
Strategische digitale autonomie en het Rijksbreed cloudbeleid

Samenvatting

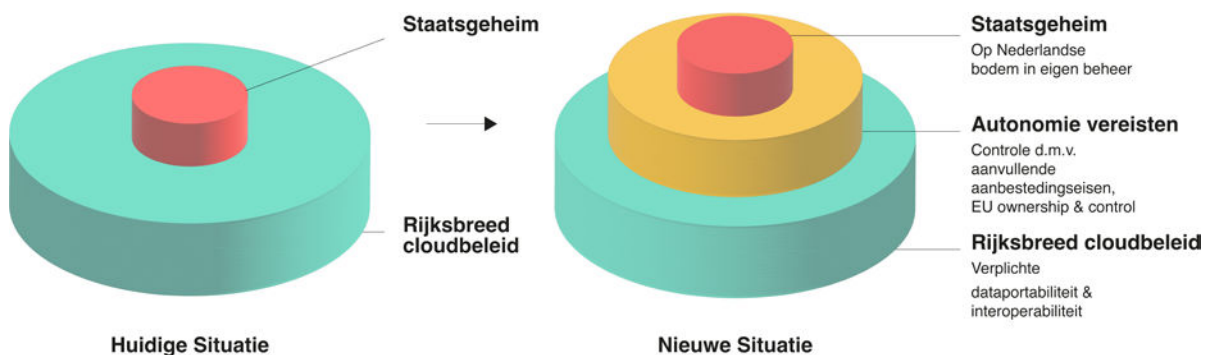
De afgelopen tijd is snel duidelijk geworden dat onze digitale afhankelijkheden op het gebied van cloud met flinke risico's gepaard gaan. Het is niet langer ondenkbaar dat toegang tot clouddiensten bij de overheid en in kritieke sectoren ingezet wordt als geopolitiek drukmiddel. De urgentie om deze risicovolle afhankelijkheden af te bouwen is groot. Er moeten daarom nu, per direct, concrete stappen gezet worden.

Als coalitie van Nederlandse bedrijven en organisaties in de digitale infrastructuur, willen we met deze position paper een bijdrage leveren aan de vormgeving van cloudbeleid dat de hierboven geschetste risicovolle afhankelijkheden snel minimaliseert. We schetsen daartoe een haalbare weg vooruit. Daarbij benadrukken we de urgentie én de mogelijkheden om nu actie te ondernemen. We suggereren het volgende:

- 1 Creëer een nieuwe categorie van clouddiensten voor gevoelige overheidsdata, essentiële overheidsdiensten en kritieke fysieke infrastructuur waaraan extra aanbestedingseisen worden gesteld op het gebied van digitale strategische autonomie.

Daarvoor zijn de volgende stappen van belang:

- Bepaal welke overheidsdata als gevoelige data geclassificeerd moeten worden, welke overheidsdiensten als essentieel en welke fysieke infrastructuur als kritiek.
- Inventariseer welke bestaande Nederlandse en Europese 'cloudneutrale' platformen kunnen worden opgeschaald voor deze nieuwe categorie. Enkele voorbeelden hiervan staan verderop in deze paper.
- Voor de juridische onderbouwing van deze nieuwe categorie kan een beroep worden gedaan op uitzonderingen op het gebied van nationale veiligheid in de General Procurement Agreement en internationale handelsverdragen. Zo kunnen deze data, diensten en infrastructuur ondergebracht worden bij Nederlandse of Europese bedrijven door middel van eisen aan eigendomsverhoudingen, governance en hoofdkantoorlocatie.
- Leer van, en bouw voort op, bestaande praktijken van Frankrijk, Estland en Luxemburg die al succesvol soevereiniteitseisen toepassen.
- Introduceer een keurmerk voor Nederlandse en Europese partijen die aan de juiste voorwaarden voldoen en creëer een loket waar overheidsinkopers aanbieders kunnen vinden die aan dit keurmerk voldoen.¹



Schematische weergave van de huidige situatie en de in dit paper voorgestelde situatie

- 2 Stimuleer keuzevrijheid en eerlijke concurrentie in de cloudmarkt door voor niet-kritieke clouddiensten dataportabiliteit en interoperabiliteit verplicht te stellen en door gedegen exit-strategieën te implementeren. Dit voorkomt bovendien het risico van vendor lock-in, waarbij migratie naar een andere leverancier nagenoeg onmogelijk is door complexiteit en/of hoge kosten.
- 3 Tot slot is het belangrijk om te benadrukken dat de discussie over de regierol binnen de overheid met betrekking tot de inkoop van clouddiensten cruciaal is voor succesvol cloudbeleid op de lange termijn. Tegelijkertijd kunnen we niet wachten op de voltooiing van die discussie alvorens concrete (bovengenoemde) stappen te nemen: de urgentie is daarvoor te hoog.

¹ Bij voorkeur worden eisen op Europees niveau via ENISA vastgesteld.

Grote risico's, hoge urgentie

De oorlog in Oekraïne, het Draghi-rapport en de veranderende geopolitieke verhoudingen sinds de start van de tweede termijn van President Trump, benadrukken de noodzaak om onze strategische autonomie in het digitale domein snel te versterken. De inzet van digitale afhankelijkheden als geopolitiek drukmiddel is nu een reële dreiging.

Vele overheidsorganisaties en organisaties in kritieke sectoren zijn voor een belangrijk deel digitaal afhankelijk van cloudaanbieders die hun hoofdzetel buiten de EU hebben. Deze dominantie van enkele niet-Europese cloudbedrijven in het IT-landschap van zo veel kritieke (overheids)organisaties maakt dat Nederland in een kwetsbare positie verkeert. De risico's van onze digitale afhankelijkheid van slechts enkele niet-Europese leveranciers zijn divers en verstrekkend:

Risico's voor nationale veiligheid

Risico's voor nationale veiligheid, bijvoorbeeld wanneer essentiële platformen van de overheid niet beschikbaar worden of daarmee kan worden bedreigd.

Risico's voor concurrentiekracht

Beperking van de Europese concurrentiekracht, economische groei en werkgelegenheid en verlies van innovatiepotentie door gebrekkige mogelijkheden voor doorgroei van startups en scaleups. Daarbij is het belangrijk om op te merken dat alle grote Amerikaanse cloud-bedrijven door de Amerikaanse overheid worden geholpen met miljarden contracten, zoals het Pentagon-contract van 9 miljard voor AWS, Microsoft, Google en Oracle en soortgelijke contracten van de CIA en andere overheidsdiensten die tientallen miljarden waard zijn.² Dergelijke ondersteuning ontbreekt in de EU en dat heeft effect op het concurrentievermogen van Nederlandse en Europese bedrijven.

Hoog risico vendor lock-in

Digitale monocultuur leidt tot een slechte onderhandelingspositie en vendor lock-in. Het wisselen van cloudleverancier is hierdoor vrijwel onmogelijk, of gaat op zijn minst gepaard met zeer hoge kosten.

Risico's van verdwijnen kennis en kunde

De opleiding van jonge IT'ers wordt steeds eenzijdiger, want kennis is steeds verder beperkt tot niet-Europese technologie. Beperkte kennis van alternatieve technieken leidt tot nog grotere vendor lock-in. Kennis binnen overheden wordt hierdoor ook eenzijdig en afhankelijkheden van externe leveranciers leiden tot continuïteitsrisico's.

De Algemene Rekenkamer³ en de Auditdienst Rijk⁴ waarschuwen dan ook voor mogelijke maatschappelijke ontwrichting en voor risico's voor de continuïteit van overheidsdienstverlening.

Tegelijkertijd biedt cloudtechnologie, mits verstandig ingezet, enorme kansen voor betere overheidsdienstverlening, innovatie en kostenefficiëntie. Nederlandse bedrijven leveren nu al essentiële clouddiensten aan overheden. We kunnen profiteren van deze voordelen én tegelijk onze afhankelijkheid van niet-Europese aanbieders verminderen door te bouwen aan een krachtige Nederlandse en Europese cloudsector.

2 <https://www.clingendael.org/publication/nederland-en-de-eu-zet-op-cloudsoevereiniteit>

3 <https://www.rekenkamer.nl/publicaties/rapporten/2025/01/15/het-rijk-in-de-cloud>

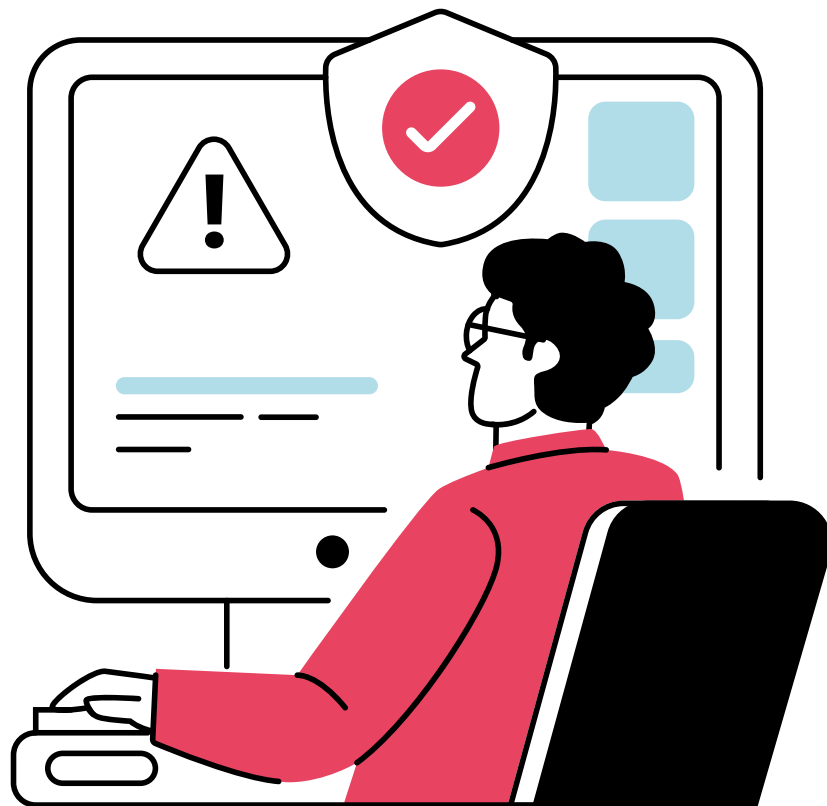
4 <https://open.overheid.nl/documenten/4a4f7ec7-a241-46bc-94a5-cb4c1587a974/file>

Krachtig signaal

De Tweede Kamer⁵ heeft bij het debat over IT-migraties naar het buitenland een krachtig signaal afgegeven. Het cloudbeleid van de overheid moet drastisch op de schop. Ook de Algemene Rekenkamer concludeert dat de Rijksoverheid ondoordacht is gaan werken in de cloud en is bezorgd over de risico's voor de dienstverlening aan burgers en bedrijven en mogelijke maatschappelijke ontwrichting.

De Algemene Rekenkamer beveelt aan om meer diensten naast het beheer van staatsgeheimen uit te sluiten van public cloud gebruik. Auditdienst Rijk raadt het kabinet aan te werken aan betere exit-strategieën voor cloudgebruik. Zij waarschuwt voor 'dreigingsaantrekkende werking' als gevolg van de afname van clouddiensten van een beperkt aantal bedrijven en noemt expliciet Microsoft 365. De Tweede Kamer stelt dat afhankelijkheden voor de continuïteit van de Nederlandse overheid afgebouwd moeten worden en dat er soevereiniteitseisen gesteld moeten worden bij de opslag van gevoelige gegevens en vitale infrastructuur.

Als antwoord daarop heeft het kabinet aangegeven het cloudbeleid te willen herzien en een "soevereine overheidscloud" op te willen zetten "om de kloof te overbruggen voor digitale dienstverlening waarvoor het gebruik van public cloud onwenselijk is".



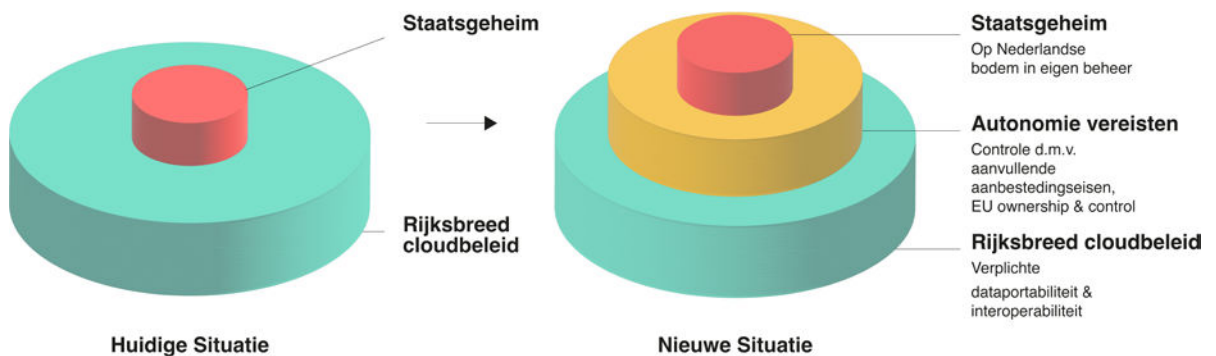
5 https://www.tweedekamer.nl/kamerstukken/plenaire_verslagen/kamer_in_het_kort/migraties-van-overheids-ict-naar-het-buitenland

De weg vooruit

Het doel is helder en de urgentie kan niet groter. De risico's van onze digitale afhankelijkheid zijn onacceptabel. We moeten nú aan de slag met het vergroten van onze strategische digitale autonomie met concrete acties op de korte, middellange en lange termijn. De noodzaak voor een 'soevereine cloud' kan niet los gezien worden van het type data en diensten die een hogere mate van autonomie vereisen. Het is belangrijk om hier de juiste accenten in aan te brengen.

Om op de korte termijn tot concrete acties te komen stellen wij de volgende aanpak voor:

- Creëer een nieuwe categorie van gevoelige overheidsdata (zoals gerubriceerde informatie, vertrouwelijke communicatie en bijzondere persoonsgegevens), essentiële overheidsdiensten (belastingen, sociale zekerheid, DigiD, etc.) en kritieke fysieke infrastructuur (het Diginetwerk, stormkeringen, sluizen, kritieke transport infrastructuur en ziekenhuizen) waar aanvullende aanbestedingseisen aan gesteld worden zodat ze ondergebracht kunnen worden bij Nederlandse of Europese bedrijven en zo immuun blijven voor buitenlandse wetgeving of inmenging.
- Omdat het hier gaat om gevoelige overheidsdata, essentiële overheidsdiensten en kritieke fysieke infrastructuur kan een beroep gedaan worden op uitzonderingen op het gebied van nationale veiligheid in internationale verdragen, zoals andere Europese landen reeds succesvol doen.



Schematische weergave van de huidige situatie en de in dit paper voorgestelde situatie

- Leer van de aanpak van Defensie, die als oefening in een 24-uurs actie alle data uit Azure naar lokaal en weer naar AWS hebben gemigreerd – als bewijs dat de uitvoering van een “Plan B bij calamiteiten” mogelijk is.
- Introduceer een keurmerk voor Nederlandse en Europese partijen die aan de juiste voorwaarden voldoen om clouddiensten voor deze nieuwe categorie data, diensten en infrastructuur te leveren. Op basis van het keurmerk kunnen de vragende en aanbiedende partijen ook samenwerken aan juridische aspecten zoals een raamovereenkomst waar Nederlandse (en eventueel Europese) bedrijven op in kunnen tekenen, zodat overheidsinstanties niet telkens nieuwe onderhandelingen hoeven aan te gaan om diensten af te nemen bij Nederlandse of Europese aanbieders.
- Creëer daarnaast een loket waar inkopers van de overheid aanbieders kunnen vinden die voldoen aan het keurmerk. Zodoende heeft de overheid via één loket toegang tot aanbieders waarvan het de garantie heeft dat ze voldoen aan een aantal van tevoren gedefinieerde eisen. Dat betekent dat overheden kunnen aankloppen bij één loket en daarachter een aantal partijen kunnen vinden die een aanbod hebben dat past bij hun behoefte.

Een praktische aanpak die tegemoetkomt aan bestaande aanbevelingen en zorgen

Door op deze manier de aangekondigde soevereine overheidscloud én bestaande kritieke digitale overheidsinfrastructuur vorm te geven, kan tegemoetgekomen worden aan de aanbevelingen van de Rekenkamer over het uitsluiten van bepaalde diensten van public cloud gebruik. Ook wordt zo tegemoetgekomen aan de aanbevelingen van de Auditdienst Rijk over het concreet vormgeven van exit-strategieën én aan de aangenomen moties van de Tweede Kamer wat betreft het afbouwen van risicovolle afhankelijkheden en het stellen van soevereiniteitseisen aan vitale overheids-IT.

Met deze aanpak worden ook de zorgen van het kabinet met betrekking tot juridische aspecten die voortvloeien uit internationale afspraken geaddresserd. Het kabinet stelt in haar reactie op de drie moties die waren ontraden maar toch zijn aangenomen door de Tweede Kamer dat er “geen mogelijkheden [zijn] om overheidsopdrachten alleen maar aan Europese en/of Nederlandse ondernemers te gunnen. Dit is juridisch niet mogelijk door de verplichtingen die voortvloeien uit de Government Procurement Agreement (GPA) en handelsakkoorden. Het categorisch uitsluiten van landen gaat tegen het landen-neutraal kabinetsbeleid in ten aanzien van bedrijven.”

Er kan een beroep gedaan worden op het belang van nationale veiligheid om immuniteit voor ‘rode knoppen’ en niet-Europese wetgeving te waarborgen. Zo kan bij de herziening van het Rijksbreed cloudbeleid en de vormgeving van de soevereine overheidscloud toch ingezet worden op aanvullende aanbestedingseisen voor gevoelige overheidsdata (zoals gerubriceerde informatie, vertrouwelijke communicatie en bijzondere persoonsgegevens), essentiële overheidsdiensten (het Diginetwerk, inning van belastingen, sociale zekerheid, DigiD, etc.) en kritieke fysieke infrastructuur (stormkeringen, sluizen en kritieke transport infrastructuur). Hiervoor bestaan reeds uitzonderingen in de GPA en handelsverdragen.

Door zo de vraag naar clouddiensten van Nederlandse en Europese bedrijven te vergroten wordt de bovendien concurrentiepositie van Europa, conform de aanbevelingen van het Draghi-rapport, versterkt. Door toenemende vraag vanuit de overheid kunnen bedrijven investeren in betere producten en dienstverlening en de cloudmarkt concurrerder maken. Daarmee kunnen zij ook andere kritieke sectoren in de samenleving bedienen die cloudoplossingen met een hogere mate van autonomie vereisen.

Aan de andere kant pleiten wij niet voor het volledig uitbannen van niet-Europese technologie – immers, we moeten ons realiseren dat we (nog) niet alles alleen kunnen en dat grote internationale leveranciers vooroplopen met technologische ontwikkelingen en innovaties die nodig zijn en waar ook wij van kunnen profiteren. We hoeven en moeten geen ‘digitaal eiland’ worden. Goede Europese wet- en regelgeving is essentieel om eerlijke concurrentie te stimuleren.

We doen al veel... en we kunnen nog meer!

Een belangrijke vraag bij de hierboven geschetste stip op de horizon is: kunnen we dit? Wat kan het Nederlandse en/of Europese bedrijfsleven aan diensten leveren op de korte en middellange termijn om deze beleidswijziging op te vangen?

Nederlandse cloudproviders leveren nu al tal van diensten aan de overheid; van de opslag van gevoelige gegevens tot veilige communicatiediensten en het draaien van kritieke digitale overheidsprocessen. Enkele voorbeelden hiervan zijn:

- Logius verzorgt veilige communicatie met burgers via een platform waarop diverse voorzieningen (MijnOverheid, Digipoort/KVK Groot) hun toepassingen reeds veilig kunnen ontwikkelen en migraties van DigiD, DigiD Machtigingen en Berichtenbox op stapel staan.
- Het ministerie van Justitie & Veiligheid beheert federale infrastructuur zodat elke deelnemer eigenaar is van zijn eigen informatie en veilig kan communiceren tussen de besloten deelnemers.
- Dienst ICT Uitvoering (DICTU) heeft zelf grote platforms gebouwd op basis van open standaarden en open source zoals Kubernetes. Voorbeelden hiervan zijn de platforms van ACM, RVO, TweedeKamer.nl, enzovoorts.
- Ook wordt reeds voor de zorgsector een essentieel platform als ZorgID in Nederland gebouwd en gehost, gebruikmakend van Nederlandse encryptie.
- Oplossingen voor veilig en efficiënt datadelen zoals CumuluZ zijn volop in ontwikkeling, waarbij dient te worden gewaarborgd dat er niet uitsluitend op Azure of AWS-technologie wordt geleund en er wordt aangesloten bij Europese afsprakenstelsels zoals EHDS.
- Ook is er een aanzienlijk aantal datacenters in Nederlandse of minimaal Europese handen en is er ruimte om hier behoorlijke hoeveelheden servers en services onder te brengen.
- Nederlandse oplossingen voor cybersecurity zijn al beschikbaar, zoals de collectieve not-for-profit DDoS-bescherming 'NaWas' die Nederland weerbaar maakt tegen DDoS-aanvallen. Het gebruik van Nederlandse en/of Europese dienstverleners op securitygebied dient de voorkeur te genieten, met inzet op collectieve cyberweerbaarheid.
- In Europees verband wordt in Nederland via IPCEI-CIS gewerkt aan 'secure by design' open source oplossingen om clouds te beveiligen, die ook toepasbaar zijn in nationale clouds. De resultaten van deze IPCEI-CIS projecten dienen ook in overheidsprojecten ingezet te worden om ook deze een extra zetje te geven.

Het ontwikkelen van cloud platforms voor vitale en belangrijke overheidsdiensten dient te gebeuren op incrementele wijze – niet uitsluitend met het einddoel voor ogen dat in beton gegoten is. Cloud technologie leent zich uitstekend voor 'agile ontwikkelen', waarbij snel bijsturen op basis van actuele inzichten en ontwikkelingen mogelijk is.

Kortom, we kunnen echt wat en doen ook al veel voor de vitale infrastructuur. Dit kan eenvoudig worden uitgebreid door het beleid voor de selectie en het toewijzen van leveranciers minimaal te wijzigen. Dan volgt automatisch ook innovatiekracht en kennisontwikkeling. Immers: wanneer er vraag is vanuit de markt, dan zal de markt hierop acteren en gaan 'bouwen'.

Ons advies is om te kijken waar deze al bestaande diensten verder geschaald kunnen worden zodat er een "kick start" gegeven kan worden aan de "soevereine overheidscloud" voor de meest kritische overheidsdata, diensten en kritieke infrastuctuur.

Middellange termijn

Voor aanbestedingen van clouddiensten waarbij niet met gevoelige overheidsgegevens of met kritieke overheidsdiensten of kritieke fysieke infrastructuur gewerkt wordt, moet gelden dat dataportabiliteit en interoperabiliteit verplicht wordt, in lijn met de Europese Data Act. Dit is cruciaal om vendor lock-in te voorkomen en het concurrentievermogen van de Nederlandse en Europese cloudsector te vergroten.

Voor deze categorie data en diensten geldt dat gebruik van clouddiensten van Azure, AWS, Google en dergelijken geen probleem oplevert, mits een overstap in geval van nood op korte termijn mogelijk is en er een goed uitgewerkte en geteste exit-strategie ligt. Goed voorbeeld hiervan is de HAVEN-standaard van de VNG. Voorwaarde daarbij is dat er wel een goed Europees alternatief moet zijn om naar uit te kunnen wijken. Daar ligt een verantwoordelijkheid voor de overheid.

Tot slot is het belangrijk dat het cloudbeleid van de overheid, conform de aanbevelingen van de Rekenkamer, uniformer en concreter wordt, dat er meer regie en coördinatie tussen ministeries en overheden plaats moet vinden en dat er meer gebruik gemaakt moet worden van open standaarden, certificering en het afdwingen van AVG-voorwaarden. Daarnaast is het van belang dat de soevereine overheidscloud en het aangepaste Rijksbrede cloudbeleid wat betreft gebruik van open standaarden goed aansluiten op Europese initiatieven om toekomstige innovatie niet in de weg te zitten.



Conclusie

Gezien de geopolitieke spanningen en de risico's van onze afhankelijkheid van niet-Europese cloudproviders is een herziening van het Nederlandse cloudbeleid dringend noodzakelijk.

De kern van onze voorgestelde aanpak is het creëren van een additionele categorie van gevoelige overheidsdata (zoals gerubriceerde informatie, vertrouwelijke communicatie en bijzondere persoonsgegevens), essentiële overheidsdiensten (belastingen, sociale zekerheid, DigiD, etc.) en kritieke fysieke infrastructuur (het Diginetwerk, stormkeringen, sluizen, kritieke transport infrastructuur en ziekenhuizen) waar additionele aanbestedingseisen aan gesteld worden. Voor deze kritieke data, diensten en infrastructuur kan een beroep gedaan worden op uitzonderingen in internationale verdragen op het gebied van nationale veiligheid om strengere aanbestedingseisen te kunnen stellen op het gebied van autonomie, waardoor Nederlandse en Europese aanbieders ingezet kunnen worden en een aantal huidige oplossingen direct opgeschaald kunnen worden.

Introduceer een keurmerk voor Nederlandse of Europese partijen die aan de juiste voorwaarden voldoen en creëer een loket waar overheidsinkopers aanbieders kunnen vinden die aan het keurmerk voldoen.

Voor overige niet-kritieke overheidsclouddiensten is het verplicht stellen van dataportabiliteit en interoperabiliteit noodzakelijk om vendor lock-in te voorkomen en de Europese concurrentiekracht te vergroten. Hoewel structurele verbeteringen in overheidsregie nodig zijn, is onmiddellijke actie geboden om deze koerswijziging in te zetten.

Deze aanpak ondervangt niet alleen de risico's van afhankelijkheden, maar komt ook tegemoet aan de aanbevelingen van de Rekenkamer, Auditdienst Rijk en de moties van de Tweede Kamer. Bovendien versterkt het de concurrentiekracht van Europa conform de aanbevelingen van het Draghi-rapport.

Tot slot is het belangrijk om te benadrukken dat de uitkomst van de discussie over de regierol binnen de overheid met betrekking tot de inkoop van clouddiensten cruciaal is voor succesvol cloudbeleid op de lange termijn. Tegelijkertijd kunnen we niet wachten op de voltooiing van die discussie alvorens concrete (bovengenoemde) stappen te nemen.

Colofon

Deze uitgave is tot stand gekomen op initiatief van een brede samenwerking van organisaties uit de Nederlandse digitale infrastructuur. Gedreven door een gevoelde maatschappelijke verantwoordelijkheid voor de veiligheid en strategische digitale autonomie van Nederland en Europa, doen zij in deze publicatie enkele concrete suggesties voor een herijking van het Rijksbreed cloudbeleid.

De volgende personen werkten aan deze uitgave mee:
Ruud Alaerds (*Dutch Cloud Community*)
Ludo Baauw (*Intermax Group*)
Simon Besteman (*Dutch Cloud Community*)
Wouter Pegtel (*Nationale Beheersorganisatie Internet Providers / Digitale Infrastructuur Nederland*)
Daniëlle Schuur (*Solvinity*)
Marijn van Vliet (*Digitale Infrastructuur Nederland*)
Octavia de Weerdt (*Nationale Beheersorganisatie Internet Providers*)

Met dank aan de bijdragen van:
Bert Hubert

Opmaak:
Bijdevleet, Rotterdam

© 2025 - alle rechten voorbehouden

Initiatiefnemers



Mede-ondertekenaars



Position Paper

Strategische digitale autonomie en het Rijksbreed cloudbeleid