De route naar digitale autonomie

Meer grip op digitale afhankelijkheden

Autoriteit Consument & Markt | AFM | AP | DeNederlandscheBank EUROSYSTEEM | Rijksinspectie Digitale Infrastructuur, Ministerie van Economische Zaken en Klimaat

Inhoudsopgave

Kernboodschappen en aanbevelingen 3
- Kernboodschappen 3
- Aanbevelingen 3

Inleiding 5

Digitale autonomie 7
- Digitale autonomie vereist keuzevrijheid 7
- Digitale autonomie vereist bewuste afwegingen 7

De route naar digitale autonomie 9
- Overheden als launching customer 9
- Samenwerking is nodig én mogelijk 9
- Borg overstapmogelijkheden 10
- Neem digitale autonomie mee in aanbesteding en inkoop 11
- Versterk kennis en bewustzijn 11
- Versterking van beleid en wet- en regelgeving 12

De rol van ACM, AFM, AP, DNB en RDI 14

Kernboodschappen en aanbevelingen

Kernboodschappen

- Het versterken van digitale autonomie vraagt niet alleen om handelen door individuele bedrijven en instellingen die gebruik maken van IT-diensten, maar ook om gecoördineerde en collectieve actie om deze complexe transitie mogelijk te maken.
- Digitale autonomie draait om keuzevrijheid en eigen regie voor bedrijven en instellingen die gebruik maken van IT-diensten, met als doel de weerbaarheid van bedrijfsprocessen te versterken. Organisaties moeten in staat zijn te bewegen wanneer omstandigheden daarom vragen.
- Digitale autonomie vraagt ook om bewuste afwegingen tussen autonomie, kosten en functionaliteit: niet elk proces vereist hetzelfde niveau van autonomie. Voor vitale processen is het van belang om aanvullende waarborgen te treffen en zou het minimaal beschikbaar hebben van een Europese fall-back een basisvoorwaarde moeten zijn.
- De overheid kan een belangrijke rol spelen door als launching customer op te treden voor Europese digitale diensten gebaseerd op open standaarden en door samen te werken en vraag te bundelen.
- Het meenemen van digitale autonomie in aanbestedingen is goed mogelijk binnen de geldende aanbestedingsregels, bijvoorbeeld door eisen te stellen aan het voldoen aan specifieke standaarden en door digitale autonomie te vertalen naar concrete, toetsbare eisen en gunningscriteria die beschermen tegen ongewenste afhankelijkheden en blootstelling aan niet-Europese juridische verplichtingen.
- We roepen ook bedrijven en instellingen op om gezamenlijk digitale autonomie te bevorderen, door bijvoorbeeld binnen sectoren in samenwerkingsverbanden als launching customer op te treden voor sectorspecifieke IT-diensten. Hiervoor is volop ruimte binnen de kaders van de Mededingingswet.
- Daarnaast is het belangrijk dat bedrijven en instellingen optionaliteit en portabiliteit in hun IT-architectuur vergroten en vendor lock-in zoveel mogelijk beperken, bijvoorbeeld via containerisatie, open source software en open standaarden. IT-leveranciers dienen hun producten en diensten zo te ontwerpen dat zij overstapmogelijkheden ondersteunen en integratie met andere (Europese) oplossingen faciliteren.

Aanbevelingen

We roepen alle organisaties op om digitale autonomie expliciet mee te nemen als kwaliteitscriterium bij aanbestedings-, inkoop- en hercontracteringstrajecten van IT-diensten. Daarbij adviseren we om concrete besliskaders te hanteren waarin per type proces wordt vastgesteld welk niveau van digitale autonomie passend is en waarin duidelijk wordt gemaakt hoe autonomie zich verhoudt tot andere doelstellingen zoals kosten en functionaliteit. Het criterium autonomie dient te worden vertaald naar toetsbare eisen in aanbestedingsdocumenten en contracten, zoals eisen rond datalocatie, het gebruik van open standaarden, interoperabiliteit, goede exit-mogelijkheden en het beperken van vendor lock-in. Overheden, bedrijven en instellingen kunnen daarbij gebruik maken van de EU Data Act, die cloudaanbieders verplicht om dataportabiliteit en interoperabiliteit te faciliteren. Daarnaast is het van belang om een gelijker speelveld

te creëren door inkoopprocessen en aanbestedingen primair te baseren op functionele behoeften in plaats van op productspecifieke eisen. Investeren in eigen kennis en personeel voorkomt dat cruciale expertise volledig bij leveranciers ligt en maakt sterker opdrachtgeverschap en beheer mogelijk. De geldende regelgeving biedt veel ruimte om aandacht te besteden aan digitale autonomie. Wij nodigen organisaties uit tot vroegtijdig overleg en dialoog, bijvoorbeeld bij twijfels over de interpretatie van regelgeving.

Beleidsmakers en wetgevers

- Laat de overheid optreden als launching customer door voor te schrijven dat een bepaald deel van de cloudvraag aan de hoogste soevereiniteitseisen voldoet.
- Neem wettelijke vereisten op rondom het minimaal beschikbaar hebben van een Europese fall-back bij vitale processen.
- Versterk het investerings- en vestigingsklimaat voor Europese IT-aanbieders, onder meer door de toegang tot kapitaal te verbeteren, de fragmentatie van de interne markt te verminderen en de schaarse ruimte voor datacenters gericht in te zetten voor projecten die bijdragen aan de Europese concurrentie-kracht, autonomie en weerbaarheid.
- Borg een effectief stelsel van investeringstoetsing om vitale sectoren te beschermen tegen overnames die risico's kunnen vormen.

Overheden als afnemer van IT-diensten

- Gebruik de ruimte binnen de Aanbestedingswet om digitale autonomie te vertalen naar concrete, toetsbare eisen en gunningscriteria. Maak daarbij expliciet gebruik van de mogelijkheden om voorkeur te geven aan oplossingen die aan de hoogste soevereiniteitseisen voldoen.
- Koop gezamenlijk in, bijvoorbeeld via inkoopcollectieven en gezamenlijke raamovereenkomsten.

Bedrijven en instellingen

- Werk sectorbreed samen om gezamenlijk eisen te stellen aan IT-aanbieders en te investeren in Europese alternatieven. Hiervoor is volop ruimte binnen de kaders van de Mededingingswet.
- Realiseer overstapmogelijkheden door exit- en overgangsplannen te ontwikkelen en te testen, vendor lock-in te beperken en kortetermijnrisico's te verkleinen via multivendor-strategieën en het gebruik van open standaarden en interoperabiliteit als expliciet ontwerpprincipe in de IT-architectuur.
- Weeg bij elke beslissing om aanvullende clouddiensten af te nemen expliciet het risico op vendor lock-in mee.
- Zet stappen op korte termijn om risico's te beperken waaronder het in eigen beheer nemen van encryptiesleutels en zorg voor EU-gebaseerde fall-backs van o.a. data en kritieke software.

IT- leveranciers

- Werk samen met andere leveranciers en partijen in het ecosysteem aan de ontwikkeling van schaalbare Europese cloud- en IT-diensten, zodat alternatieven kunnen ontstaan voor dominante niet-Europese aanbieders. Hiervoor is ruimte binnen de Mededingingswet.
- Ontwikkel diensten die expliciet aansluiten op publieke en private eisen rond digitale autonomie, zoals interoperabiliteit, open source oplossingen, open standaarden en dataportabiliteit.
- Ontwerp producten en diensten zo dat zij overstapmogelijkheden ondersteunen, vendor lock-in beperken en integratie met andere (Europese) oplossingen faciliteren.

Inleiding

ACM, AFM, AP, DNB en RDI presenteren dit position paper gezamenlijk om bij te dragen aan de transitie naar meer digitale autonomie en het verminderen van afhankelijkheden van dominante niet-Europese IT-leveranciers, om zo de weerbaarheid, continuïteit en veiligheid van bedrijfsprocessen te vergroten. De digitale infrastructuur van Nederland en Europa leunt sterk op een beperkt aantal (veelal niet-Europese) technologiebedrijven voor clouddiensten, software en hardware. Dit brengt concentratie- en systeemrisico's met zich mee, zeker in het huidige geopolitieke klimaat. Ook voor de economische ontwikkeling van Europa zijn er risico's. Er kunnen zich verschillende scenario's voordoen; zo kan dienstverlening plots wegvallen als gevolg van een storing, cyberincident of politieke druk uit derde landen, of kunnen derde landen toegang tot data afdwingen, bijvoorbeeld via wetgeving zoals de Amerikaanse Cloud Act. Verder maakt vendor lock-in overstappen en risicospreiding moeilijk en kostbaar, waardoor de onderhandelingspositie verzwakt en prijzen kunnen stijgen. Voor overheden, financiële instellingen en andere vitale organisaties raakt digitale afhankelijkheid daarmee direct aan de veiligheid en continuïteit van dienstverlening. Voor de economie wordt door de afhankelijkheden het verdienvermogen op termijn aangetast.

Het weerbaarder maken van de Nederlandse economie door het versterken van digitale autonomie is inmiddels een breed gedragen doel. In het coalitieakkoord is digitale autonomie expliciet opgenomen als leidend uitgangspunt voor het overheidsbeleid. Ook de Nederlandse Digitaliseringsstrategie en de visie Digitale autonomie en soevereiniteit van de overheid benadrukken het belang van regie, keuzevrijheid en overstapmogelijkheden in het digitale domein. Desondanks constateren de toezichthouders dat de afhankelijkheden in de praktijk blijven toenemen. De Nederlandse situatie is daarbij illustratief voor de bredere Europese ontwikkeling, terwijl effectieve oplossingsrichtingen grotendeels op Europees niveau moeten worden gerealiseerd. Digitale autonomie vraagt om een betere balans in afhankelijkheden ten opzichte van regio's buiten Europa. Dit vergt niet alleen het verminderen van risico's, maar ook het actief versterken van het Europese digitale ecosysteem, onder meer door zelf strategische capaciteiten verder te ontwikkelen, de diversiteit in het aanbod van IT-diensten te vergroten, de vraagkracht van organisaties beter te bundelen en samenwerking te stimuleren.

Voor elke toezichthouder is dit vraagstuk vanuit het eigen mandaat van groot belang. De Autoriteit Consument & Markt (ACM) signaleert dat vendor lock-in bij grote technologieleveranciers leidt tot een beperking van het aanbod en daarmee tot belemmeringen voor een goede marktwerking.[1] De Rijksinspectie Digitale Infrastructuur (RDI) ziet als toezichthouder op basis van onder meer de Telecommunicatiewet, NIS2, EIDAS en CSA dat de digitale weerbaarheid van Nederland afhankelijk is van een beperkte set bedrijven, wat systeemrisico's met zich meebrengt.[2] De Autoriteit Financiële Markten (AFM) en De Nederlandsche Bank (DNB) houden toezicht op een beheerste en integere bedrijfsvoering van financiële ondernemingen en, meer specifiek, op hun digitale weerbaarheid zoals vastgelegd in de Verordening digitale operationele weerbaarheid (DORA) en signaleren dat toenemende afhankelijkheid van een beperkt aantal (veelal niet-Europese)

1 Staat van de Markt 2026 | ACM
2 Toezicht op gebruik van clouddiensten | Rijksinspectie Digitale Infrastructuur | RDI

technologieaanbieders leidt tot concentratie- en systeemrisico's, die de stabiliteit van het stelsel en de belangen van consumenten in gevaar kunnen brengen.[3] Digitale afhankelijkheid brengt ook het risico met zich mee dat persoonsgegevens in vitale processen op grote schaal, langdurig niet beschikbaar zijn of worden aangetast. Op grond van de AVG moeten overheden en bedrijven hier maatregelen tegen treffen. De AP vindt het van groot belang dat deze vitale processen beter worden beschermd.[4]

Het is vooral belangrijk dat bedrijven en instellingen hun risico's spreiden en niet alle eieren in één mandje hebben waar het gaat om digitale infrastructuur en dienstverlening. Op dit moment is Europa afhankelijk van kritieke infrastructuur uit verschillende regio's buiten Europa ten aanzien van bijvoorbeeld clouddienstverlening, security en datacenters. De aanbevelingen in dit position paper richten zich dus niet tegen een bepaalde jurisdictie of regio die deze diensten of infrastructuur aanbiedt. Evenmin bevat het position paper nieuwe regels of verplichtingen voor bedrijven en instellingen onder ons toezicht. Wel loopt Europa achter waar het gaat om digitale innovatie en is het daarom, zowel om strategische als economische redenen, belangrijk dat Europa op dit gebied een inhaalslag maakt; een ambitie die ook centraal staat in het recent gepresenteerde Tech Sovereignty Package van de Europese Commissie, dat inzet op het structureel versterken van de Europese digitale capaciteit en het terugdringen van strategische afhankelijkheden.

3 Digitale afhankelijkheid in de financiële sector | DNB, AFM
4 Brief aan minister EZ over digitale soevereiniteit | AP

Digitale autonomie

Digitale autonomie vereist keuzevrijheid

Digitale autonomie betekent dat overheden en organisaties in staat zijn om zelf keuzes te maken over hun IT en hier daadwerkelijk regie over hebben. We bedoelen hier nadrukkelijk niet mee dat alle technologie in eigen beheer moet worden ontwikkeld of dat volledige technologische onafhankelijkheid wordt nagestreefd. Centraal staat de beperking van ongewenste strategische afhankelijkheden en het hebben van keuzevrijheid bij overstappen tussen leveranciers. Het betekent ook handelingsperspectief wanneer zich ongunstige scenario's voordoen.

Digitale autonomie vraagt om het fundamenteel nadenken over de inrichting van de IT-architectuur. Keuzevrijheid ontstaat alleen wanneer de IT-architectuur open is ingericht, gebaseerd op open standaarden en interoperabele oplossingen, waarbij overheden en organisaties niet vastzitten aan één leverancier. Op dit moment leiden dominante cloudoplossingen van (niet-Europese) hyperscalers echter tot sterke afhankelijkheden en vendor lock-in.

Digitale autonomie heeft in de huidige geopolitieke context ook een link met juridische soevereiniteit. Afhankelijkheid van niet-Europese IT-dienstverleners kan ertoe leiden dat organisaties te maken krijgen met buitenlandse wetgeving, wat de eigen regie over data en digitale processen kan beperken. Zolang er in Europa nog onvoldoende volwaardige alternatieven beschikbaar zijn, zijn scenario's denkbaar waarin statelijke actoren de afhankelijkheid van niet-Europese dienstverleners als machtsmiddel inzetten. Om de weerbaarheid tegen dit soort scenario's te vergroten is versterking van het Europese aanbod van IT-diensten belangrijk. In dit kader is het begrip juridische soevereiniteit van belang, waarmee wordt bedoeld dat bepaalde juridische risico's voorkomen moeten worden, zoals dat data niet eenzijdig kan worden gevorderd door niet-Europese overheden.

Digitale autonomie vereist bewuste afwegingen

Digitale autonomie is geen absoluut doel, maar een kwestie van bewuste en proportionele afwegingen. Niet elke toepassing vereist hetzelfde niveau van autonomie of soevereiniteit. Daarom is het nodig om onderscheid te maken tussen verschillende categorieën processen en diensten, en om per categorie expliciet vast te stellen welk niveau van autonomie en controle noodzakelijk is. Dit onderscheid is al in wetgeving terug te vinden. In de financiële sector gelden onder DORA eisen voor 'kritieke en belangrijke' functies[5], terwijl in een aantal andere sectoren onder de NIS2-richtlijn regels gelden voor 'essentiële en belangrijke' entiteiten[6] en hun diensten. Een aantal van deze functies en entiteiten kunnen daarenboven ook worden aangemerkt als 'vitaal', namelijk wanneer uitval, verstoring of manipulatie kan leiden tot ernstige maatschappelijke ontwrichting, ernstige economische schade of – in het uiterste geval – een bedreiging van de nationale veiligheid. In de financiële sector gaat het dan bijvoorbeeld om

5 Kritieke of belangrijke functies zijn functies waarvan de verstoring wezenlijk afbreuk zou doen aan de financiële prestaties van een financiële entiteit of aan de soliditeit of de continuïteit van haar diensten en activiteiten.

6 Essentiële en belangrijke entiteiten zijn entiteiten die kritiek zijn door hun sector of het soort door hen verleende diensten, rekening houdend met hun omvang.

het betalings- en effectenverkeer en het saldobeheer door banken.[7]

Voor vitale processen is het van belang om aanvullende waarborgen te treffen om afhankelijkheden en concentratierisico's te beperken. Het is van cruciaal belang dat wordt voorkomen dat dienstverlening door een storing, cyberincident of politieke druk uit derde landen wegvalt of dat derde landen toegang tot data kunnen afdwingen. Als de nationale veiligheid in het geding is, biedt wetgeving ook de mogelijkheden om aanbieders van diensten bij een aanbesteding uit te sluiten op basis van soevereiniteitsrisico's.

Voor vitale processen zou vanwege geopolitieke risico's het minimaal beschikbaar hebben van een Europese fall-back een basisvoorwaarde moeten zijn om de continuïteit te waarborgen. We vragen de Europese wetgevers om dit als wettelijke vereiste op te nemen. Voor zover op de korte termijn de afhankelijkheid van niet-Europese leveranciers blijft bestaan is het voor organisaties in deze sectoren ook belangrijk om maatregelen te treffen die acute risico's mitigeren. Zo vergroot het zelf beheren van encryptiesleutels de controle over data en wordt het risico op ongewenste toegang tot data door derden beperkt. Onafhankelijke back ups, bij voorkeur on premise of binnen de EU, zorgen voor herstelmogelijkheden bij uitval of incidenten in de primaire cloudomgeving.

Voor alle kritieke, belangrijke en essentiële functies en diensten moeten de risico's van afhankelijkheden van IT-dienstverleners worden beheerst. Specifiek voor de financiële sector geldt dat op grond van de DORA-verordening aanbieders van IT-ondersteuning van kritieke en belangrijke functies en de financiële instellingen zelf moeten voldoen aan vereisten rond o.a. informatiebeveiliging, businesscontinuïteitsplannen en exitstrategieën. De ECB *Guide on outsourcing cloud services to cloud service providers* beoogt daarbij nadere duidelijkheid te geven over de verwachtingen onder DORA en geeft bij de verschillende vereisten 'best practices' om hieraan te voldoen.[8] Naast het sectorspecifieke kader voor de financiële sector geldt voor andere sectoren dat op grond van de NIS2-richtlijn[9] essentiële en belangrijke entiteiten en de door hen geleverde essentiële diensten aan verhoogde cyberweerbaarheids en zorgplichtvereisten moeten voldoen, waaronder op het gebied van de beveiliging van de toeleveringsketen en afhankelijkheden van IT-dienstverleners. In een recent gepubliceerde opinie[10] heeft de RDI al aangegeven dat bedrijven en instellingen meer grip moeten krijgen op hun afhankelijkheden.

Voor niet-vitale processen kan het versterken van digitale autonomie ook binnen het aanbod van niet-Europese leveranciers worden vormgegeven, mits een bewuste afweging wordt gemaakt waarin de risico's zorgvuldig in kaart zijn gebracht. Optionaliteit, portabiliteit en het voorkomen van lock-in zijn daarbij belangrijk. Hiervoor zijn een beter aanbod van IT-diensten, open standaarden en interoperabiliteit nodig. Verder kunnen organisaties die niet-vitale processen beheren technische maatregelen nemen om de belangrijkste risico's te verkleinen, zoals het zelf beheren van encryptiesleutels en het zorgen voor onafhankelijke fall-backs.

---

7 Zie voor een compleet overzicht van vitale processen Aanpak vitaal | Nationaal Coördinator Terrorismebestrijding en Veiligheid, en voor meer informatie over vitale processen in de financiële sector Kamerstuk 30821, nr. 323 | Overheid.nl > Officiële bekendmakingen.

8 ECB Guide on outsourcing cloud services to cloud service providers

9 De NIS2-richtlijn wordt in Nederland omgezet in de Cyberbeveiligingswet (Cbw), die in 2026 in werking treedt.

10 Toezicht op gebruik van clouddiensten | RDI

De route naar digitale autonomie

De route naar digitale autonomie vraagt om gezamenlijke inspanningen van meerdere partijen. Het verminderen van digitale afhankelijkheden en het vergroten van keuzevrijheid is geen opgave die door individuele organisaties of de markt alleen kan worden gerealiseerd. Overheden, beleidsmakers en wetgevers vervullen een bepalende rol door richting te geven via beleid, inkoop en regelgeving. Bedrijven en vitale organisaties maken de concrete keuzes in hun IT-strategie. IT leveranciers beïnvloeden met hun ontwerpkeuzes en de mate van interoperabiliteit of overstappen daadwerkelijk mogelijk is. Toezichthouders dragen bij door ruimte en duidelijkheid te bieden binnen bestaande kaders en door belemmeringen voor samenwerking en overstappen weg te nemen. In dit hoofdstuk werken we uit welke stappen nodig zijn om, langs deze sporen, te komen tot een meer autonome en weerbare IT-infrastructuur.

Overheden als launching customer

Een gecoördineerde aanpak onder regie van Europese overheden is noodzakelijk. Organisaties die als eerste overstappen naar een Europese aanbieder maken extra kosten en lopen risico. Daardoor ontstaat een situatie waarin marktwerking en concurrentie onvoldoende leiden tot de ontwikkeling van alternatieven. Zonder coördinatie blijven noodzakelijke stappen richting digitale autonomie daardoor uit. Europese alternatieven kunnen alleen groeien wanneer Europese publieke organisaties zich voor langere tijd als afnemer verbinden. Door hun schaal en continuïteit kunnen overheden vraagzekerheid bieden, waardoor marktontwikkeling wordt gestimuleerd en een meer geïntegreerd aanbod ontstaat. Daarbij is het belangrijk om gericht te werken aan een zichtbaar succes binnen de overheid. Door kennis en expertise te bundelen en in te zetten op een succesvolle overstap bij één of enkele organisaties, kan een concreet en navolgbaar voorbeeld worden neergezet. De geleerde lessen kunnen vervolgens worden benut om de transitie naar een meer autonome IT-stack te versnellen.

Samenwerking is nodig én mogelijk

Samenwerking binnen overheden en sectoren biedt kansen om gezamenlijk sterker te staan. Een groep afnemers kan gezamenlijk eisen formuleren richting aanbieders van cloud- en softwarediensten. Door vraag te bundelen en gezamenlijke eisen te stellen (bijvoorbeeld gericht op autonomie, het beperken van vendor lock-in, het vergroten van transparantie en het waarborgen van continuïteit), ontstaat meer invloed op het aanbod. Organisaties kunnen samen investeren in de ontwikkeling van bestaande en nieuwe (Europese) clouddiensten of infrastructuur, inclusief open source-alternatieven. Dit verlaagt de risico's voor individuele organisaties en versnelt de beschikbaarheid van alternatieven.

Schaalgrootte is nodig om een Europees aanbod te creëren dat kan concurreren met grote spelers van buiten Europa; bundeling van zowel vraag als aanbod kan daarbij helpen. Denk bijvoorbeeld aan afspraken tussen financiële instellingen om clouddiensten af te nemen van een Europese aanbieder met nu nog onvoldoende schaalgrootte. De vraagbundeling stelt deze aanbieder in staat om snel op te schalen, en daarmee kosten te reduceren en te investeren in kwaliteit en functionaliteit. Bundeling van het aanbod kan ook helpen voor het verkrijgen van de benodigde schaalgrootte. Afspraken over bundeling van vraag en aanbod kunnen daarmee uiteindelijk leiden tot meer concurrentie.

De toezichthouders zien bij bedrijven vaak terughoudendheid om samen te werken, maar de Mededingingswet staat samenwerking in veel gevallen toe. Veel vormen van gezamenlijke inkoop, investering en het stellen van technische eisen beperken de concurrentie niet en kunnen juist bijdragen aan een diverser en autonomer aanbod. Ook kunnen samenwerkingsverbanden de keuzemogelijkheden vergroten door bijvoorbeeld eisen te stellen aan interoperabiliteit, dataportabiliteit en het voldoen aan toezichtseisen. Aan de aanbodkant kan bijvoorbeeld het maken van afspraken over het hanteren van open standaarden het veranderen van aanbieder faciliteren, en daarmee de concurrentiemogelijkheden juist versterken.

Borg overstapmogelijkheden

Om de mogelijkheden om te kunnen overstappen te versterken, zijn bewuste architectuur- en inkoopkeuzes nodig, zoals het gebruik van open standaarden, die gezamenlijk worden opgesteld. Open standaarden en open source software versterken controle, interoperabiliteit en overstapmogelijkheden. Wanneer systemen gebaseerd zijn op open standaarden, wordt het eenvoudiger om onderdelen te vervangen, nieuwe aanbieders toe te laten en diensten te migreren, wat vendor lock-in beperkt. Het gebruik van open standaarden draagt bij aan overstapmogelijkheden, maar biedt op zichzelf geen volledige garantie op onafhankelijkheid of digitale autonomie. Daarom is het van belang dat open standaarden waar mogelijk gezamenlijk worden opgesteld. Samenwerkingsverbanden van afnemers kunnen hierin een rol spelen door eisen te stellen aan interoperabiliteit en data- en applicatieportabiliteit.

Een multivendorstrategie vergroot de handelingsvrijheid doordat organisaties niet afhankelijk zijn van één aanbieder binnen de IT-stack. Door voor vitale processen meerdere (deels overlappende) leveranciers in te zetten, ontstaat echte optionaliteit en portabiliteit en neemt de drempel om te switchen af. Dit vraagt wel om investeringen in interoperabiliteit, het gebruik van open standaarden en portable architecturen, bijvoorbeeld via containerisatie. Tegelijkertijd kan een multivendorstrategie extra kosten, complexiteit, beheerlast en potentiële security-risico's met zich meebrengen, waardoor een zorgvuldige afweging noodzakelijk is. Belangrijk hierbij is dat voor de verschillende leveranciers de ketenrisico's in beeld gebracht worden. Voor overheden ligt er een voorbeeldrol: door multivendor, modulaire architecturen en open standaarden structureel op te nemen in aanbestedingen, wordt de markt actief in beweging gezet.

Daarnaast kunnen organisaties expliciete eisen stellen aan IT-leveranciers, bijvoorbeeld dat zij hun oplossingen zó inrichten dat deze in verschillende omgevingen inzetbaar zijn. Door te zorgen dat applicaties en diensten in verschillende cloudplatforms en on-premise kunnen draaien, behouden afnemers de mogelijkheid om keuzes te heroverwegen wanneer risico's, kosten of strategische omstandigheden veranderen. Dit vraagt van IT leveranciers dat zij hun oplossingen ontwerpen met portabiliteit en interoperabiliteit als uitgangspunt, en geen onnodige technische of contractuele afhankelijkheden creëren.

Realistische exit- en overgangsplannen vergroten de flexibiliteit en maakt overstappen concreet uitvoerbaar. Onder DORA zijn financiële instellingen al verplicht om exit- en overgangs-

plannen te ontwikkelen, maar ook daarbuiten is het essentieel om vooraf na te denken over scenario's waarin switching noodzakelijk wordt. Zo stelt NIS2 ook eisen aan goed leveranciersmanagement. Om tot realistische exit- en overgangsplannen te komen zijn investeringen in de kwaliteit en uitvoerbaarheid van deze plannen nodig, inclusief het periodiek testen ervan.

Neem digitale autonomie mee in aanbesteding en inkoop

We roepen organisaties en overheden op om digitale autonomie expliciet mee te nemen als kwaliteitscriterium bij inkoopkeuzes om zo een gelijk speelveld te creëren voor Europese, open-source oplossingen. Dat betekent bijvoorbeeld dat eisen kunnen worden gesteld aan juridische soevereiniteit, zoals het enkel en alleen vallen onder Europese wetgeving. Autonomie moet daarbij worden gezien als een volwaardig kwaliteitscriterium, naast prijs en functionaliteit. Voor vitale infrastructuur en diensten zou autonomie een randvoorwaarde moeten zijn. Een rijksbreed referentiekader voor digitale autonomie kan hierbij ondersteuning bieden.

Het versterken van digitale autonomie kan gepaard gaan met tijdelijke concessies op het gebied van kwaliteit of kosten. In een transitieperiode kan het noodzakelijk zijn om hogere uitgaven te accepteren of genoegen te nemen met minder uitgebreide functionaliteiten. Dit is verdedigbaar wanneer het bijdraagt aan meer controle, minder afhankelijkheid en een sterker digitaal fundament op de lange termijn. Gezien het belang van digitale autonomie voor vitale processen weegt dit criterium bij dergelijke processen zwaarder dan bij niet-vitale processen.

Het meenemen van digitale autonomie in aanbesteding en inkoop hoeft het gebruiken van innovatieve toepassingen niet in de weg te staan. Zeker bij niet-vitale processen kunnen overwegingen ten aanzien van functionaliteit, stabiliteit en efficiency een relatief zwaar gewicht krijgen. Wel zouden ook in dat geval realistische exitplannen moeten worden opgesteld, waarbij van de IT-dienstverlener ook vereist moet worden dat die deze faciliteert.

In de praktijk bestaat terughoudendheid om autonomie mee te nemen als kwaliteits-criterium, vanwege onduidelijkheid rondom de juridische toelaatbaarheid. Binnen de kaders van de Aanbestedingswet is er wel degelijk ruimte om digitale autonomie als kwaliteitscriterium mee te nemen. Om dit in de praktijk mogelijk te maken, moeten organisaties in staat zijn om zich te verweren tegen juridische procedures bij een aanbesteding. De rijksoverheid kan hiervoor expertise en middelen beschikbaar stellen. We roepen op om bij eventuele knelpunten in het meenemen van autonomie in een aanbesteding contact op te nemen met de toezichthouders.[11]

Versterk kennis en bewustzijn

Het is van belang de kennis bij inkoop en IT teams te versterken. Het gaat daarbij om kennis op het vlak van 1) soevereiniteit en autonomie, en de mogelijkheden en vereisten die de wetgeving biedt om dit mee te nemen; en 2) de technologie,

11 Organisaties kunnen hiervoor terecht bij ACM en/of PIANOo. ACM kan meedenken vanuit het mededingingsperspectief, terwijl PIANOo kan ondersteunen bij vragen over de toepassing en mogelijkheden binnenhet aanbestedingsrecht.

kwetsbaarheid van bepaalde workloads, en alternatieven. Deze kennis is essentieel om goed onderbouwde keuzes te maken. Voor financiële instellingen geldt dat deze kennis in veel gevallen al in belangrijke mate aanwezig is, gezien de bestaande vereisten op het gebied van risicomanagement en toezicht. Tegelijkertijd blijft het van belang om deze kennis actueel te houden en waar nodig verder te verdiepen, met name in het licht van nieuwe technologische en geopolitieke ontwikkelingen. Ook is het van belang dat inkopers aanbestedingen functioneel en technologieneutraal formuleren, zodat Europese aanbieders ook kunnen voldoen.

Digitale autonomie kan ook worden versterkt binnen het aanbod van niet-Europese aanbieders, maar dit vraagt van organisaties dat zij zorgvuldig nagaan in hoeverre aangeboden alternatieven de digitale autonomie en de weerbaarheid daadwerkelijk vergroten. Niet Europese aanbieders presenteren steeds vaker soevereine cloud-varianten voor de Europese markt. Deze oplossingen kunnen bepaalde risico's beperken. Tegelijkertijd is het belangrijk om zorgvuldig na te gaan in hoeverre de aangeboden alternatieven aansluiten bij specifieke behoeften en eisen op het gebied van digitale autonomie. Wat hierin acceptabel is, verschilt per organisatie en proces en hangt samen met de eigen risicobereidheid. Wanneer het van belang is dat de oplossing volledig is afgeschermd van niet EU-wetgeving, zal het aanbod van een niet-Europese hyperscaler naar verwachting niet kunnen voldoen.

Versterking van beleid en wet- en regelgeving

Een effectief stelsel van investeringstoetsing is nodig om vitale sectoren te beschermen tegen overnames die risico's kunnen vormen. In Nederland toetst het Bureau Toetsing Investeringen fusies, investeringen en overnames die onder dit stelsel vallen op risico's voor de nationale veiligheid en het publieke belang.[12] Het doel is om Nederland te beschermen tegen bijvoorbeeld de uitval van vitale processen en het weglekken van gevoelige technologie wanneer een derde partij zeggenschap krijgt in een bedrijf. Als investeringen of overnames risico's opleveren is het van belang dat er voldoende alternatieven beschikbaar zijn met een lager risicoprofiel. Het functioneren van de Europese kapitaalmarktunie blijft bijzondere aandacht vragen om alternatieven te kunnen bieden.

Wet- en regelgeving gericht op autonomie kan het gevoel van urgentie versterken door lock-ins actief te ontmoedigen en overstappen expliciet mogelijk en proportioneel verplicht maken. De Data Act en DORA, en mogelijk in de toekomst ook de Digital Markets Act, zetten hierin al belangrijke stappen door dataportabiliteit, exitstrategieën en operationele weerbaarheid te normeren. De Data Act stelt eisen aan interoperabiliteit en dataportabiliteit om overstappen en multi-vendor strategieën te faciliteren. Daarnaast doet de Europese Commissie momenteel onderzoek naar het aanwijzen van twee belangrijke cloudaanbieders als poortwachter in de Digital Markets Act. Hiermee zouden aanvullende verplichtingen gelden die verder helpen bij het overstappen en combineren van diensten.

12 Het BTI is onderdeel van de directie TEVEA binnen het Ministerie van Economische Zaken en Klimaat.

Het stimuleren van concurrerend Europees aanbod, en daarmee de versterking van de digitale autonomie, is alleen mogelijk als ook de onderliggende oorzaken van digitale afhankelijkheid worden aangepakt. Zoals benadrukt in de Draghi- en Letta-rapporten vereist dit een structurele verbetering van het investeringsklimaat en een versterking van de aantrekkelijkheid voor scale-ups en strategische technologiebedrijven. Dit betekent een betere toegang tot kapitaal, minder fragmentatie van de interne markt, ruimte voor de bouw van datacenters en waar relevant het bieden van omzetgaranties aan innovatieve spelers. Om voldoende kapitaal te mobiliseren is een belangrijke rol weggelegd voor de 'spaar- en investeringsunie'. Toegang tot financiering met het oog op schaalvergroting van innovatieve ondernemingen is daarbij een belangrijk aandachtspunt. Zonder deze randvoorwaarden blijft het aanbod versnipperd en onvoldoende concurrerend, waardoor afhankelijkheden in stand blijven.

De rol van ACM, AFM, AP, DNB en RDI

We bieden ruimte en duidelijkheid aan organisaties, onder andere via gerichte guidance over toelaatbare samenwerking, bijvoorbeeld bij gezamenlijke inkoop, gezamenlijk investeren, het bundelen van aanbod en andere vormen van samenwerking. Wij herkennen dat er vragen bestaan over de mogelijkheden tot samenwerking rond digitale autonomie. ACM, AFM, AP, DNB en RDI vinden het belangrijk dat deze vragen geen belemmering vormen voor de ontwikkeling van een meer autonome IT-stack. Er is vaak meer mogelijk dan wordt gedacht.

We nodigen organisaties expliciet uit tot vroegtijdig overleg en dialoog, bijvoorbeeld bij twijfel over de interpretatie van regelgeving. Neem bij twijfel over de interpretatie van regelgeving of toezichteisen vroegtijdig contact op.

We werken onderling samen om belemmeringen voor overstappen en het gebruik van Europese alternatieven te verminderen en signalen uit de praktijk, zoals knelpunten en marktfalen, gezamenlijk op te pakken. Wij onderzoeken waar knelpunten zitten en treden op wanneer wet- en regelgeving wordt overtreden, met bijzondere aandacht voor praktijken die de ontwikkeling van een autonome IT-stack onnodig belemmeren.

We brengen onze eigen afhankelijkheden in kaart en maken bewuste keuzes om deze waar mogelijk te verkleinen. Digitale autonomie vraagt ook inspanningen van toezichthouders als IT-gebruikers. Zo heeft DNB recent een contract gesloten met een Europese clouddienstverlener. Met dergelijke keuzes doen we zelf ervaring op met de afwegingen, kansen en beperkingen die gepaard gaan met het gebruik van Europese alternatieven, wat helpt om het gesprek met de sector concreter en realistischer te voeren en om beleid en toezicht beter te laten aansluiten bij de uitvoerbaarheid in de praktijk.

We zetten ons in om het belang van digitale autonomie actief te agenderen bij onze Europese collega-toezichthouders, zoals de ECB, ESMA, EIOPA en ENISA. We zullen digitale autonomie nadrukkelijk inbrengen in Europese overlegstructuren, met als doel bij te dragen aan een consistent en toekomstgericht beleidskader. Tegelijkertijd zien we een belangrijke rol voor de Nederlandse overheid om in Europees verband te sturen op het versterken van strategische coördinatie rondom het aanbod en de ontwikkeling van Europese IT-diensten. Zo kan gezamenlijk worden gewerkt aan een robuust, concurrerend en veerkrachtig Europees digitaal ecosysteem.