijk om de mogelijkheden voor het genereren van extra inkomsten uit hun cloudservices te vergroten. Als zodanig is het echter onwaarschijnlijk dat deze aanwezigheid van innovatie op zichzelf een goedwerkende en innovatieve markt impliceert[57]. Meer onderzoek is echter in bredere zin nodig om te kunnen concluderen dat het innovatievermogen op de cloudmarkt niet wordt beperkt door de bestaande marktstructuren.

Concurrentiepositie in de AI-markt
Bij de inzet, maar vooral bij de training van AI-modellen zijn grote hoeveelheden aan rekenkracht en dataopslag nodig. De cloud fungeert hierbij als katalysator en biedt on-demand de mogelijkheid tot vrijwel onbeperkte bronnen, zodat organisaties kostenefficiënt en snel kunnen opschalen. De innovatiecyclus wordt versneld door deze flexibiliteit, omdat experimenten effectiever en efficiënter kunnen worden doorgevoerd. Schaalbare rekenkracht en dataopslag zijn elementen die de cloud een belangrijke bouwsteen maken voor ontwikkelaars, aanbieders en gebruikers van AI-modellen en systemen.

In de relatie tussen cloud en AI leidt de huidige marktproblematiek tot risico's op het gebied van concurrentie. Zo lopen er verschillende onderzoeken op Europees niveau naar exclusieve partnerschappen tussen sommige hyperscalers en aanbieders van generatieve AI. De toenemende interesse in generatieve AI modellen en toepassingen versterkt de afhankelijkheid voor aanbieders van generatieve AI van hyperscalers, omdat alternatieven veelal ontbreken door de hoge investeringen die gepaard gaan met de infrastructuur die nodig is voor het trainen van grote en geavanceerde (generatieve) AI-modellen.

Gezien de (potentiële) economische en maatschappelijke impact van grote geavanceerde AI-modellen, heeft de Europese Commissie begin dit jaar de 'AI-fabrieken' geïntroduceerd om het concurrentievermogen en innovatievermogen van het Europese AI-ecosysteem te versterken.[58] De AI-fabrieken zullen een netwerk vormen van Europese AI-supercomputers die toegankelijk worden gemaakt voor Europese AI-bedrijven en wetenschappers om grootschalige AI-modellen te kunnen trainen met een grote hoeveelheid rekenkracht. Het kabinet verkent momenteel de mogelijkheden voor een dergelijke AI-faciliteit met AI-geoptimaliseerde supercomputer in Nederland.[59]

2. Gebrek aan keuzevrijheid voor eindgebruikers

Waar het vorige probleem voornamelijk voortkomt uit oorzaken aan de aanbodzijde van de markt voor clouddiensten, spelen er ook problemen aan de vraagzijde van de markt: afnemers hebben beperkte keuzevrijheid op de markt

[57] Cloud services market investigation - Competitive landscape working paper (23 May 2024)
[58] BNC-fiche Verordening supercomputerinitiatief kunstmatige intelligentie (COM(2024) 29)
[59] Kamerstuk 26643, nr. 1180

voor clouddiensten. Voor een deel zijn is dit het gevolg van de hoge mate van concentratie op de markt: organisaties die een geïntegreerd pakket aan clouddiensten op de SaaS, PaaS en IaaS lagen willen afnemen, zijn grotendeels afhankelijk van het aanbod van grote niet-Europese technologiebedrijven.

Een ander belangrijk obstakel voor keuzevrijheid is de *vendor lock-in* die afnemers kunnen ervaren. Er is sprake van lock-in als cloudaanbieders door middel van belemmeringen de mogelijkheden van afnemers beperken om over te stappen naar een andere cloudaanbieder. Aan deze lock-in liggen verschillende oorzaken ten grondslag, zoals ook ACM in haar marktstudie gedetailleerd heeft uitgewerkt.[60] Overstapbelemmeringen kunnen technisch, organisatorisch en financieel van aard zijn. Generiek mededingingsrecht biedt veelal niet de instrumenten om dergelijke problemen op te lossen. De technische en organisatorische belemmeringen zijn in grote mate gerelateerd aan beperkte dataportabiliteit en interoperabiliteit.

Gebrekkige dataportabiliteit
Dataportabiliteit betreft de mogelijkheid om gegevens over te zetten van één clouddienst naar een ander. Door de sterke verwevenheid tussen de verschillende clouddiensten en bedrijfsprocessen van een organisatie kost het veel tijd en werk om (alle) diensten te ontvlechten en opnieuw in te richten. Ook is er niet voor elk product een passend alternatief, door het uiteenlopende productaanbod bij de verschillende cloudaanbieders. Tot slot, hoewel Application Programming Interfaces (API's) helpen bij het borgen van dataportabiliteit, kunnen gegevens door het gebruik van verschillende (niet openbare) API's en standaarden, niet altijd (goed) worden overgezet, waardoor dataportabiliteit niet altijd mogelijk is.

Gebrekkige interoperabiliteit
Interoperabiliteit is de mogelijkheid om herhaaldelijke en gelijktijdig verschillende clouddiensten te gebruiken en met elkaar te verbinden, ook wanneer deze van verschillende cloudaanbieders zijn. Een vaak genoemde oplossing om lock-in te voorkomen is de inzet van multi-cloud. Hierbij nemen gebruikers clouddiensten af van verschillende aanbieders en verbinden ze deze met elkaar. Dit kan een effectieve manier zijn om lock-in bij en afhankelijkheid van één aanbieder te voorkomen. In de praktijk zijn de mogelijkheden om door middel van multi-cloud lock-in te voorkomen echter beperkt.[61] Dit is het gevolg van het feit dat er belemmeringen bestaan voor interoperabiliteit tussen clouddiensten van verschillende aanbieders. Diensten van verschillende aanbieders kunnen vaak niet (makkelijk) met elkaar worden gekoppeld, omdat grote aanbieders gebruik maken van eigen standaarden die niet compatibel zijn. Hierdoor kunnen deze diensten niet effectief met elkaar communiceren en samenwerken.

Gebruikers zijn bij het kiezen van nieuwe diensten, die moeten samenwerken met bestaande diensten, in de praktijk vaak beperkt tot dezelfde aanbieder of een derde partij die gebruik maakt van een compatibele cloudinfrastructuur. Gebruikers hebben hierdoor minder vrijheid om diensten van verschillende aanbieders te combineren. Dit leidt tot hogere overstapdrempels en beperkt de

[60] Marktstudie clouddiensten | ACM.nl
[61] Marktstudie clouddiensten | ACM.nl, zie paragraaf 2.5 en 6.2.

concurrentie tussen cloudaanbieders op het niveau van dienstverlening. Gebrekkige interoperabiliteit versterkt zo vendor lock-in.

Financiële overstapbelemmeringen
Naast technische en organisatorische obstakels zijn er ook financiële overstapbelemmeringen. Deze ontstaan met name door de tariefstructuur die veel cloudaanbieders hanteren. Deze tariefstructuur is complex en niet transparant: voor elke handeling, opgeslagen Gigabyte of seconde rekenkracht wordt betaald. Dat zorgt voor onvoorspelbaarheid over de uiteindelijke totale kosten van gebruik van clouddiensten. Verder kan een eventuele overstap ook leiden tot een gecontroleerde groei van kosten.

Daarnaast is het plaatsen van data in de cloud van een cloudaanbieder in veel gevallen gratis (ingress fees), maar worden er wel kosten gerekend voor het verplaatsen van data uit de cloud, bijvoorbeeld naar een andere aanbieder (egress fees). Deze laatste problematiek lijkt recentelijk al te worden verminderd door de drie grootste marktpartijen, door deze kosten niet langer door te berekenen.[62]

Al met al wordt de marktconcentratie aan de aanbodzijde door vendor lock-in verder versterkt: financiële overstapdrempels en technische barrières zoals gebrekkige dataportabiliteit en interoperabiliteit versterken het concurrentievoordeel van leidende marktpartijen.

3. Publieke belangen, databescherming en rechtsmachtconflicten

De commercialisering van de digitale leefomgeving door grote technologiebedrijven, in combinatie met hun marktmacht, kan een effect hebben op de manier waarop publieke waarden zoals privacy, transparantie en keuzevrijheid worden gehandhaafd. De commerciële belangen van deze bedrijven kunnen botsen met publieke waarden. Dit is op zich niet inherent problematisch, maar door de grote mate van marktmacht van grote technologiebedrijven kan dit leiden tot situaties waarin publieke waarden ondergeschikt worden gemaakt aan commerciële doeleinden met nadelige gevolgen voor de samenleving als geheel. Het blijft van belang dat de juiste afwegingen gemaakt worden bij het inzetten van public clouddiensten. Daarbij is het belangrijk dat de departementen binnen de

rijksoverheid hun keuzes vastleggen in de departementale cloudstrategie.

Databescherming
Voor een evenwichtige afweging van publieke waarden is het van belang dat data worden beschouwd als een ‘asset’, ofwel waardevolle bron. Net zoals machines,

Digitale gemeenschapsgoederen als mogelijke oplossing
Digitale gemeenschapsgoederen, zoals open source software en open data, bieden een model dat is gebaseerd op gedeeld eigendom en collectieve besluitvorming, waarbij publieke waarden centraal staan. Dit model kan mogelijk helpen de afhankelijkheid van niet-waardengedreven aanbieders te verkleinen en biedt een democratischer en transparanter alternatief voor commerciële cloudoplossingen die momenteel door hyperscalers worden gedomineerd.

[62] Amazon AWS Joins Google Cloud In Removing Egress Costs (forrester.com)

gebouwen en geld horen data strategisch te worden beheerd, beschermd en benut. De cloud is niet alleen een technische kwestie en een efficiëntiemaatregel, maar cloud als technisch hulpmiddel kan impact hebben op publieke belangen: de nationale veiligheid, grondrechten en gevoelige gegevens van en over Nederlandse burgers moeten worden beschermd. En toegang tot data in de cloud die nodig zijn voor het uitvoeren van overheidstaken en dienstverlening aan burgers en bedrijven moet worden geborgd. Hierbij moet ook speciale aandacht gegeven worden aan gerubriceerde informatie. Het uitgangspunt is en blijft dat staatsgeheim gerubriceerde informatie nooit de public cloud in mag.

Data-classificatie verdient in dit kader bijzondere aandacht, aangezien het beoordelen van data op gevoeligheid en waarde bepaalt hoe goed de beveiliging en toegankelijkheid moet zijn. Dit hoort bij een gedegen aanpak door organisaties voor het beheer van data, waarbij ze de waarde ervan maximaliseren en de risico's minimaliseren. Indien risicovolle strategische afhankelijkheden ontstaan of de nationale veiligheid in het geding kan komen dienen mitigerende maatregelen genomen te worden.

De huidige problematiek op de cloudmarkt als gevolg van marktdominantie kan hierbij belemmerend werken. Door de beperkte keuze op de cloudmarkt is het namelijk niet altijd mogelijk voor een datahouder om een clouddienst af te nemen die enerzijds passend is bij het benodigde veiligheidsniveau voor de vastgestelde dataclassificatie, en anderzijds de gewenste functionaliteit biedt om de data ook optimaal te kunnen benutten.

Rechtsmachtconflicten
Een belangrijke oorzaak voor zorgen over databescherming in de cloud zijn rechtsmachtconflicten tussen staten of machtsblokken. Diverse landen kennen wet- en regelgeving met extraterritoriale werking die medewerking aan veiligheidsdiensten verplicht, zoals de CLOUD Act in de VS.[63] Dergelijke wet- en regelgeving kan, in bepaalde gevallen mogelijk leiden tot ongewenste toegang tot Nederlandse gegevens wanneer dit conflicteert met regelgeving als de AVG. Hier is uw Kamer eerder over geïnformeerd[64].

Op verzoek van het Nationaal Cyber Security Centrum (NCSC) heeft advocatenkantoor 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.[65]

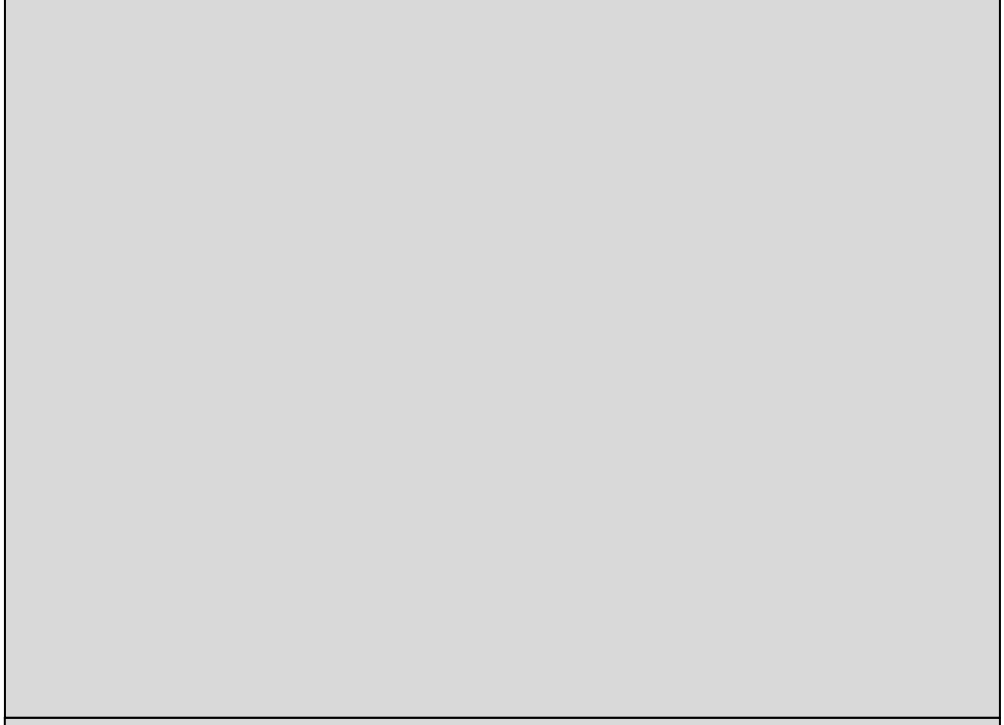
Zorg
Cloudoplossingen worden ook in de zorg steeds vaker gebruikt. Effectief gebruik van cloudoplossingen kan bijdragen aan administratieve lastenverlichting, verminderen van de werkdruk en betere informatiedeling tussen verschillende medische teams. Daarmee kan de betaalbaarheid, toegankelijkheid en kwaliteit van de zorg worden vergroot.

Maar het gebruik van cloudoplossingen brengt ook risico's met zich mee, zoals ook geschetst in de initiatiefnota. Aan de ene kant is het van belang dat er door zorgmedewerkers op een juiste manier wordt omgegaan met de cloud, en dat de cloud (technisch) op de juiste manier wordt ingeregeld. En aan de andere kant is de in de initiatiefnota geschetste afhankelijkheid van een beperkt aantal clouddiensten voor bedrijven die op het gebied van onderwijsapplicaties en leermiddelen opereren, samen worden gevoegd. Ook bijgeleverde bedrijven die actief zijn binnen de infrastructuur of aanverwante diensten zijn vaak onderwijsapplicaties en leermiddelen. Tot slot zien we ook dat zowel scholen als bedrijven uit de leermiddelenmarkt vaak bouwen op de cloud en ICT-platforms van grote aanbieders, waardoor de afhankelijkheid van deze

Cloudproblematiek in het onderwijs en de zorg

Zoals Amazon, Microsoft en Google door verschillende ontwikkelingen een steeds grotere plaats innemen in het Nederlandse onderwijslandschap.

En ontstaan er nieuwe samenwerkingen tussen (Nederlandse) bedrijven uit de leermiddelenmarkt en grote (internationale) techbedrijven. Daarnaast zien we dat bedrijven die op het gebied van onderwijsapplicaties en leermiddelen opereren, samen worden gevoegd. Ook bijgeleverde bedrijven die actief zijn binnen de infrastructuur of aanverwante diensten zijn vaak onderwijsapplicaties en leermiddelen. Tot slot zien we ook dat zowel scholen als bedrijven uit de leermiddelenmarkt vaak bouwen op de cloud en ICT-platforms van grote aanbieders, waardoor de afhankelijkheid van deze



Directoraat-generaal
Economie en Digitalisering
Directie Digitale Economie

Ons kenmerk
DGED-DE / 95898883

[66] Staat van de Europese Unie 2023 | Tweede Kamer der Staten-Generaal
[67] Policy_brief_Cloud_sovereignty.pdf (clingendael.org)