

# **Rapport: Streven naar Digitale Autonomie in Amsterdam**

Maart 2025

## Samenvatting

De Amsterdamse gemeenteraad heeft op 28 maart 2024 unaniem ingestemd met het gewijzigde initiatiefvoorstel 'Amsterdam Digitaal Onafhankelijk' van het lid IJmker. Dit initiatiefvoorstel verzoekt om de gemeente Amsterdam minder afhankelijk te maken van grote techbedrijven voor haar digitale diensten en producten. In oktober 2024 heeft de gemeenteraad een raadsinformatiebrief met de tussenstand van de verkenning ontvangen.

Op het verzoek van de gemeenteraad is verder onderzocht hoe Amsterdam digitaal onafhankelijk kan worden, met aandacht voor het beperken van afhankelijkheden van grote (niet-Europese) technologiebedrijven (Big Tech) en het versterken van de controle over data en technologie. Dit rapport is het resultaat van onderzoek naar de digitale autonomie van de gemeente Amsterdam.

### **Streven naar digitale autonomie**

Zorgen over digitale afhankelijkheid spelen breder in de samenleving, bijvoorbeeld in het onderwijs, in media en journalistiek, in het bankwezen en bij andere overheden. Voor de gemeentelijke dienstverlening is digitale autonomie van belang voor vertrouwelijkheid (wie kan er bij welke informatie?), wendbaarheid (ondersteunt IT de politieke en beleidskeuzes, of is de IT bepalend?) en weerbaarheid (is de organisatie in staat zelf IT weer werkend te krijgen na uitval?). Autonomie stelt de overheid in staat om strategische keuzes te maken zonder externe afhankelijkheden die de controle over kritieke systemen en processen beperken. Het betekent dat de overheid een stevige basis nodig heeft om haar taken uit te voeren, zelfs in tijden van geopolitieke of technologische druk. De eerlijkheid gebiedt te zeggen dat het college – net als veel andere overheden, organisaties en bedrijven – die autonomie nu niet of niet in voldoende mate voelt. Dat gaat veel verder dan de plotselinge kostenstijgingen waar grote leveranciers ons mee confronteren. Recente geopolitieke ontwikkelingen benadrukken hoe kwetsbaar Europa, Nederland en Amsterdam zijn geworden door de afhankelijkheid van enkele Amerikaanse techbedrijven. Zeker nu de vermenging van big tech en het politieke bestuur steeds verder lijkt te gaan.

Voor het college is het dan ook helder: Amsterdam, Nederland en Europa moeten digitaal onafhankelijker worden. Niet per se omdat we ontevreden zijn over de dienstverlening van onze huidige leveranciers, maar omdat we onze eigen keuzes willen blijven maken, omdat we de privacy van Amsterdammers, organisaties en bedrijven willen beschermen, en omdat in het belang is van onze veiligheid.

Amsterdam kan dit niet alleen. Er is nationale en Europese actie nodig om echt stappen te zetten naar een digitaal autonoom Europa. In Amsterdam wil ik graag realistische eerste stappen zetten die hieraan bijdragen, door bijvoorbeeld specifieke kennis op te bouwen en door in de inkoop digitale autonomie mee te nemen als criterium. Ik realiseer mij dat 'even overstappen' vaak niet mogelijk is, om technische en financiële redenen, of omdat Europese alternatieven niet dezelfde dienstverlening bieden als de huidige Amerikaanse leveranciers. Ik realiseer mij ook dat u verwacht dat de kwaliteit en continuïteit van onze dienstverlening minimaal op hetzelfde niveau blijven. Toch zullen we wat het college betreft stappen moeten zetten, te beginnen met enkele kleinere stappen. In het vervolg op deze verkenning wil het college onder andere kijken naar de inrichting van onze werkplekken (inclusief software voor email, tekstverwerking en spreadsheets) en de software die we gebruiken voor interactie met Amsterdammers voor onze dienstverlening.

Deze verkenning biedt een basis voor het gesprek over de keuzes die uw gemeenteraad wil maken voor de toekomst, inclusief de financiële keuzes die daarbij horen.

### **De huidige situatie**

In de 'Tussenstand van de verkenning Amsterdam Digitaal Onafhankelijk' die ik u op 17 oktober 2024 heb gestuurd, heb ik inzicht gegeven in de dynamiek rondom digitale autonomie. Duidelijk is dat de gemeente Amsterdam niet alleen staat in de ambitie om minder afhankelijk te zijn van enkele partijen. Zowel op Europees als landelijk niveau wordt het belang onderschreven en gewerkt aan visies en beleidskaders. Amsterdam zal de komende tijd nauw optrekken met het Rijk en de VNG.

- Uit het onderzoek blijkt dat Amsterdam, net als andere overheidsorganisaties, afhankelijk is van grote leveranciers voor de diensten zoals de cloudomgeving, kantoorautomatisering en datamanagement. De gemeente Amsterdam is afhankelijk van meerdere grote leveranciers, zoals Microsoft, Salesforce, SAP, Centric en PinkRoccade.
- De afhankelijkheid zal niet vanzelf minder worden: het is een bewust gevolg van de besluiten in Amsterdam om de kern ICT-taken uit te besteden en om vooral voor SAAS-toepassingen (software die als een onlinedienst wordt aangeboden) te kiezen. Dit is in lijn met het huidige cloudbeleid van het Rijk. Staatssecretaris Szabó heeft de Tweede Kamer toegezegd dat cloudbeleid te herzien en dat te doen met/voor de hele overheid, inclusief lokale overheden.
- Amsterdam is hierin niet uniek. De keuzes die in de afgelopen jaren zijn gemaakt rondom het IT-beleid, zijn mede gebaseerd op cyberdreigingen die vanuit de gemeente zelf niet te beheersen zijn. De geboden functionaliteit en gebruiksvriendelijkheid, veiligheid en compliance, kennis en support zijn voor overheden redenen om te kiezen voor de standaardoplossingen.
- Het potentieel van samenwerken met andere overheden nog onvoldoende benut. Er is aandacht voor het beschermen van belangen en te continueren diensten. Echter vraagt een stap naar digitale autonomie op opbouw van kennis en kunde, en dus inzet op meer samenwerking.
- Voornaamste redenen om te streven naar digitale autonomie zijn:
  - Grip op uitval van diensten (voor korte tijd, zoals een storing of voor langere tijd door uitval van een leverancier) en de impact daarvan (hersteltijden, backup oplossingen)
  - Begrip van complexiteit en betere wendbaarheid (zoals doorlooptijd migraties)
  - Keuzevrijheid
  - Zelfbeschikking versus leverancierslock-in (data, privacy, functionaliteiten, innovatie)

### **Een realistische eerste stap naar digitale autonomie**

De beschikbare capaciteit en middelen voor digitale autonomie van de gemeente zijn beperkt. De invloed op de belangrijke aspecten (marktaanbod, financieringsinstrumenten) zijn vanuit Amsterdam ook beperkt.

Verschillende huidige maatregelen versterken al digitale autonomie. Denk bijvoorbeeld aan het scheiden van data van applicaties of de inzichten uit business Continuïteitsmanagement waarbij gekeken wordt naar de continuïteit van de meest kritische bedrijfsprocessen. Ook zijn er verbeterprocessen, zoals de evaluatie op regie op applicaties die bij leveranciers staan en het inkoopproces. In deze verbeterprocessen zullen we digitale autonomie meenemen en verkennen wat er nodig is. Onderstaande maatregelen zijn gericht op het vergroten van digitale autonomie door risico's te beperken, beleidsstructuren te verbeteren, en technologische oplossingen te diversifiëren.

We versterken onze inzet op:

### 1. Samenwerking versterken Europees en landelijk: en stap naar digitale autonomie

Om onafhankelijk(er) van leveranciers te zijn is het noodzakelijk om intensiever samen te werken met andere overheden. Europese, nationale en lokale samenwerking op dit onderwerp versterken de positie van Amsterdam en Amsterdam zal haar beleid waar nodig herijken op basis van ontwikkelingen zoals Nederlandse Digitalisering Strategie (NDS). Deze maand ga ik hieronder ook in gesprek met de staatssecretaris van Digitale Zaken.

Dit doen we door:

- a. Kennis intern uit te breiden over IT die we gebruiken en over alternatieven van huidige producten. Denk bijvoorbeeld aan kennis opbouwen om beter open source producten te integreren met bestaande applicaties. Tegelijkertijd zetten we een stap in de samenwerking met andere gemeentes door het initiatief te nemen voor een uitvoeringsorganisatie die over en weer diensten levert tussen lokale overheden, natuurlijk samen met de VNG e.a.
- b. Amsterdam actief aan te laten sluiten op de visie en het beleidskader digitale autonomie en soevereiniteit overheid die voor de zomer van 2025 door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties gepubliceerd wordt. Deze zijn onderdeel van de Nederlandse Digitaliseringsstrategie (NDS). Aansluitend op de ambities van de NDS zullen we ook ons cloudbeleid en sourcingstrategie daarop aanpassen.

### 2. Regie op data

Om onafhankelijk(er) van leveranciers te zijn is het noodzakelijk om data en applicaties van elkaar te scheiden, zodat er gewisseld kan worden van leverancier als we dat willen. Daarom passen we de volgende principes toe:

- a. Contractueel blijft opgeslagen data altijd van de gemeente Amsterdam
- b. We slaan op conform algemene standaarden
- c. Amsterdam werkt vanuit het principe: de data is van de Amsterdammer en we slaan zo weinig mogelijk op (minimalisatie)

In de huidige geopolitieke context vraagt de toepassing van deze principes wat het college betreft om een extra stap. Daarom gaan we onderzoeken welke data we in eigen omgevingen willen opslaan, in plaats van alleen in de huidige public cloud omgeving. Hierbij kijken onder andere naar wat we als real time kopie en wat we als bron willen bewaren. Als we onze data (deels) in eigen beheer hebben kunnen we gemakkelijker wisselen van software en kunnen afhankelijkheden fors worden verminderd.

### 3. Digitaal onafhankelijke infrastructuur en applicaties

Om onafhankelijk(er) van leveranciers te zijn is het noodzakelijk om maatregelen te nemen om keuzevrijheid te creëren:

- a. Bij de komende aanbestedingen nemen we digitale autonomie mee als criterium om scherper te krijgen wat het vraagt, en om de markt uit te dagen met oplossingen te komen. De komende aanbestedingen voor de dienstverlening Public Cloud en HenT (hosting) zijn de eerste grote aanbestedingen waarin we dit gaan doen. Bij de aanbesteding dienstverlening Public Cloud vragen we 'Eén excellente opdrachtnemer die in staat is om de huidige dienstverlening op de Public Cloud van de stad (Azure) over te nemen, te beheren, te onderhouden en door te ontwikkelen'. In het contract komt de mogelijkheid om de inkoop van de diensten af te schalen

indien we naast Azure ook andere platformen gaan ondersteunen. Verder werken we criteria uit voor inkoop, dit doen we samen met AMS-institute en de VNG.

- b. We bevorderen digitale autonomie bij kritische bedrijfsprocessen en bijhorende applicaties door waar relevant ons huidig beleid op business continuïteitsmanagement te versterken (denk aan exit-plannen en aangescherpte afspraken over regie op de data).
- c. Bij keuzes rondom applicaties zullen we explicieter sturen op aansluiting op Common Ground en voldoen aan standaarden (zoals Europese standaarden voor steden met Living-in.EU). In Living-in.EU worden standaarden ontwikkeld voor inkoop van software zodat deze uitwisselbaar wordt tussen Europese steden. Als we samenwerken met andere organisaties kunnen we gemeenschappelijk (de facto) standaarden maken en zorgen dat er voldoende markt is voor leveranciers om verantwoorde producten te ontwikkelen.
- d. We werken mee aan de 'proof of concept' van de open source samenwerksoftware van het Rijk. Denk hierbij aan open source software voor werkplekken (inclusief software voor email, tekstverwerking en spreadsheets).
- e. We gaan concrete voorstellen doen voor experimenten voor software die we gebruiken voor interactie met Amsterdammers voor onze dienstverlening.

Aan de gemeenteraad worden keuzes voorgelegd op welke schaal en in welke breedte we dit gaan doen, inclusief de financiële consequenties op korte en lange termijn.

### **Tot slot**

De verkenning 'Versterking van Digitale Autonomie in Amsterdam' identificeert een dringende behoefte aan digitale autonomie om risico's te beheersen, zoals cyberdreigingen en de afhankelijkheid van een beperkt aantal leveranciers. Even overstappen is niet mogelijk. Om technische en financiële redenen, maar ook omdat het niet wenselijk is gezien de kwaliteit en continuïteit van onze dienstverlening: er is geen of beperkt aanbod wat aan onze eisen en wensen voldoet.

De beschreven maatregelen zijn erop gericht niet nog afhankelijker te worden. We maken geen apart actieplan voor digitale autonomie maar zorgen dat we dit onderdeel maken van ons huidig beleid. Stap voor stap worden we op die manier steeds autonomer, waarbij we ons aansluiten bij Europese en landelijke initiatieven.

## Inhoudsopgave

|   |    |
|---|----|
| Samenvatting .....  | 2  |
| Inhoudsopgave .....   | 6  |
| Digitale autonomie .....  | 7  |
| Wat is digitale autonomie? .....  | 8  |
| Waarom willen we digitale autonomie? .....  | 9  |
| Welke risico's brengt streven naar digitale autonomie? .....                          | 10 |
| Hoe werken andere overheden aan digitale autonomie? .....                             | 12 |
| Hoe ziet de IT in Amsterdam eruit? .....  | 15 |
| De stack van Amsterdam, het digitale bestemmingsplan .....                            | 16 |
| Cloud .....   | 17 |
| Inkoop .....  | 18 |
| Uitgaven .....  | 19 |
| 180 graden de andere kant op? .....   | 20 |
| Wat kan Amsterdam doen? .....   | 22 |
| Infrastructuur .....  | 24 |
| Platform .....  | 24 |
| Applicaties .....   | 26 |
| Aanbevelingen en mogelijke maatregelen .....  | 26 |
| 1. Samenwerking versterken: Europees en landelijk, stap naar digitale autonomie ..... | 26 |
| 2. Regie op data .....  | 27 |
| 3. Digitaal onafhankelijke infrastructuur en applicaties .....                        | 27 |
| Conclusies en Vervolgstappen .....  | 27 |
| Bijlagen .....  | 29 |
| Bijlage A - Wat is digitale autonomie? .....  | 30 |
| Bijlage B - Beleidsdocumenten en strategische notities .....                          | 32 |
| Bijlage C - Overzicht ontwikkelingen en samenwerkingsverbanden .....                  | 33 |
| Bijlage D - Geraadpleegde literatuur en bronnen .....                                 | 35 |

## Digitale autonomie

De gemeenteraad heeft op 28 maart 2024 unaniem ingestemd met het gewijzigde initiatiefvoorstel 'Amsterdam Digitaal Onafhankelijk' van het lid IJmker. Dit initiatiefvoorstel verzoekt om de gemeente Amsterdam minder afhankelijk te maken van grote techbedrijven voor haar digitale diensten en producten. In oktober 2024 heeft de Raad een raadsinformatiebrief met de tussenstand van de verkenning ontvangen.

De noodzaak om digitaal onafhankelijk te worden wordt al langer door de Europese Commissie geagendeerd. De Europese Commissie koerst al een aantal jaar op een Europa dat beter in staat is om meer in haar eigen behoefte te voorzien. Ook de Rijksoverheid heeft met de agenda DOSA (Agenda Digitale Open Strategische Autonomie, 2023) een richtinggevend document gepubliceerd waarin staat dat ook Nederland zich meer wil inzetten voor digitale autonomie. De nieuwe Nederlandse Digitaliseringsstrategie (NDS) zet deze koers voort.

De oproep voor meer digitale autonomie wordt breed gedeeld door Tweede Kamerleden zoals in het initiatiefvoorstel 'Wolken aan de Horizon', individuele experts en maatschappelijke instanties zoals Freedom Labs, Waag, Commons Network, PublicSpaces.

Om een geïnformeerde dialoog te voeren over wat Amsterdam kan doen om meer digitaal autonoom te zijn, behandelen we in deze verkenning de volgende punten:

- Wat is digitale autonomie?
- Waarom willen we digitale autonomie?
- Welke risico's brengt streven naar digitale autonomie?
- Hoe werken andere overheden aan digitale autonomie?

Vervolgens biedt dit rapport inzicht in de huidige stand van zaken:

- Hoe ziet de IT in Amsterdam eruit?
- Aan welke knoppen kan Amsterdam draaien?

Om op basis van deze inzichten te komen tot de contouren voor een actieplan om de digitale autonomie van Amsterdam tegen 2030 te versterken:

- Aanbevelingen en mogelijke maatregelen

## Wat is digitale autonomie?

### **Digitale autonomie =**

We streven naar digitale autonomie, en dat betekent dat we streven naar controle over onze data en IT-systemen, maatregelen voor veiligheid en privacy, interoperabiliteit en standaarden, strategische inkoop en wendbare en weerbare systemen.

In bijlage A is een uitgebreidere toelichting op verschillende definities.

Digitale autonomie is een groot en onbegrensd thema. Het gaat van eigenaarschap van internetkabels in de zee, grondstoffen om hardware te produceren, kennis om infrastructuur te beheren, tot grip op technologie om nepnieuws te voorkomen. Het gaat in deze verkenning om de digitale autonomie van de gemeentelijke diensten van de gemeente Amsterdam. Digitale autonomie van de stad (denk aan de digitale publieke ruimte, online leefwereld en connectiviteit) vraagt om een vervolgonderzoek.

Er worden verschillende termen gebruikt, zoals digitale onafhankelijkheid, strategische autonomie, digitale autonomie en digitale soevereiniteit en aanverwante termen zoals digitale gemeenschapsgoederen. In deze verkenning wordt de definitie van de Europese Commissie, de vertaling hiervan naar de Nederlandse Agenda DOSA en de definitie uit verkenning digitale autonomie van het Ministerie van BZK gehanteerd. Die luidt:

**We streven naar digitale autonomie, en dat betekent dat we streven naar controle over onze data en IT-systemen, maatregelen voor veiligheid en privacy, interoperabiliteit en standaarden, strategische inkoop en wendbare en weerbare systemen.**

Deze definitie is niet precies genoeg om bijvoorbeeld te werken aan inkoopvoorwaarden en andere maatregelen. Het Rijk werkt aan een Nederlandse Digitaliseringsstrategie (NDS). In de NDS is ook aandacht voor digitale autonomie. Dit wordt nader uitgewerkt in een visie en beleidskader 'digitale autonomie en soevereiniteit overheid' welke voor de zomer van 2025 door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties gepubliceerd wordt. Die definitie zullen we straks volgen. Het landelijke beleid en de definities vragen vervolgens om een verdieping en vertaling naar lokaal niveau. Hier wordt samengewerkt met o.a. Vereniging Nederlandse Gemeenten, Digicampus en AMS Institute.

## Waarom willen we digitale autonomie?

De groter wordende afhankelijkheid van een beperkt aantal spelers ('big tech') is zorgelijk. De gemeente Amsterdam kan het zich niet veroorloven om grote delen van haar bedrijfsvoering in de handen van een enkele partij te leggen. Voor het college gaat dit onderzoek dan ook over het goed organiseren van bedrijfscontinuïteit voor de dienstverlening aan onze inwoners.

In relatief korte tijd heeft digitale autonomie veel aandacht gekregen. De urgentie wordt breder gedeeld, maar de argumenten voor het belang hiervan zijn verschillend. Gaat het om bedrijfscontinuïteit van onze dienstverlening of zijn het maatregelen tegen big tech?

Voor de gemeente Amsterdam hoeft dit – in ieder geval in praktische zin – geen tegenstelling te zijn. Mocht een bewezen alternatief beter aansluiten bij onze waarden en de mogelijkheid bieden om onafhankelijk te worden van grote (commerciële) partijen dan kunnen we onderzoeken of overstappen mogelijk is en/of bij te dragen aan de ontwikkeling daarvan.

Voornaamste redenen om te streven naar digitale autonomie zijn:

- Grip op uitval van diensten (voor 1 dag, 1 week, 1 maand) en de impact daarvan (hersteltijden, backup oplossingen)
- Begrip van complexiteit en betere wendbaarheid (doorlooptijd migraties)
- Keuzevrijheid
- Zelfbeschikking versus leverancierslock-in (data, privacy, functionaliteiten, innovatie)

### Naderend "point of no return"

We komen op een punt waar afhankelijkheid dreigt van Amerikaanse infrastructuur en technologie. Dit betekent dat onze digitale infrastructuur afhangt van Amerikaanse kabelverbindingen en de bereidheid van de VS om ons te ondersteunen.

Deze boodschap werd door verschillende experts (onder andere het Rathenau Instituut, Wigo4it, individuele experts en bedrijven) onderschreven tijdens het Rondetafelgesprek van de vaste commissie Digitale Zaken van de Tweede Kamer in februari 2025 over 'Digitale soevereiniteit bij de Rijksoverheid'.

Veel digitale systemen worden door marktpartijen en niet door de gemeente zelf ontwikkeld. Deze systemen zijn in de loop van de tijd complexer geworden en met elkaar verweven. We zijn daardoor van deze leveranciers afhankelijk geworden. De gemeente beperkte zich tot het uitvragen, beoordelen en controleren van de levering van deze diensten. Maar daarvoor is ook technische kennis bij de gemeente nodig. Die technische kennis wordt vooral opgedaan door het bouwen en beheren van technische systemen, en dat doen we nu nog maar beperkt.

Er zijn voor gemeente specifieke toepassingen een beperkt aantal leveranciers. En overstappen is vaak een complexe en dure onderneming, waarvoor vaak ook expertise van de markt nodig is. Er zijn zorgen dat het niet lukt om tegen acceptabele kosten te wisselen van product of leverancier. Daarbij gebeurt het ook dat er helemaal geen oplossing is die voldoet aan de beleidswensen van de gemeente.

Daarbij leveren steeds meer partijen Software-as-a-Service. In dat model is het niet langer de gemeente die servers draait en beheert, maar de leverancier. Wat de vrijheidsgraden en de controle voor de gemeente minder maakt. Steeds vaker is SaaS de enige vorm waarin software wordt aangeboden.

De gemeente Amsterdam kan kiezen voor beste oplossing voor Amsterdam, waarbij afwegingen worden gemaakt over doel van de applicatie en kosten. Dat doet elke organisatie. Dat heeft ertoe geleid dat de gemeente afgelopen jaren een overstap heeft gemaakt naar voornamelijk Software as a Service (SaaS).

Veel SaaS-diensten worden geleverd door Amerikaanse bedrijven. En Europese SaaS-aanbieders maken grotendeels gebruik van Amerikaanse clouddiensten, zoals die van Amazon, Google en Microsoft. De Europese IT-sector raakt steeds meer verweven met Amerikaanse bedrijven. Als gevolg hiervan is het Nederlandse IT-denken grotendeels gebaseerd op niet-Europese technologieën, en alternatieven krijgen beperkt nog aandacht.

### **Rol gemeente Amsterdam**

De gemeente Amsterdam is wat betreft big tech vooral afhankelijk van Microsoft. Dit in cloud en kantoorautomatisering. Daarnaast is de stad is op allerlei aspecten digitaal afhankelijk van verschillende partijen, zoals bijvoorbeeld hardware, software, data-inwinning, glasvezelkabels en datacenters. We moeten onderscheid maken in afhankelijkheid, autonomie en rol van de gemeente hierin.

Voor digitale autonomie spelen Europese en Nationale belangen waar de gemeente Amsterdam een van de vele spelers is. Om digitale soevereiniteit te bereiken moet er gewerkt worden aan volledige controle en jurisdictie, nationale technologieën, onafhankelijkheid van externe invloeden, maximale veiligheid en versterken van weerbaarheid. Dat is aan de Europese Commissie en de Rijksoverheid. De gemeente kan hier wel een bijdrage aan leveren door te streven naar digitale autonomie.

Omdat als elke organisatie voor zichzelf de meest praktische oplossing kiest we als collectief voorbij het "point of no return" gaan en dus ook de gemeente niet meer voor die meest praktische oplossing kan kiezen. De rol van de gemeente is dus om actief bij te dragen aan digitale autonomie zodat we samen een veilige weerbare digitale infrastructuur kunnen gebruiken.

### **Welke risico's brengt streven naar digitale autonomie?**

We hebben het met name over de risico's van digitale afhankelijkheid. "De voornaamste drie aspecten van digitale onafhankelijkheid voor overheden zijn vertrouwelijkheid (wie kan er bij welke informatie?), wendbaarheid (ondersteunt IT de beleidskeuzes, of is de IT bepalend?) en weerbaarheid (is de organisatie in staat zelf IT weer werkend te krijgen na uitval?)", aldus experts<sup>1</sup> op het gebied van digitale autonomie.

Hoewel het nastreven van digitale autonomie belangrijk is, brengt het ook enkele risico's en uitdagingen met zich mee. Kunnen Europese oplossingen of common grond initiatieven genoemde risico's verminderen? Enkele mogelijke risico's van digitaal onafhankelijk zijn:

#### **1. Kosten en investeringen**

Het opzetten van lokale infrastructuren en ontwikkelen van digitale capaciteiten brengen hoge kosten met zich mee

#### **2. Complexiteit van beheer**

Lokale beheerprocessen kunnen complexer zijn dan het gebruik van beheerdiensten van gevestigde externe dienstverleners. Het vereist gespecialiseerde vaardigheden en middelen die niet direct beschikbaar zijn.

Het handhaven van lokale systemen en het regelmatig bijwerken van software en infrastructuur kan

---

<sup>1</sup> Deze indeling is gebaseerd op werk van expert Bert Hubert, berthub.eu.

arbeidsintensief zijn. Het risico van verouderde systemen neemt toe als er onvoldoende aandacht wordt besteed aan onderhoud.

In een verkaveld landschap zijn integratievraagstukken veel complexer: toegangsbeheer, connectiviteit, interoperabiliteit, etc.

3. **Afhankelijkheid van lokale experts**

Het opbouwen en behouden van lokale expertise kan een uitdaging zijn. Er kan een risico bestaan van afhankelijkheid van een beperkt aantal lokale experts, wat problematisch kan zijn bij personeelsverloop.

“War on Talent” - het werven, opleiden, en behouden van de juiste, soms geavanceerde, expertise is zeer schaars.

4. **Snelle technologische veroudering**

Lokale systemen kunnen sneller verouderen dan externe dienstverleners die voortdurend investeren in de nieuwste technologieën. Dit kan leiden tot het gebruik van verouderde systemen met verminderde functionaliteit en prestaties en daarmee toenemen van security risico's.

5. **Gebrek aan flexibiliteit**

Een rigide focus op digitale onafhankelijkheid kan leiden tot een gebrek aan flexibiliteit. Het kan moeilijk zijn om snel te reageren op veranderende bedrijfsbehoeften als gevolg van de noodzaak om lokale systemen aan te passen.

6. **Lokale infrastructuren**

Kunnen beperkte schaalbaarheid hebben in vergelijking met grootschalige externe cloudservices. Bij een plotselinge toename van de vraag kan het nodig zijn om snel uit te breiden, wat uitdagend kan zijn.

7. **Gemiste innovatiemogelijkheden**

Door te veel te focussen op digitale autonomie kunnen organisaties innovatiemogelijkheden missen die externe dienstverleners kunnen bieden. Dit kan leiden tot stagnatie in technologische vooruitgang.

8. **Belemmeringen bij aanbestedingen**

Complexe eisen ontmoedigen kleinere leveranciers en open source-oplossingen.

9. **Privacy en security**

Nu lijkt het alsof privacy en security dwingende redenen zijn om te streven naar digitale autonomie. Zorgen om privacy is een van argumenten welke genoemd zijn in het initiatiefvoorstel 'Amsterdam Digitaal Onafhankelijk'. Dat ligt genuanceerd: door het gebruik van bijvoorbeeld Microsoft<sup>365</sup> en Azure kunnen we gebruik maken van de enorme kennis, slagkracht en maatregelen van Microsoft om onze data te beveiligen tegen hacks of datalekken. In de vorige versie van de Amsterdamse Digitale Werkplek (ADW) hadden we dit nooit kunnen doen. Ook gaan we starten met Cloud for Sovereignty, wat juist is bedoeld om overheidsorganisaties volledige controle te geven over hun cloud-omgeving. Dat neemt niet weg dat er zorgen zijn over privacy en security. Denk bijvoorbeeld aan de inzet van Microsoft's kunstmatige intelligentie suite CoPilot. Deze zorgen en afwegingen zijn niet specifiek voor Amsterdam. Naast direct contact met Microsoft onderhouden we nauw contact met de Rijksoverheid. In dit geval overlegt zij met Microsoft over het verkleinen van de privacy risico's die kleven aan het gebruik van Microsoft 365 Copilot.

Terwijl digitale autonomie streeft naar meer controle over beveiliging, kan het ook leiden tot verhoogde veiligheidsrisico's. Lokale infrastructuren kunnen kwetsbaar zijn als ze niet adequaat worden beschermd tegen cyberbedreigingen, bijvoorbeeld omdat de specifieke kennis en kunde ontbreekt.

10. **Risico van puntoplossingen**

De aandacht van opiniemakers, onderzoekers en politici voor digitale onafhankelijkheid groeit. Op

verschillende plekken wordt gewerkt aan agenda's, denkkaders, nieuwe modellen van eigendom. Er ontstaan verschillende initiatieven om losse oplossingen te maken.

Het is belangrijk om deze risico's in overweging te nemen bij het streven naar digitale autonomie en een evenwicht te vinden tussen controle en de voordelen van externe dienstverlening. Een grondige risicoanalyse en een flexibele benadering zijn cruciaal om de nadelen te minimaliseren en de voordelen van digitale onafhankelijkheid te maximaliseren.

### Hoe werken andere overheden aan digitale autonomie?

De Amsterdamse inspanningen om digitale onafhankelijkheid te vergroten sluiten aan bij de inzet van steden zoals Rotterdam en Den Haag, waarbij technologie steeds vaker als strategisch hulpmiddel wordt ingezet.

In bijlage B is een uitgebreidere toelichting op hoe andere overheden werken aan digitale autonomie. Om een goede afweging te maken in Amsterdam is het zinvol om kennis te nemen van de ontwikkelingen bij de Rijksoverheid (waarin de ontwikkelingen van de Europese Commissie zijn meegenomen) en de Vereniging Nederlandse Gemeenten.

- **Europese Unie:** Digital Sovereignty-beweging met initiatieven zoals EDIC (European Digital Infrastructure Consortium).
- **Rijksoverheid:** Ontwikkeling van de Digitale Open Strategische Autonomie (DOSA) en implementatie van Europese wetgeving zoals de Data Act. Belangrijk is de ontwikkeling van de nieuwe NDS, de Nederlandse Digitaliseringsstrategie.
- **Technologische Trends:** Focus op open source, clouddiversiteit en cybersecuritystandaarden.

In februari 2025 heeft de vaste commissie Digitale Zaken van de Tweede Kamer een Rondetafelgesprek georganiseerd over 'Digitale soevereiniteit bij de Rijksoverheid'. De adviezen door onder andere het Rathenau Instituut, Wigo4it, individuele experts en bedrijven zijn naast de Rijksoverheid ook relevant voor andere overheden.

In 2023 lanceerde de Rijksoverheid de Agenda Digitale Open Strategische Autonomie (DOSA). In de DOSA wordt verwezen naar een open source strategie 'Opensource werken: de vrijblijvendheid voorbij' en als vervolg van de beleidslijn 'Open, tenzij...' uit 2020: de broncode van overheidssoftware (software gebruikt door de overheid) moet open source zijn, tenzij er gegronde redenen zijn hiervan af te wijken. Hierin staat ook argumentatie rond de Wet Open Overheid, het oprichten van Open Source Program Office (OSPO) en een 'open, tenzij' afwegingskader. In de DOSA wordt ook beschreven hoe het Kabinet aankijkt tegen digitale onafhankelijkheid en kantoorautomatisering. Het Ministerie van BZK is trekker van de verkenning Kantoorautomatisering voor de DOSA. De gemeente Amsterdam neemt deel aan deze verkenning.

Tweede Kamerlid Kathmann heeft in juni 2024 het initiatief genomen voor een debat over uitbesteding van ICT aan Big Tech. Samen met Tweede Kamerlid Dijkstra presenteerde zij op 18 juni 2024 namens GroenLinks-PvdA en NSC een initiatiefnota voor een Nederlandse Cloud, genaamd 'Wolken aan de Horizon'. Zij stellen dat sommige gemeenten een te grote leveranciersafhankelijkheid hebben. De Kamerleden zijn in september langs geweest bij het CIO-overleg van de G4. De G4 hebben hier een gezamenlijke reactie aangegeven en uitgesproken intensiever te willen samenwerken. Sindsdien zijn er in de Tweede Kamer verschillende moties geweest die digitale autonomie voor Nederland kunnen bevorderen.

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft in september 2024 een strategische verkenning naar digitale autonomie en de Rijksoverheid afgerond<sup>6</sup>. Deze strategische verkenning onderstreept het belang van een betrouwbare en bereikbare overheid die zelfstandig beslissingen kan nemen en opereren, zonder buitensporige afhankelijkheid van buitenlandse technologieën en diensten. Deze verkenning bevat een eerste aanzet richting een Actieagenda Digitale Autonomie (ADA). De verkenning voor de Rijksoverheid geeft een goed overzicht van de verschillende ontwikkelingen en aspecten van digitale autonomie. Op basis van deze verkenning ontwikkelt het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties een visie en strategie met daarin maatregelen. Denk daarbij aan een afwegingskader voor Cloud keuzes.

### **De Nederlandse Digitaliseringsstrategie**

De Nederlandse Digitaliseringsstrategie (NDS) 2025 is een initiatief van staatssecretaris Zsolt Szabó, gericht op het verantwoord inzetten van digitale technologie en het verbeteren van overheidsdienstverlening aan burgers en ondernemers.

De hoofddoelen van de NDS in 2025 zijn:

1. **Werken als één overheid:** Het streven is om burgers en ondernemers te bedienen als één samenhangende overheid, in plaats van als afzonderlijke organisaties. Dit moet het contact met de overheid vereenvoudigen en efficiënter maken.
2. **Verbeteren van digitale dienstverlening**
3. **Versterken van samenwerking binnen de overheid**
4. **Proactief inspelen op technologische ontwikkelingen**
5. **Verhogen van digitale weerbaarheid:** Het vergroten van de veiligheid en onafhankelijkheid van digitale systemen binnen de overheid is een prioriteit om bedreigingen het hoofd te bieden.
6. **Stimuleren van digitaal vakmanschap**

De NDS 2025 wordt in fases ontwikkeld. Van september tot en met november 2024 lag de focus op het opstarten en prioriteren van de strategie (fase 1: het 'wat'). Vanaf december 2024 richt men zich op het uitwerken en formaliseren (fase 2: het 'hoe'). De definitieve versie van de NDS wordt in het voorjaar van 2025 aan de Tweede Kamer aangeboden. Door deze strategie beoogt de overheid de digitale transitie in Nederland succesvol te begeleiden, met aandacht voor zowel kansen als risico's die digitalisering met zich meebrengt.

### **Prioriteiten van de NDS 2025**

In de startbrief over de Nederlandse Digitaliseringsstrategie (NDS) heeft staatssecretaris Zsolt Szabó zeven prioriteiten benoemd waarop de overheid zich zal richten:

1. **Goede dienstverlening van de overheid voor burgers en ondernemers:** Het verbeteren van de digitale interactie tussen overheid, burgers en bedrijven om deze begrijpelijk en toegankelijk te maken.
2. **Versterken van digitale weerbaarheid en autonomie:** Het vergroten van de veiligheid en onafhankelijkheid van digitale systemen binnen de overheid.
3. **Politiek-bestuurlijke aansturing en efficiëntere samenwerking als één overheid:** Het bevorderen van een geïntegreerde aanpak en samenwerking tussen verschillende overheidslagen en publieke dienstverleners.
4. **Digitaal vakmanschap:** Het ontwikkelen en versterken van digitale vaardigheden binnen de overheid om effectief gebruik te maken van technologische mogelijkheden.

5. **Artificiële Intelligentie (AI):** Het verkennen en verantwoord inzetten van AI-toepassingen binnen overheidsdiensten.
6. **Data:** Het verbeteren van data-uitwisseling en -gebruik binnen de overheid, met aandacht voor standaardisatie en veiligheid.
7. **Cloud:** Het onderzoeken en implementeren van cloudoplossingen om de digitale infrastructuur van de overheid te optimaliseren.

Deze prioriteiten worden de komende tijd verder uitgewerkt in de nieuwe NDS, die naar verwachting in het voorjaar van 2025 aan de Tweede Kamer zal worden aangeboden.

#### **VNG en G4**

De G4-samenwerking tussen Amsterdam, Rotterdam, Den Haag en Utrecht biedt een krachtig platform om als grote steden gezamenlijk op te treden en digitale uitdagingen te adresseren. Door onze gedeelde schaal, ambities en verantwoordelijkheden kunnen we versneld innoveren, kosten besparen en maatschappelijke impact realiseren. Focus in deze samenwerking is gericht op:

- Common ground: Het opbouwen van een toekomstbestendige digitale infrastructuur en applicatielandschap.
- Arbeidsmarktkrapte: Het ontwikkelen van innovatieve oplossingen om het tekort aan personeel het hoofd te bieden.
- Strategisch leveranciersmanagement en gezamenlijke inkoop: Een gezamenlijke aanpak richting leveranciers voor betere voorwaarden en risicobeheersing.
- AI en data: Verantwoord gebruik van AI en data, met aandacht voor ethische en transparante toepassingen.

De VNG werkt aan een position paper over digitale afhankelijkheid vanuit de VNG-commissiemijsie Digitale Samenleving. De VNG is ook betrokken bij de uitwerking van de NDS.

## Hoe ziet de IT in Amsterdam eruit?

De Amsterdamse IT is omvangrijk. We praten over ruim 20.000 werkplekken, 1.300 applicaties en meer dan 200 locaties.

De medewerkers hebben beschikking over een moderne werkplek op basis van Microsoft 365-producten, waarmee zowel thuiswerken als op kantoor werken wordt ondersteund. Het netwerk om op kantoor te werken is op meer dan 200 locaties beschikbaar. Deze locaties variëren van grote kantoorgebouwen tot kleine sportlocaties. Alle grote locaties zijn aangesloten op een eigen glasvezelnetwerk. Voor kleine locaties wordt gebruik gemaakt van beveiligde verbindingen over internet (SD-WAN).

De Basis IT Infrastructuur diensten zijn uitbesteed in vier kavels aan vier strategische leveranciers:

- Het netwerk / connectiviteit bij Proximus NXT
- De werkomgeving bij Sogeti
- Applicatiehosting en technisch applicatiebeheer bij KPN
- Security Dienstverlening bij Accenture

Daarnaast heeft de gemeente een cloudplatform op basis van Microsoft Azure, waar zelf ontwikkelde, maar ook opensource en closed source applicaties worden gehost. Verder is het dataplatform gerealiseerd op dit Azure.

In het totaal heeft Amsterdam zo'n 1.300 applicaties. Ongeveer de helft hiervan is centraal in beheer bij de directie Digitale Voorzieningen, het aandeel dat in beheer is groeit en het doel is om zoveel mogelijk centraal te beheren.

Van de 1.300 applicaties is ongeveer de helft SaaS (een afgenomen dienst, bij een externe leverancier). Daarnaast kennen we zo'n 150 applicaties gehost in het datacenters van KPN en een ongeveer even groot aantal applicaties gehost op ons eigen cloudplatform. De overige applicaties zijn voornamelijk werkplekapplicaties. Hieruit is te constateren dat de afhankelijkheid niet vanzelf minder zal worden. Dat is een bewust gevolg van de besluiten om de kern ICT-taken uit te besteden en om vooral voor SAAS-toepassingen te gaan.

In deze verkenning maken we onderscheid tussen:

1. Applicaties
2. Hosting
3. Generieke voorzieningen
4. Kennis en kunde

De voornaamste afhankelijkheden daarin zijn:

1. Applicaties & leveranciers
  - a. 1.300 applicaties, voornamelijk SAAS
  - b. Datedgedreven werken, inclusief AI-ondersteuning
  - c. Er zijn 'grote brokken' voor gestandaardiseerde, secundaire bedrijfsprocessen zoals:
    - i. CRM door Salesforce, ERP door SAP en ook leveranciers zoals Pinkroccade en Centric.
    - ii. Financiële systemen (inkomsten, beheer, uitgaven), payroll

- iii. Taak- en Zaaksystemen, inclusief interne ticket software (Case Management zoals ITSM).
- 2. Hosting
    - a. Applicaties worden gehost bij KPN/HenT of op het cloudplatform.
    - b. Enkele applicaties gericht op industriële automatisering draaien op VOR-IN.
    - c. SAAS-applicaties worden gehost op de hosting partij van de leverancier.
  - 3. Generieke voorzieningen
    - a. Kantoorautomatisering, met name de werkplek ADW met M365 van Microsoft.
    - b. Het cloudplatform Azure van Microsoft.
  - 4. Kennis en kunde
    - a. Op het cloudplatform Azure draaien ca. 70 applicaties ondersteund door DevOps-teams. Dat zijn teams die applicaties (door-)ontwikkelen en ondersteunen.
    - b. Er is interne kennis bij VOR-IN (zie kader).
    - c. Vanuit je regieverantwoordelijkheid wil je kennis in huis hebben over gemeentelijke processen. Op het moment dat we kiezen voor 'buy' moet een van de variabelen zijn voor de afweging of we de kennis om inhoudelijke regie op het proces te houden in huis heb. Regie is niet alleen een lijstje afvinken, dat betekent dat een dienst die je krijgt voldoet aan de eisen die je stelt en wat je nodig hebt. Onze regiefunctie op uitbestede diensten is wordt geëvalueerd.

**Een voorbeeld voor digitale autonomie is VOR-IN.**

VOR-IN is een autonoom operationeel ICT-netwerk van de directie Verkeer en Openbare ruimte ter ondersteuning van de gemeentelijke mobiliteitsketen. Er draaien (grotendeels eigen) applicaties op zoals aansturing van openbare verlichting, het Langzaam Verkeer Monitoringssysteem Amsterdam (LVMA), handhavingssysteem Cleopatra en dynamische verkeersinformatie.

VOR-IN is in 2016 begonnen met 2 servers en inmiddels een volwaardige functionaliteit die draait op eigen hardware met eigen beheer.

Er is interesse vanuit andere steden om hierop aan te sluiten. Het is belangrijk voor digitale autonomie om dit systeem te behouden en te bestendigen - denk daarbij aan personeelsplanning en het behouden van talent.

**De stack van Amsterdam, het digitale bestemmingsplan.**

Om sturing te geven aan de IT in Amsterdam is de enterprise architectuur belangrijk. De enterprise architectuur is te vergelijken met een bestemmingsplan. Hierin staat hoe al die 1.300 applicaties, platformen en koppelingen naar andere instanties zich tot elkaar moeten verhouden. En belangrijk, hierin staan ook de referentie-architecturen. Een referentiearchitectuur biedt een samenhangend overzicht van hoe mensen, processen en technologie in een sector samenwerken. Zo werken gemeenten samen met een referentiearchitectuur en dat zorgt ervoor dat diensten en producten uitwisselbaar zijn en op elkaar aansluiten. Als er in Amsterdam applicaties worden gekocht of gebouwd moeten deze passen in dit bestemmingsplan, de enterprise architectuur. In deze architectuur komen de regels,

waarden en bouwblokken voor de IT van Amsterdam samen. Sturing gebeurt dus voor een belangrijk deel via de architectuur.

## Cloud

Amsterdam neemt diensten af van alle grote platformproviders. Direct, en indirect via leveranciers (bijvoorbeeld: Amsterdam gebruikt Salesforce die op haar beurt weer gebruik maakt van AWS en Oracle). Amsterdam neemt verschillende clouddiensten af en je zou kunnen spreken van een multicloudstrategie. Echter heeft Amsterdam geen expliciete multicloudstrategie. Kennis, kunde en sturing in Amsterdam is georganiseerd rondom Microsoft's Azure.

De cloudstrategie beschrijft bovendien een prioritering van 'SaaS boven PaaS boven IaaS'. Dat wil zeggen: onder hosting vallen de infrastructuur (de hardware of capaciteit zoals rekenkracht en opslag dus IaaS) het platform (wat binnen Amsterdam bedoeld wordt als men spreekt over 'de Cloud' of het Cloudplatform dus PaaS). Onder applicaties vallen Software/Applicaties (dus SaaS). We focussen in de digitale autonomie discussie veel op het Cloudplatform en Microsoft, waarmee je dus juist een aantal onbekende risico's buiten de scope plaatst. Zo brengen SaaS partijen ook risico's met zich mee (en vaak maken ze van precies dezelfde platformen gebruik).

De Algemene Rekenkamer heeft in haar recente rapport "Rijk in de Wolken" stevige kritiek geuit op het gebruik van de cloud door ministeries. Begrippen als 'beperkt zicht', 'onvoldoende risicoafwegingen', en 'zorgwekkend gebrek aan controle' domineren de conclusies. De Algemene Rekenkamer wijst terecht op de risico's van data-soevereiniteit bij cloudgebruik, zoals een leverancierslock-in<sup>2</sup>, afhankelijkheid van buitenlandse partijen en het meekijken door andere overheden.

Wigo4it heeft gereageerd op het rapport. Wigo4it, de IT-organisatie van de vier grootste gemeenten (G4), bewijst dat grip op de cloud niet alleen haalbaar is, maar ook een fundament kan zijn voor succes en innovatie in het sociaal domein. Soortgelijke argumenten zijn ook genoemd in de Amsterdamse Cloudstrategie van 2020-2022.

Amsterdam heeft in 2022 een DPIA (Data Protection Impact Assessment) en DTIA (Data Transfer Impact Assessment) gedaan voor de cloudvoorziening. De cloudvoorziening is Azure Cloud van Microsoft waar hosting en applicatiebouw plaatsvindt. Onderdelen van deze dienstverlening (bv: hosting) waren al in werking; en vinden bijvoorbeeld al in HenT-datacentra (hosting bij KPN) plaats. De DTIA en DPIA geven een beeld van de informatieverwerking van bijvoorbeeld persoonsgegevens en van de risico's. En helpt de juiste maatregelen te formuleren.

Een belangrijke constatering in 2022 was dat het vrij onwaarschijnlijk is dat er verzoeken of inzage in persoonsgegevens zal worden gevraagd door opsporings- of inlichtingendiensten in de VS. Navraag leverde de bevestiging dat er tot op heden geen inzageverzoeken bekend zijn over overheidsorganisaties zoals gemeenten. Dit wordt ook aangegeven in het rapport van de Algemene Rekenkamer.

---

<sup>2</sup> Een vendor lock-in is het verschijnsel dat een organisatie zo afhankelijk wordt van een leverancier dat afscheid nemen of overstappen niet mogelijk is zonder grote (financiële) gevolgen.

Ondanks de onwaarschijnlijkheid op inzageverzoeken van publieke autoriteiten zijn wel specifieke technische maatregelen getroffen. We zijn nu de Hoogvertrouwelijke Landingzone aan het inrichten. Die is nog niet 'af'. De doorlooptijd is lang omdat het complexe materie is rondom cryptografie. Amsterdam heeft in deze landingzones de encryptiesleutels in eigen beheer en daardoor heeft de leverancier geen toegang tot de informatie. De maatregel wordt van toepassing op BBN2+ en bijzondere persoonsgegevens. BBN2+ is in het leven geroepen omdat het voor gemeenten soms noodzakelijk is om aanvullende maatregelen te nemen boven BBN2. Voor overige gegevens (BBN2) zijn bestaande maatregelen voldoende.

Er is kritiek<sup>3</sup> op het gebruik van Microsoft en encryptiesleutels. Die zorgen zijn er bij andere platforms ook. Een voorbeeld van zo'n zorg is dat Microsoft ongevraagd co-pilot aan wil zetten en de gemeente dat weer uit moet zetten. Dat is de omgekeerde wereld. De geopolitieke situatie vraagt erom om scherp te blijven. Het is niet zo dat als de Amerikaanse overheid nog geen informatie opgevraagd heeft bij de gemeente Amsterdam, dit ook nooit zal gebeuren.

Elke leveranciersafhankelijkheid is een risico. Dat zal ook zijn met Europese of lokale cloudproviders. Willen we alle risico's nagenoeg uitsluiten, dan moeten we alle infrastructuur in eigen huis nemen en ontwikkelen en beheer ook zelf uitvoeren. Dat is op lokaal niveau geen reëel scenario. Belangrijkste is daarom dat we nu onze informatie goed beschermd hebben en dat we constateren dat dit niet iets is wat we lokaal moeten organiseren.

Kortom: we hebben een DTIA, een DPIA en we werken aan een Hoogvertrouwelijke Landingzone. We werken binnen Azure aan het uitwijken naar andere locaties. Als we dat gereed hebben kunnen we kijken naar andere aanbieders. Het vraagt een continu risicoafwegingen.

Dit geldt voor alles binnen het cloudplatform. Niet alles draait in Amsterdam via het cloudplatform. De verschillende diensten zijn verantwoordelijk voor DPIA's en DTIA's voor de applicaties die zij inkopen.

We onderschrijven de reactie van wigo4it: "Het rapport van de Algemene Rekenkamer is waardevol als wake-up call. Maar laten we niet vervallen in doemdenken. De vraag is niet óf de overheid de cloud aankan, maar hóe we er samen voor zorgen dat het werkt." Staatssecretaris Szabó schreef in zijn reactie op de Kamerbrief evaluatie Rijksbreed cloudbeleid dat de inzet op cloudbeleid voor de hele overheid moet. Die beweging zetten we ook in met de Nederlandse Digitaliseringstrategie.

## Inkoop

Een van de aspecten voor digitale autonomie is dat we indien nodig kunnen migreren naar een ander platform. Daarvoor is nodig dat er andere aanbieders zijn die kunnen leveren op een schaal van Amsterdam. De IT van Amsterdam is omvangrijk en het verschilt per applicatie, maar in algemene zin zien we dat de GovTech markt bestaat uit enkele leveranciers. Er zijn voor verschillende applicaties ook alternatieven, maar die worden de aanbestedingen niet gegund. Dit niet op de laatste plaats omdat zij niet meedingen op de aanbestedingen.

Een van de aannames is dat dit komt omdat het beeld is dat de gemeente veel voorwaarden stelt aan haar inkoop. De inkoopvoorwaarden van de gemeente zijn omvangrijk. Op de site<sup>4</sup> van Amsterdam kan een leverancier zien waar zij aan moet voldoen als je aan de gemeente Amsterdam levert. Aan deze voorwaarden kunnen aanvullende eisen gesteld worden, zoals bijvoorbeeld gebeurt met een data-

---

<sup>3</sup> <https://berthub.eu/articles/posts/servers-in-de-eu-eigen-sleutels-helpt-het/>

<sup>4</sup> [www.amsterdam.nl/ondernemen/inkoop-opdrachten/maatschappelijke-doelen-inkoopbeleid](http://www.amsterdam.nl/ondernemen/inkoop-opdrachten/maatschappelijke-doelen-inkoopbeleid)

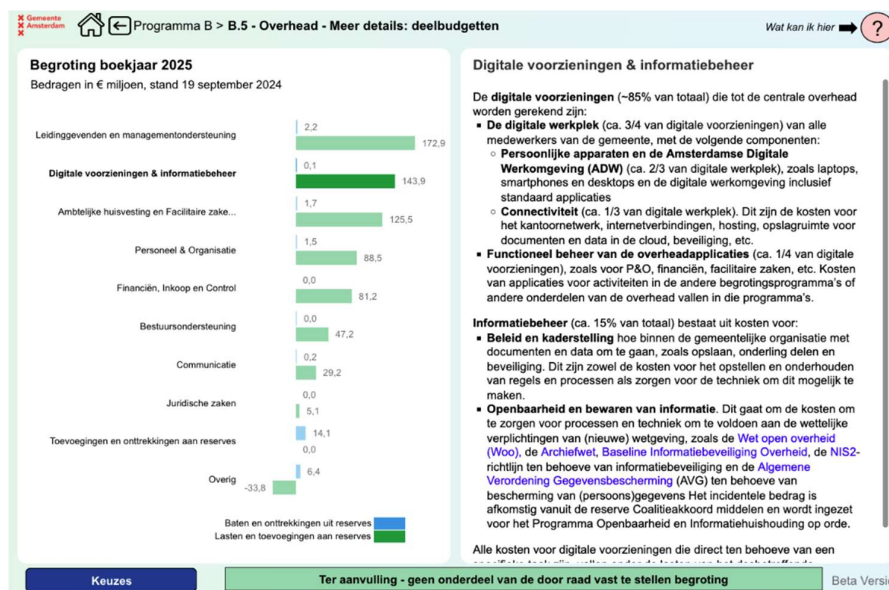
paragraaf wanneer er afspraken gemaakt moeten worden over het gebruik van data door een leverancier. In de inkoopvoorwaarden worden bijvoorbeeld afspraken gemaakt over wat te doen als ene leverancier onverhoopt uitvalt en hoe dan een exit-plan wordt opgesteld.

Een tweede aanname is dat marktpartijen te laat kunnen zien wat ingekocht wordt door de gemeente. Daarvoor is de inkoopkalender ontwikkeld. Een derde aanname is dat nieuwe leveranciers niet voldoen aan vereisten zoals certificering of bedrijfsgrootte.

Het raadsinitiatief Amsterdam Digitaal Onafhankelijk vraagt expliciet inkoopvoorwaarden voor digitale autonomie te verkennen. Samen met het AMS-instituut is een prototype van een inkooptool voor digitale autonomie bij het inkoopproces van digitale diensten van gemeenten getest<sup>5</sup>. Dit heeft inzicht gegeven in hoe digitale autonomie praktisch te vertalen naar inkoopvoorwaarden. Ondertussen wordt bij het Rijk gewerkt aan inkoop en digitale autonomie. Samen met de VNG en het AMS-instituut worden inkoopvoorwaarden verder verkend.

## Uitgaven

In de begroting van de gemeente Amsterdam voor 2025 worden de kosten voor digitale voorzieningen als volgt weergegeven (interactief te raadplegen op [magazines.amsterdam.nl/begroting-2025](https://magazines.amsterdam.nl/begroting-2025)):



De digitale voorzieningen (~85% van totaal) die tot de centrale overhead worden gerekend zijn:

- De digitale werkkplek (ca. 3/4<sup>e</sup> van digitale voorzieningen) van alle medewerkers van de gemeente, met de volgende componenten:

<sup>5</sup> <https://responsiblesensinglab.org/nl/projecten/prototype-inkooptool-voor-autonoom-inkoopproces-digitale-diensten-van-gemeenten>

- o Door Amsterdam uitgegeven en beheerde Persoonlijke apparaten en de Amsterdamse Digitale Werkomgeving (ADW) (ca. 2/3<sup>e</sup> van de digitale werkplek), zoals laptops, smartphones en desktops en de digitale werkomgeving inclusief standaard applicaties
- o Connectiviteit (ca. 1/3<sup>e</sup> van digitale werkplek). Dit zijn de kosten voor het kantoor netwerk, internetverbindingen, hosting, opslagruimte voor documenten en data in de cloud, beveiliging, etc.
- Functioneel beheer van de overheadapplicaties (ca. 1/4 van digitale voorzieningen), zoals voor P&O, financiën, facilitaire zaken, etc. Kosten van applicaties voor activiteiten in de andere begrotingsprogramma's of andere onderdelen van de overhead vallen in die programma's.

Informatiebeheer (ca. 15% van totaal) bestaat uit kosten voor:

- Beleid en kaderstelling hoe binnen de gemeentelijke organisatie met documenten en data om te gaan, zoals opslaan, onderling delen en beveiliging. Dit zijn zowel de kosten voor het opstellen en onderhouden van regels en processen als zorgen voor de techniek om dit mogelijk te maken.
- Openbaarheid en bewaren van informatie. Dit gaat om de kosten om te zorgen voor processen en techniek om te voldoen aan de wettelijke verplichtingen van (nieuwe) wetgeving, zoals de [Wet open overheid \(Woo\)](#), de [Archiefwet](#), [Baseline Informatiebeveiliging Overheid](#), de [NIS2-richtlijn](#) ten behoeve van informatiebeveiliging en de [Algemene Verordening Gegevensbescherming](#) (AVG) ten behoeve van bescherming van (persoons)gegevens Het incidentele bedrag is afkomstig vanuit de reserve Coalitieakkoord middelen en wordt ingezet voor het Programma Openbaarheid en Informatiehuishouding op orde.

Alle kosten voor digitale voorzieningen die direct ten behoeve van een specifieke taak zijn, vallen onder de lasten van het desbetreffende begrotingsonderdeel en vallen dus niet binnen dit budget.

## 180 graden de andere kant op?

De afgelopen jaren zijn belangrijke beslissingen genomen die van invloed zijn op de digitale autonomie van de gemeente nu.

### 2017-2020: van zelf in beheer naar de markt.

Met de uniformering van 40+ separate IT-landschappen ging de gemeente van 5.931 naar 1.100 applicaties. Tegelijkertijd zijn diensten die tot dan toe in eigen beheer waren - zoals toegangsbeheer, werkplekbeheer, netwerk en een deel van de hosting - uitbesteed aan de markt.

### 2020 tot nu: Ingekocht waar mogelijk, eigen oplossingen waar nodig.

In de bestuursopdracht i-domein in 2020 zijn de uitgangspunten voor het i-domein vastgesteld. Bijvoorbeeld zo veel mogelijk gebruik van open source en open standaarden. Andere voorbeelden hiervan zijn:

- **Migratie naar de Cloud**  
Eén stedelijk generieke clouddienst, zodat de organisatie ontlast wordt in beheer. Dit zodat gegevens beter ontsloten kunnen worden en de infrastructuur voldoet aan de strenger worden veiligheidseisen.
- **Common ground**  
Open source en samenwerken met andere overheden voor ontwikkeling en beheer heeft

regelmatig aandacht. Bijvoorbeeld met common ground. Dat heeft enkele mooie voorbeelden opgeleverd, zoals Signalen.

**Een voorbeeld:**

**Sommige toepassingen maken we zelf in Amsterdam.**

In het verleden heeft de gemeente Datapunt zelf ontwikkeld. Met een 100% open stack.

Inmiddels is Datapunt volledig opgenomen in het Dataplatform op de omgeving van Microsoft Azure.

## Wat kan Amsterdam doen?

Iedereen wil meer digitale autonomie, maar niemand weet precies waar te beginnen, omdat het een groot en onbegrensd thema is. Digitale autonomie komt niet vanzelf. We moeten verschillende beleidsdoelen, agenda's, partijen en middelen verbinden. Dat moet lokaal, maar vooral ook landelijk en Europees. Hierbij is het van belang om oud (huidige systemen en processen) te kunnen verbinden met nieuw (data wallets, data spaces, AI).

Maatregelen voor het versterken van digitale autonomie hangen nauw samen met het informatiebeleid, financiering en keuzes bij het Rijk en de Europese Commissie. De vraag is waar de lokale overheid in deze opgave verschil maakt. Daarom focussen we in deze verkenning op de rol van de lokale overheid, erop vertrouwend dat de Rijksoverheid stevig inzet op digitale autonomie. De ontwikkelingen rondom de Nederlandse Digitaliseringsstrategie geven in ieder geval dat signaal af.

### Wat zijn de knoppen?

In algemene zin kan Amsterdam:

- Koers waarop beleid kan worden aangepast;
- Inkoop (zoals voorwaarden, inbesteden in plaats van uitbesteden, en het stimuleren van de markt zodat er andere aanbieders ontstaan en er keuzevrijheid ontstaat);
- Grip op uitval van diensten en de impact daarvan;
- Regie op data (zoals data onafhankelijk maken van applicaties);
- Samenwerking op inkoop en uitvoering (zoals een uitvoeringscoöperatie);
- Aansluiten op standaarden en samenwerkingen (zoals Common Ground en Living-in.EU);
- Vergroten van begrip van complexiteit en betere wendbaarheid (zoals versterken inhoudelijke regie op ingekochte software en ruimte voor open source);
- Lobby voor zaken waar de invloed van de gemeente beperkt is (zoals voor financiering, stimulering van alternatieven en reactie op geopolitieke ontwikkeling).

### Waar is onze invloed beperkt?

In algemene zin heeft Amsterdam beperkte invloed op:

- Marktaanbod (inclusief digitale gemeenschapsgoederen);
- Aanpak in Nationaal en Europees verband (zoals regelgeving en investering);
- Voorwaarden voor ontwikkeling en groei van alternatieve diensten (zoals een stimuleringsfonds);
- Risico's van puntoplossingen (op verschillende plekken wordt gewerkt aan agenda's en maatregelen. Er ontstaan verschillende initiatieven om losse oplossingen te maken);
- Financieringsinstrumenten voor (noodzakelijke) samenwerking op uitvoering, zoals een uitvoeringscoöperatie) en gezamenlijke kennisontwikkeling.

### Overwegingen die hierbij een rol spelen zijn:

- Digitale autonomie vereist vaak hogere initiële kosten en langere implementatietijden. Dus een langere termijn aanpak hierop is cruciaal.
- Strategisch management is belangrijk: architectuur volgt de business afweging, en dat kan afwijken van het belang voor digitale autonomie.
- Digitale autonomie vereist inleveren van lokale beleidsautonomie. Concreet betekent dat geen typische Amsterdam oplossingen meer die zich vertalen in IT-oplossingen. Samenwerken met andere gemeenten vraagt rigoureuze vereenvoudiging van bijvoorbeeld vergunningen (zoals

parkeren) en ontheffingen (landelijke regeling), maar ook onze communicatiekanalen en dienstverlening uniformeren met andere gemeenten.

- Tempo bepalen (waarin volgen en waarin voorlopen). Migreren kan niet altijd zomaar, daarvoor moeten bijvoorbeeld exitstrategieën en raamovereenkomsten in orde zijn, data gescheiden van applicaties zijn, en er simpelweg andere mogelijkheden op de markt zijn.

Dit vraagt om keuzes en inzet die ervoor zorgen dat:

- Wisselen van leverancier eenvoudiger wordt (grip op IT)
- Aanbod om naartoe te wisselen versterkt wordt (stimuleren en samenwerken met GovTech)

Belangrijk hierbij is dat de kwaliteit van onze dienstverlening op peil blijft en dat de maatregelen beoordeeld worden in de context van beperkt beschikbare middelen.

### Verschillende lagen van technologie

We maken hierbij onderscheid in verschillende lagen, zoals applicaties, data, hosting, generieke voorzieningen en kennis en kunde. Op elk van deze lagen verschilt ambitieniveau. Zo is voor de generieke voorziening Cloudplatform diversifiëren (zorgen dat we meerdere leveranciers hebben) op dit moment erg kostbaar, als dit technisch al haalbaar is. Wel zullen we hiervoor in de volgende aanbestedingen aandacht hebben voor digitale autonomie en zorgen voor flexibiliteit.

Voor de data-laag is het versterken van digitale autonomie door data-minimalisatie en het scheiden van data van applicaties al huidig beleid. Aanvullende maatregelen, zoals extra data-backups worden onderzocht op nut en noodzaak. Bij elke laag verschilt de afhankelijkheid en de risico's hierin. De kern van meer digitale autonomie is om voor elk van deze lagen te diversifiëren in leveranciers om de continuïteit van dienstverlening te kunnen waarborgen.

Hieronder gaan we gedetailleerder in op infrastructuur en platform. Onder hosting vallen de infrastructuur (de hardware of capaciteit zoals rekenkracht en opslag dus IaaS) het platform (wat binnen Amsterdam bedoeld wordt als men spreekt over 'de Cloud' of het Cloudplatform dus PaaS). Onder applicaties vallen Software/Applicaties (dus SaaS). Hiervoor geldt dat als de gemeente een voorkeursbeleid heeft voor (open source, tenzij) dat open-source oplossingen dit digitale autonomie. Dit vraagt wel om nuance: open source is – zeker gezien de focus op kernprocessen – geen magische oplossing omdat voor die processen de inschatting is dat er beperkter open source beschikbaar is. Dat neemt niet weg dat actiever inzetten op opensourcesoftware bij kan dragen. Actiever inzetten vraagt een investering in de vakgroep softwareontwikkeling en randvoorwaarden zoals continuering van gestandaardiseerde hosting van de open source applicaties en investeren in de opensource community. Dit kan overwogen worden als het sourcingsbeleid wordt bijgewerkt.

Naast applicaties hosting, generieke voorzieningen Er zijn ook andere onderdelen, zoals connectiviteit (WAN en (W)LAN) en de Amsterdam Digitale Werkomgeving (ADW).

|      |            | Huidige kennis in huis:   | Voorgestelde beweging:                | Dat vraagt:   | Financiële impact: |
|------|------------|---|---------------------------------------|---|--------------------|
| IaaS | HenT (KPN) | 'Kale' regie bij Dienstverlening en Samenwerking. Inhoudelijke kennis bij afdeling Platformen en Softwareontwikkeling | Naar volwassen ook inhoudelijke regie | Meer technische architectuur kennis in huis voor sterkere regievoering. | Beperkt            |

|      |                 |                                       |   |  |                                     |
|------|-----------------|---------------------------------------|---|--|-------------------------------------|
| PaaS | Microsoft Azure | Over Azure                            | Samen met de andere overheden opbouwen kennis en ervaring met andere PaaS-leveranciers (Hyperscalers of anders) | Brede samenwerking binnen de overheid                                  | Afhankelijk van financierings keuze |
| SaaS | Divers          | Wisselend, over het algemeen minimaal | Ook regie voeren op SaaS. Ontkoppeling op Dataniveau organiseren.   | Visie en uitgewerkte kaders/standaarden. Actief bewerken van de markt. | Per domein verschillend             |

## Infrastructuur

De Hosting en TAB (HenT) verzorgt de hosting en het technisch applicatiebeheer van businessapplicaties. Het grootste gedeelte van de applicaties (150) is in beheer bij de strategisch partner (KPN). Inmiddels staat er vrijwel niets meer in onze eigen datacenters en is alles gemigreerd naar HenT, Cloud of SaaS.

De diensten neemt Amsterdam af. De technisch inhoudelijke kennis bij de gemeente Amsterdam is beperkt, lees de kennis die in huis is opgebouwd door en voor het gebruik van de platformen.

### Keuzemogelijkheden:

- Zelf hardware in huis en beheren
- Hardware uitbesteden en beheer en regie in nauwe samenwerking met leverancier
- Volledig uitbesteden

### Afweging:

De impact die deze laag maakt op digitale autonomie is beperkt. Er zijn verschillende leveranciers die dit kunnen leveren. Wisselen van leverancier is ingewikkeld, maar niet ondoenlijk. Er is in het verleden bewust gekozen voor een Nederlandse leverancier.

Bovendien is de leverancier maar beperkt bepalend voor de technologie die wordt gebruikt, die wordt namelijk bepaald door de (los van elkaar door de tijd heen aangeschafte) applicaties. Deze applicaties zijn bepalend voor onderliggende besturingssystemen, databasesystemen, etc. De afhankelijkheid van de huidige leverancier is vooral groot doordat kennis van integratie van applicatie en infrastructuur voornamelijk bij de leverancier ligt en Amsterdam hier zelf beperkte kennis van heeft. Dit maakt een goede manier regie voeren, of de transitie na een volgende aanbesteding uitvoeren minder makkelijk.

Amsterdam evalueert haar regierol. Deze rol zal ook bij volgende leveranciers nodig zijn. De diensten nemen we af van een partij die is gevestigd in Nederland en waarbij data de Europese unie niet verlaat. Deze kennisopbouw vergroot de mogelijkheden om de laag infrastructuur samen met andere gemeenten af te nemen.

## Platform

Amsterdam maakt nu gebruik van PAAS, platform-as-a-service. Waarbij in theorie alle platformen mogelijk zijn wordt in de praktijk nagenoeg alles bij Microsoft Azure ondergebracht. Amsterdam kan het hele aanbod van Azure afnemen. Dit aanbod met innovatieve functies zijn nodig voor de diensten die nu worden geleverd.

De inzet om een cloudplatform te ondersteunen en leveren is ca. 4 miljoen euro per jaar aan exploitatielasten. Dat bestaat uit kennis en kunde om adequaat regie te voeren op het gebruik van een platform. Denk hiervan aan de inrichting, toegangsbeheer, compliance, security, dienstverlening aan collega's om toepassingen te migreren naar Azure (bijvoorbeeld Parkeren).

Dit zijn de kosten voor de regievoering voor Azure. Daarnaast zijn er kosten per gebruik van de diensten, zoals voor het draaien van de 150 applicaties. Andere mogelijke platformen zijn AWS en Google. Kosten om een ander platform te ondersteunen zijn eenzelfde orde van grootte. Om een ander platform te ondersteunen (multicloud) moet meer interne kennis en kunde worden opgebouwd.

#### **Keuzes:**

- Continueren van inzet op migratie naar Azure
- Zelf diversifiëren (naast Azure ook AWS en Google actief ondersteunen)
- Samen diversifiëren (platform van Amsterdam aanbieden aan andere gemeenten en met het vrijgekomen budget door schaalvoordeel een tweede platform ondersteunen)

#### **Afweging:**

- Dekt de multicloudstrategie de risico's af die je af wil dekken? Een tweede of derde platform ondersteunen voor Amsterdam levert beperkte voordelen ten opzichte van de kosten.
- Met redelijk beperkte extra kosten kunnen we de PAAS omgeving inrichten voor G4 en anderen (zoals Zaanstad en Delft). De kosten daarvoor zijn niet x keer het aantal gemeenten, maar slechts een beetje meer per gemeente die aansluit.
- Vanuit je regie moet je weten wat de ketenafhankelijkheid is bij andere producten (dus AWS of Google). Beperkte ondersteuning hierop heeft risico's. Die zijn er nu ook. Die accepteren we dan expliciet.
- Naast de Big Tech platform aanbieders zijn er op dit moment geen leveranciers die op de schaal van de gemeente Amsterdam kunnen leveren. De markt is wel in beweging en bij keuzes is flexibiliteit inbouwen wenselijk om hierop in te kunnen spelen. Dit gaat over functionaliteit op het gebied van compliance en security die we hiervoor niet tot onze beschikbaarheid hadden. Zo is ook cybersecurity in 10-15 jaar gegroeid van een 'non-functional' (een contract) naar een functionele requirement. Er wordt ingezet op een scala aan security-inzichten waar op geacteerd kan worden. Dat was hiervoor nauwelijks mogelijk. Op dit moment bieden helaas alleen grote cloudpartijen deze inzichten aan omdat zij in staat zijn hierin te investeren.

#### **Voorgestelde verandering:**

- a. Samen met andere overheden in lijn met de Nederlandse Digitaliseringsstrategie (NDS) werken aan Europese initiatieven.
- b. Kennis intern opbouwen zodat we beter begrip hebben van de IT die we gebruiken, en hierdoor tegelijkertijd een stap zetten in de samenwerking met andere gemeente door het initiatief te nemen voor een uitvoeringsorganisatie die over en weer diensten levert tussen lokale overheden. Dit doen we samen met de VNG e.a. Bijvoorbeeld door actief de diensten van de afdeling platform van de gemeente Amsterdam in te zetten in samenwerking met andere gemeenten. Dat schaalvoordeel levert ruimte op om kennis en kunde op te bouwen voor andere platforms.

## Applicaties

Het applicatielandschap van de gemeente bestaat uit ongeveer 1.300 applicaties. Dit zijn voornamelijk SaaS applicaties. Er zijn 'grote brokken' voor gestandaardiseerde, secundaire bedrijfsprocessen zoals

- CRM door Salesforce, ERP door SAP en ook leveranciers zoals Pinkroccade en Centric;
- Financiële systemen (inkomsten, beheer, uitgaven), payrolling;
- Taak- en Zaaksystemen, inclusief interne ticket software (Case Management zoals ITSM).

Security eisen en gebruikersgemak zijn redenen om steeds vaker te kiezen voor 'suites'. Dat zijn grotere pakketten software die goed met elkaar geïntegreerd zijn. Overigens zijn alternatieven met meerdere systemen die samenwerken een mogelijkheid. Echter vraagt dat interne kennis die we daarvoor eerst moeten opbouwen. Nu doen we het tegenovergestelde: we gaan van losse applicaties naar grote suites.

Voor kantoorapplicaties werkt de gemeente mee met OpenBureau. Dat is een proof of concept vanuit de OPSO (Open Source Office) van het Ministerie van Binnenlandse Zaken voor Rijksoverheid om te bewijzen dat open source kantoorautomatisering een bruikbaar alternatief is. Hier worden in 2025 de eerste bevindingen verwacht.

### Keuzes:

- Voor gemeentespecifieke toepassingen sturen op Common Ground (zoals met applicaties als OpenStad en Signalen).
- Expliciet sturen op voldoen aan standaarden en interoperabiliteit (met mogelijk extra kosten)
- Expliciet sturen op open source. Dat betekent bijvoorbeeld interne kennisopbouw om open source pakketten aan elkaar te koppelen als tegenhanger voor 'suites'.
- Geen bedrijfsspecifieke applicaties meer ombouwen naar Microsoft's Sharepoint.

### Afwegingen:

- Diversifiëren betekent extra kosten: In de praktijk betaal je bij Microsoft voor het hele pakket, dus als je een onderdeel ergens anders ook neerzet betaal je dubbel.
- Security eisen en gebruikersgemak zijn redenen om steeds vaker te kiezen voor 'suites'. Dat zijn grotere pakketten software die goed met elkaar geïntegreerd zijn.

## Aanbevelingen en mogelijke maatregelen

Verschillende huidige maatregelen versterken al digitale autonomie. In deze verbeterprocessen zullen we digitale autonomie meenemen en verkennen wat er nodig is. Denk hierbij aan de evaluatie van de regiefunctie (zoals interne kennis over ingekochte software) en het verbeteren van het inkoopproces. Onderstaande maatregelen zijn gericht op het vergroten van digitale autonomie door risico's te beperken, beleidsstructuren te verbeteren, en technologische oplossingen te diversifiëren.

We versterken onze inzet op:

### 1. Samenwerking versterken: Europees en landelijk, stap naar digitale autonomie

Om onafhankelijk(er) van leveranciers te zijn is het noodzakelijk om intensiever samen te werken met andere overheden. Europese, nationale en lokale samenwerking op dit onderwerp versterken de positie

van Amsterdam en Amsterdam zal haar beleid waar nodig herijken op basis van ontwikkelingen zoals Nederlandse Digitalisering Strategie (NDS). Dit doen we door:

- a. Kennis intern op te bouwen, zodat we beter begrip hebben van de IT die we gebruiken. En hierdoor tegelijkertijd een stap te zetten in de samenwerking met andere gemeentes door het initiatief te nemen voor een uitvoeringsorganisatie die over en weer diensten levert tussen lokale overheden, natuurlijk samen met de VNG e.a.
- b. Amsterdam actief aan te laten sluiten op de visie en het beleidskader digitale autonomie en soevereiniteit overheid die voor de zomer van 2025 door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties gepubliceerd wordt. Deze zijn onderdeel van de Nederlandse Digitaliseringsstrategie (NDS). Aansluitend op de ambities van de NDS zullen we ook ons cloudbeleid en sourcingstrategie daarop aanpassen.

## 2. Regie op data

Om onafhankelijk(er) van leveranciers te zijn is het noodzakelijk om data en applicaties van elkaar te scheiden, zodat er gewisseld kan worden van leverancier als we dat willen. Daarom passen we de volgende principes toe:

- a. Contractueel blijft opgeslagen data altijd van de gemeente Amsterdam
- b. We slaan op conform algemene standaarden
- c. Amsterdam werkt vanuit het principe: de data is van de Amsterdammer en we slaan zo weinig mogelijk op (minimalisatie).

## 3. Digitaal onafhankelijke infrastructuur en applicaties

Om onafhankelijk(er) van leveranciers te zijn is het noodzakelijk om maatregelen te nemen om keuzevrijheid te creëren:

- a. Bij de komende aanbestedingen nemen we digitale autonomie mee als criterium om scherper te krijgen wat het vraagt, daarbij realiseren we ons dat we afhankelijk zijn van de markt, maar we gaan voor het meest haalbare. De aankomende aanbestedingen voor de voor dienstverlening Public Cloud en HenT (hosting) zijn de eerste grote aanbestedingen waarin we dit gaan doen. Denk hierbij aan de mogelijkheid bij aanbestedingen om de contracten af te kunnen schalen.
- b. We bevorderen digitale autonomie bij kritische bedrijfsprocessen en bijhorende applicaties door ons huidig beleid op business continuïteitsmanagement te versterken (denk hierbij aan migratiestrategieën, exit-plannen en aangescherpte afspraken over regie op de data).
- c. Bij keuzes rondom applicaties explicieter sturen voor aansluiting op Common Ground: voldoen aan standaarden (zoals Europese standaarden voor steden met Living-in.EU).

## Conclusies en Vervolgstappen

De verkenning 'Versterking van Digitale Autonomie in Amsterdam' identificeert een dringende behoefte aan digitale autonomie om risico's te beheersen, zoals cyberdreigingen en de afhankelijkheid van een beperkt aantal leveranciers. Even overstappen is niet mogelijk. Om technische en financiële redenen, maar ook omdat het niet wenselijk is gezien de kwaliteit en continuïteit van onze dienstverlening: er is geen of beperkt aanbod wat aan onze eisen en wensen voldoet.

De beschreven maatregelen zijn erop gericht niet nog afhankelijker te worden. We maken geen apart actieplan voor digitale autonomie maar zorgen dat we dit onderdeel maken van ons huidig beleid. Stap voor stap worden we op die manier steeds autonomer, waarbij we ons aansluiten bij Europese en landelijke initiatieven.

We versterken onze inzet op:

1. Samenwerking versterken: Europees en landelijk, stap naar digitale autonomie
2. Regie op data
3. Digitaal onafhankelijke infrastructuur en applicaties

## Bijlagen

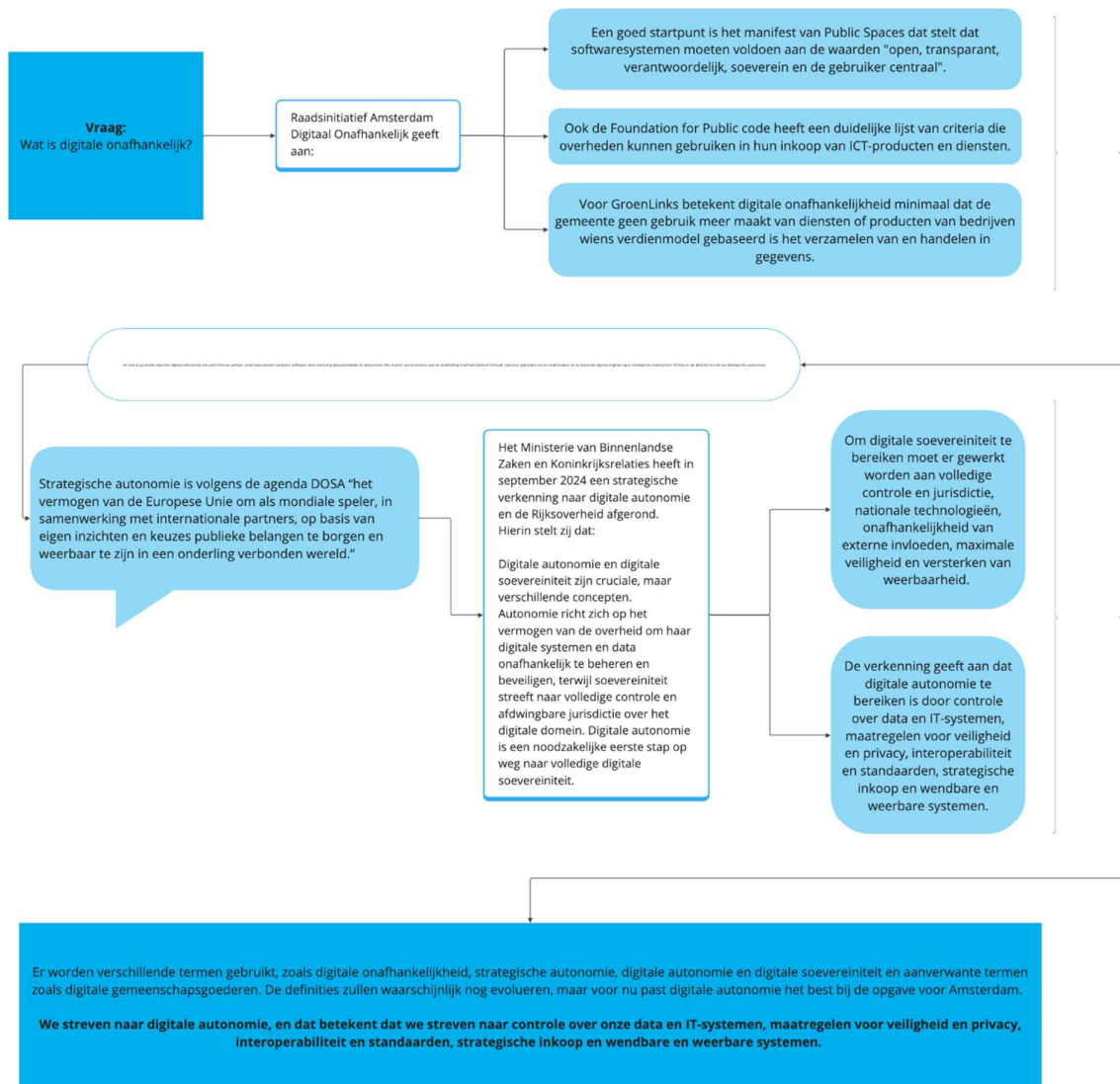
## Bijlage A - Wat is digitale autonomie?

Er zijn verschillende definities en aanverwante onderwerpen. Belangrijkste hierin zijn de definities van de Europese Commissie, de vertaling hiervan naar de Nederlandse Agenda DOSA en de definitie uit verkenning digitale autonomie van het Ministerie van BZK.

Het Rijk werkt aan een Nederlandse Digitaliseringsstrategie. Deze wordt voor de zomer van 2025 verwacht. In het traject van de NDS is ook aandacht voor digitale autonomie en de definitie hiervan.

Die definitie zullen we volgen. Tot die tijd gebruiken we de definitie uit de verkenning verkenning digitale autonomie van het Ministerie van BZK.

Echter is deze niet precies genoeg om bijvoorbeeld te werken aan inkoopvoorwaarden en andere maatregelen. Samen met o.a. AMS Institute wordt gewerkt aan het preciezer maken van de definitie.



Aspecten die in ieder geval van belang zijn voor deze verkenning zijn de volgende. "Digitaal autonomie" verwijst naar de mate waarin een entiteit, zoals een stad, land, organisatie, of individu, in staat is om digitale technologieën te beheren, gebruiken en innoveren op een manier die niet afhankelijk is van externe invloeden of controle. Het omvat het vermogen om zelfstandig

beslissingen te nemen over digitale infrastructuur, gegevensbeheer, informatiebeveiliging, technologische innovatie en andere aspecten van de digitale omgeving.

Belangrijke aspecten van digitaal onafhankelijk zijn onder andere:

1. **Technologische infrastructuur:** Het vermogen om lokale digitale infrastructuren te ontwikkelen, te onderhouden en te beheren, zoals datacenters, communicatienetwerken en cloudservices, zonder overmatige afhankelijkheid van externe providers.
2. **Data-eigendom en privacy:** De mogelijkheid om eigenaar te zijn van en controle te hebben over de data die wordt gegenereerd en verzameld binnen een entiteit, evenals het implementeren van robuuste privacybeschermingsmaatregelen.
3. **Digitale vaardigheden:** Het bevorderen van lokale digitale geletterdheid en het ontwikkelen van een vaardige lokale beroepsbevolking die in staat is digitale technologieën te begrijpen en te beheren.
4. **Cybersecurity:** Het vermogen om de digitale omgeving te beschermen tegen cyberbedreigingen door lokale expertise in cybersecurity op te bouwen en effectieve maatregelen voor incidentrespons te implementeren.
5. **Open data en transparantie:** Het implementeren van open data-initiatieven om niet-gevoelige gegevens toegankelijk te maken voor het publiek en het bevorderen van transparantie en verantwoordingsplicht.
6. **Diversificatie van toeleveringsketens:** Het verminderen van risico's door het diversifiëren van toeleveringsketens voor kritieke digitale componenten en mogelijk lokaal produceren van essentiële digitale technologieën.

Digitaal onafhankelijk zijn betekent over het algemeen streven naar autonomie, veerkracht en controle over de digitale middelen, systemen en processen, met het doel om een duurzame en veilige digitale toekomst te waarborgen.

## Bijlage B - Beleidsdocumenten en strategische notities

1. **Cloudstrategie Gemeente Amsterdam 2022-2025**
  - a. Kernpunten: Diversificatie van cloudleveranciers, implementatie van een multicloudstrategie en focus op Europese cloudopties.
  - b. Doel: Verminderen van afhankelijkheid en vergroten van veerkracht door gebruik te maken van meerdere leveranciers en te voldoen aan Europese wet- en regelgeving.
2. **Sourcingstrategie Amsterdam 2019**
  - a. Kernpunten: Efficiëntie, onafhankelijkheid en autonomie bij inkoop van technologie en diensten.
  - b. Beperkingen: Nog beperkt rekening gehouden met strategische autonomie en digitale onafhankelijkheid.
3. **Datastrategie Gemeente Amsterdam 2022-2026**
  - a. Doel gemeente breed: Onze data principes kader stellend zijn voor de datatransformatie en worden vertaald naar sturing in de praktijk voor elk team.
  - b. Doel directie Data: onze doelen gericht zijn op het faciliteren van de implementatie data gedreven werken binnen de gemeente waarbij elk team een meetbare bijdrage levert.
4. **Agenda Digitale Stad**
  - a. Onderwerpen: Digitale inclusie, publieke waarden in technologie en samenwerking binnen de stad.
  - b. Focus: Het versterken van de digitale infrastructuur en het betrekken van burgers en ondernemers.
5. **Architectuurprincipes**
  - a. Richtlijnen: Open standaarden, interoperabiliteit, schaalbaarheid en datatoegankelijkheid.
  - b. Voorbeeld: Gebruik van containertechnologieën om overstappen tussen cloudproviders te vergemakkelijken.

## Bijlage C - Overzicht ontwikkelingen en samenwerkingsverbanden

### 1. Nationale Ontwikkelingen

- a. **Digitale Autonomie Strategie Nederland (DOSA):** Beleid van het Rijk gericht op het versterken van digitale autonomie.
- b. **Tweede Kamerbrief Evaluatie Rijksbreed Cloudbeleid:** Inzicht in afhankelijkheid van buitenlandse technologie en strategische aanbevelingen.
- c. **Forum Standaardisatie:** Bevordering van open standaarden en interoperabiliteit.

### 2. Europese Initiatieven

- a. **European Digital Infrastructure Consortium (EDIC):** Gericht op het ontwikkelen van Europese cloud- en datainfrastructuren.
- b. **Data Act en Data Governance Act:** Wetgeving ter bevordering van datadeling en gegevenssoevereiniteit.

### 3. Lokale Samenwerkingen

- a. **G4-steden:** Gezamenlijke aanbestedingen en uitwisseling van kennis en best practices.
- b. **Waag en PublicSpaces:** Partners in het bevorderen van open source en publieke digitale infrastructuren.

## De Nederlandse Digitaliseringsstrategie

De Nederlandse Digitaliseringsstrategie (NDS) 2025 is een initiatief van staatssecretaris Zsolt Szabó, gericht op het verantwoord inzetten van digitale technologie en het verbeteren van overheidsdienstverlening aan burgers en ondernemers.

De hoofddoelen van de NDS in 2025 zijn:

7. **Werken als één overheid:** Het streven is om burgers en ondernemers te bedienen als één samenhangende overheid, in plaats van als afzonderlijke organisaties. Dit moet het contact met de overheid vereenvoudigen en efficiënter maken.
8. **Verbeteren van digitale dienstverlening:** Het doel is om de digitale interactie met de overheid begrijpelijker en toegankelijker te maken, zodat burgers en ondernemers eenvoudiger zaken kunnen regelen.
9. **Versterken van samenwerking binnen de overheid:** Door nauwere samenwerking tussen verschillende overheidslagen en publieke dienstverleners wil men dubbel werk voorkomen en besluitvorming versnellen.
10. **Proactief inspelen op technologische ontwikkelingen:** De NDS richt zich op het tijdig adopteren van nieuwe technologieën, zoals cloud computing en artificiële intelligentie (AI), om de digitale infrastructuur te optimaliseren.
11. **Verhogen van digitale weerbaarheid:** Het vergroten van de veiligheid en onafhankelijkheid van digitale systemen binnen de overheid is een prioriteit om bedreigingen het hoofd te bieden.
12. **Stimuleren van digitaal vakmanschap:** Het ontwikkelen en versterken van digitale vaardigheden binnen de overheid is essentieel voor het effectief gebruik van technologische mogelijkheden.

De NDS 2025 wordt in fases ontwikkeld. Van september tot en met november 2024 lag de focus op het opstarten en prioriteren van de strategie (fase 1: het 'wat'). Vanaf december 2024 richt men zich op het uitwerken en formaliseren (fase 2: het 'hoe'). De definitieve versie van de NDS wordt in het voorjaar van 2025 aan de Tweede Kamer aangeboden. Door deze strategie beoogt de overheid de digitale transitie in

Nederland succesvol te begeleiden, met aandacht voor zowel kansen als risico's die digitalisering met zich meebrengt.

### **Prioriteiten van de NDS 2025**

In de startbrief over de Nederlandse Digitaliseringsstrategie (NDS) heeft staatssecretaris Zsolt Szabó zeven prioriteiten benoemd waarop de overheid zich zal richten:

8. **Goede dienstverlening van de overheid voor burgers en ondernemers:** Het verbeteren van de digitale interactie tussen overheid, burgers en bedrijven om deze begrijpelijk en toegankelijk te maken.
9. **Versterken van digitale weerbaarheid en autonomie:** Het vergroten van de veiligheid en onafhankelijkheid van digitale systemen binnen de overheid.
10. **Politiek-bestuurlijke aansturing en efficiëntere samenwerking als één overheid:** Het bevorderen van een geïntegreerde aanpak en samenwerking tussen verschillende overheidslagen en publieke dienstverleners.
11. **Digitaal vakmanschap:** Het ontwikkelen en versterken van digitale vaardigheden binnen de overheid om effectief gebruik te maken van technologische mogelijkheden.
12. **Artificiële Intelligentie (AI):** Het verkennen en verantwoord inzetten van AI-toepassingen binnen overheidsdiensten.
13. **Data:** Het verbeteren van data-uitwisseling en -gebruik binnen de overheid, met aandacht voor standaardisatie en veiligheid.
14. **Cloud:** Het onderzoeken en implementeren van cloudoplossingen om de digitale infrastructuur van de overheid te optimaliseren.

Deze prioriteiten worden de komende tijd verder uitgewerkt in de nieuwe NDS, die naar verwachting in het voorjaar van 2025 aan de Tweede Kamer zal worden aangeboden.

## Bijlage D - Geraadpleegde literatuur en bronnen

### 1. Experts

Er zijn - naast collega's bij de VNG en het Ministerie van Binnenlandse Zaken - oriënterende gesprekken geweest met verschillende experts, waaronder Bert Hubert, Thijs Turèl (AMS-Institute), Hans de ZXwart (HvA), Nitesh Bharosa (TU Delft en Digicampus), Sander van der Waal (Waag), Sophie Bloemen (Commons Network) en Marijn Janssen (TU Delft).

### 2. Rapporten

- a. "Break Open Big Tech" manifest en whitepaper: Aanbevelingen voor publieke digitale infrastructuren.
- b. "Digitale Autonomie Strategie Nederland" (DOSAN): Richtsnoeren voor nationale digitale onafhankelijkheid.
- c. Evaluatie Rijksbreed Cloudbeleid (2024).

### 3. Wet- en Regelgeving

- a. Data Governance Act en Data Act (EU).
- b. Nederlandse Algemene Inkoopvoorwaarden Rijksoverheid (ARBIT).

### 4. Interne Documenten

- a. Overzicht huidige Amsterdamse IT-strategie en architectuurprincipes.
- b. Aanbestedingsdocumenten en sourcingsstrategieën van de gemeente Amsterdam.
- c. [Datastrategie 2022-2026](#)

### 5. Externe Bronnen

- a. Publicaties van de Europese Commissie over digitale soevereiniteit.
- b. Onderzoek naar digitale gemeenschapsgoederen door VNG en Commons Network.
- c. Position papers van verschillende experts (onder andere het Rathenau Instituut, Wigo4it, individuele experts en bedrijven) welke gepubliceerd zijn voor het Rondetafelgesprek van de vaste commissie Digitale Zaken van de Tweede Kamer in februari 2025 over 'Digitale soevereiniteit bij de Rijksoverheid'.  
[https://www.tweedekamer.nl/debat\\_en\\_vergadering/commissievergaderingen/details?id=2024A06698](https://www.tweedekamer.nl/debat_en_vergadering/commissievergaderingen/details?id=2024A06698)

1. SURF. (z.d.).leergang **Digitale soevereiniteit op basis van publieke waarden**. Geraadpleegd op [datum], van <https://www.surf.nl/agenda/digitale-soevereiniteit-op-basis-van-publieke-waarden>
2. Volkskrant. (2024, [datum]). **Staatssecretaris zet verhuizing van overheidsgegevens naar de cloud voorlopig stil: 'Dit gaat om de Nederlandse veiligheid'**. Geraadpleegd op [datum], van <https://www.volkskrant.nl/tech/staatssecretaris-zet-verhuizing-van-overheidsgegevens-naar-de-cloud-voorlopig-stil-dit-gaat-om-de-nederlandse-veiligheid~bf8d9544/>
3. UCL. (2024, december). **Reclaiming Digital Sovereignty**. Geraadpleegd op [datum], van <https://www.ucl.ac.uk/bartlett/public-purpose/publications/2024/dec/reclaiming-digital-sovereignty>
4. **Rijksoverheid**. (2024, 22 november). *Kamerbrief over geplande en voorgenomen cloudmigraties van overheids-ICT naar het buitenland*. Geraadpleegd via <https://www.rijksoverheid.nl/documenten/kamerstukken/2024/11/22/kamerbrief-over-geplande-en-voorgenomen-cloudmigraties-van-overheids-ict-naar-het-buitenland>

5. **FD.** (z.d.). Strategische autonomie is extreem kostbaar en niet per se veiliger. Geraadpleegd via <https://fd.nl/economie/1537595/strategische-autonomie-is-extreem-kostbaar-en-niet-per-se-veiliger>
6. **SURF.** (2024, 10 oktober). *Nieuwe strategie voor gebruik van clouddiensten in onderwijs en onderzoek.* Geraadpleegd via <https://www.surf.nl/nieuws/nieuwe-strategie-voor-gebruik-van-clouddiensten-in-onderwijs-en-onderzoek>
7. **SURF.** (2024). *Cloud sourcing strategie.* Geraadpleegd via <https://www.surf.nl/files/2024-10/surf-cloud-sourcing-strategie.pdf>
8. **UCL.** (2024, maart). *Digital public infrastructure and public value: What is public about DPI?.* Geraadpleegd via <https://www.ucl.ac.uk/bartlett/public-purpose/publications/2024/mar/digital-public-infrastructure-and-public-value-what-public-about-dpi>
9. **VNG.** (z.d.). Gezamenlijke prioriteitstelling Huis van Thorbecke. Geraadpleegd via <https://vng.nl/brieven/gezamenlijke-prioriteitstelling-huis-van-thorbecke>
10. **TNO.** (2024). *TNO rapport R10300.* Geraadpleegd via <https://publications.tno.nl/publication/34642268/05remY/TNO-2024-R10300.pdf>
11. **TNO.** (2022). *TNO rapport R10507.* Geraadpleegd via <https://publications.tno.nl/publication/34639349/urAkBu/TNO-2022-R10507.pdf>
12. **Binnenlands Bestuur.** (z.d.). Het cloudbeleid van de Nederlandse overheid onveilig. Geraadpleegd via <https://www.binnenlandsbestuur.nl/digitaal/het-cloudbeleid-van-de-nederlandse-overheid-onveilig>
13. **SLM Microsoft Rijk.** (2024, 2 september). *Memo on EU-based public cloud providers.* Geraadpleegd via <https://slmmicrosoftrijk.nl/wp-content/uploads/2024/09/20240902-Memo-on-EU-based-public-cloud-providers.pdf>
14. **UCL.** (2024). *IIPP Working Paper 2024-05.* Geraadpleegd via [https://www.ucl.ac.uk/bartlett/public-purpose/sites/bartlett\\_public Purpose/files/iipp\\_wp\\_2024-05.pdf](https://www.ucl.ac.uk/bartlett/public-purpose/sites/bartlett_public Purpose/files/iipp_wp_2024-05.pdf)
15. **Springer.** (2024). *Article on digital sovereignty.* Geraadpleegd via <https://link.springer.com/article/10.1007/s44206-024-00140-z>
16. **Europese Commissie.** (z.d.). *Digital strategy: EDIC.* Geraadpleegd via <https://digital-strategy.ec.europa.eu/en/policies/edic>
17. **Nesta.** (z.d.). *Towards Public Digital Infrastructure.* Geraadpleegd via [https://media.nesta.org.uk/documents/TowardsPublicDigitalInfrastructure\\_vo.2.pdf](https://media.nesta.org.uk/documents/TowardsPublicDigitalInfrastructure_vo.2.pdf)
18. **Open Future.** (z.d.). *Digital Commons and Public Digital Infrastructure.* Geraadpleegd via <https://openfuture.pubpub.org/pub/digital-commons-public-digital-infra/release/2>
19. **Europese Commissie.** (z.d.). *The future of European competitiveness: A competitiveness strategy for Europe.* Geraadpleegd via [https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92\\_en](https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en)
20. **iBestuur.** (z.d.). BZK start strategische verkenning naar digitale soevereiniteit. Geraadpleegd via <https://ibestuur.nl/artikel/bzk-start-strategische-verkenning-naar-digitale-soevereiniteit>
21. **Cyber Security Raad.** (2021). *Onderzoeksrapport over nationale digitale autonomie.* Geraadpleegd via <https://www.cybersecurityraad.nl/actueel/nieuws/2021/02/22/onderzoeksrapport-over-nationale-digitale-atonomie>
22. **Rathenau Instituut.** (z.d.). Het behoud van digitale autonomie. Geraadpleegd via <https://www.rathenau.nl/nl/berichten-aan-het-parlement/het-behoud-van-digitale-autonomie>

23. **Berthub.** (z.d.). Digitale autonomie - PublicSpaces-notes. Geraadpleegd via <https://berthub.eu/autonomie/Digitale%20autonomie%20PublicSpaces-notes.pdf>
24. **YouTube.** (2024). Digitale autonomie, een duivels dilemma - Uitvoeringscongres 2024. Geraadpleegd via <https://www.youtube.com/watch?v=nmUlykem6jk>

## Bijlage E Maatregelen en activiteiten uit verkenning Digitale autonomie van BZK (oktober 2024)

en de overzicht van BZK activiteiten uit de agenda DOSA

### B Bijlage B – Aanbevolen acties

| Onderwerp   | Actie  | Aanpak   | Impact  |
|---|--|--|---|
| 1. Opstarten van de Actieagenda Digitale Autonomie (ADA)                        | Opzetten en inrichten van de ADA en de bijbehorende actielijnen vanuit een coördinerende rol binnen BZK.     | BZK neemt de leidende rol in het coördineren van de ADA, waarbij duidelijke actielijnen worden uitgezet en gevolgd. Er wordt een centrale coördinator aangesteld om de voortgang te bewaken en samenwerking tussen verschillende directies en ministeries te bevorderen. | Verbeterde coördinatie en effectiviteit in de uitvoering van acties gericht op digitale autonomie.                        |
| 2. Ontwikkeling van autonome/ soevereine IT-voorzieningen                       | Ontwikkelen en implementeren van autonome/soevereine IT-voorzieningen zoals cloudoplossingen en datacenters. | Implementeer een soevereine cloud waarbij gevoelige informatie vanuit extra beveiligde voorzieningen wordt aangeboden, bestuurd en beheerd. Zorg ervoor dat deze voldoen aan Nederlandse wet- en regelgeving en vrij zijn van buitenlandse inmenging.                    | Versterking van de controle over gevoelige informatie en vermindering van afhankelijkheid van buitenlandse technologieën. |
| 3. Implementatie van geavanceerde cybersecuritymaatregelen                      | Implementeren van geavanceerde cybersecuritymaatregelen.   | Versterk het Nationaal Cyber Security Centrum (NCSC) en ontwikkel een robuuste digitale informatie- en veiligheidsarchitectuur. Zorg voor continue evaluatie en verbetering van cybersecuritypraktijken.   | Verhoogde beveiliging van digitale infrastructures en bescherming tegen cyberdreigingen.                                  |
| 4. Inventarisatie van strategische afhankelijkheden en opstellen afwegingskader | Inventariseren van strategische afhankelijkheden en opstellen van een afwegingskader                         | Voer een uitgebreide inventarisatie uit van strategische afhankelijkheden binnen de Rijksoverheid en vertaal deze naar een kader met risicocategorieën (hoog, gemiddeld, laag risk-appetite)   | Helder inzicht in de afhankelijkheden en duidelijke richtlijnen voor risicobeheer.  |

### Uitwerking ondersteunende ontwikkelingen

| Ontwikkelingen   | Geadviseerde activiteiten  | Relevantie voor digitale autonomie   |
|--|--|--|
| Strategisch inkoopbeleid                                   | <ul style="list-style-type: none"> <li>- Ontwikkelen van duidelijke richtlijnen of scherp bestaande kaders aan voor de inkoop van IT-diensten en -producten in het kader van strategische autonomie</li> <li>- Formuleren van afwegingskaders voor strategische inkoop.</li> <li>- Uitvoeren van verkenningen naar inkoopstrategieën die bijdragen aan digitale autonomie.</li> <li>- Ontwikkelen specifieke kaders voor de inkoop van kantoorsoftware.</li> </ul> | Strategisch inkoopbeleid zorgt ervoor dat aankopen bijdragen aan autonomie en voldoen aan ethische en publieke waarden van de Rijksoverheid.   |
| Structurele monitoring van opkomende technologieën         | <ul style="list-style-type: none"> <li>- Continu beoordelen van de impact van nieuwe technologische ontwikkelingen.</li> <li>- Proactief identificeren van potentiële risico's en kansen vanuit het perspectief van autonomie, veiligheid en beleidsimplementatie.</li> <li>- Samenwerken met technologische experts, academische instellingen en internationale partners.</li> </ul>  | Dit traject is essentieel om ervoor te zorgen dat de Rijksoverheid niet alleen reageert op technologische veranderingen, maar ook voorbereid is op toekomstige uitdagingen en mogelijkheden. |
| Richtlijnen voor ethiek en publieke waarden                | <ul style="list-style-type: none"> <li>- Ontwikkelen van beleid voor de ethische inzet van digitale technologieën.</li> <li>- Formuleren van richtlijnen voor de bescherming van publieke waarden.</li> <li>- Uitvoeren van verkenningen naar ethische vraagstukken en publieke waarden.</li> <li>- Samenwerken met ethische commissies en maatschappelijke organisaties.</li> </ul>   | Het waarborgen van ethische aspecten en publieke waarden zorgt ervoor dat de digitale transformatie bijdraagt aan een eerlijke, inclusieve en transparante samenleving.                      |
| Capaciteitsopbouw en scholing                              | <ul style="list-style-type: none"> <li>- Opzetten Digital Autonomy Center of Excellence (DACoE)</li> <li>- Organiseren van trainingen voor overheidsmedewerkers.</li> <li>- Ontwikkelen van vaardigheden voor digitale transformatie.</li> <li>- Formuleren van beleidsmaatregelen voor continue scholing en ontwikkeling.</li> <li>- Samenwerken met onderwijsinstellingen voor capaciteitsopbouw.</li> </ul>   | Het ontwikkelen van de noodzakelijke vaardigheden bij overheidsmedewerkers is essentieel voor de implementatie en beheer van nieuwe technologieën,   |
| Toepassen en (mede) ontwikkelen van veiligheidsstandaarden | <ul style="list-style-type: none"> <li>- Toepassen of (mede)ontwikkelen van veilige IoT-standaarden en -toepassingen.</li> <li>- Investeren in quantumveilige cryptografie.</li> <li>- Experimenteren met AI-applicaties binnen overheidsdiensten.</li> <li>- Ontwikkelen van veilige digitale identiteiten voor personen, organisaties en devices.</li> </ul>   | Het ontwikkelen van veiligheidsstandaarden voor nieuwe technologieën zorgt voor een veilige implementatie en gebruik van deze technologieën, wat cruciaal is voor de bescherming van         |

|   |   |  |
|---|---|--|
|   | <ul style="list-style-type: none"> <li>- Aansluiten op of mede-ontwikkelen van internationale veiligheidsstandaarden.</li> <li>- Toepassen van deze standaarden in een veilige omgeving om de effecten en impact ervan te kunnen beoordelen.</li> </ul>   | nationale belangen en digitale autonomie.  |
| Europese en internationale samenwerking                   | <ul style="list-style-type: none"> <li>- Actief samenwerken met Ministerie van Economische Zaken en Defensie in verband met economisch beleid en nationale veiligheid met als inzet Europese beïnvloeding van wet- en regelgeving, het verkrijgen van subsidies en het gezamenlijk doen van investeringen.</li> <li>- Actief samenwerken met Europese partners.</li> <li>- Deelnemen aan internationale initiatieven voor digitale autonomie.</li> <li>- Ontwikkelen van beleidskaders voor internationale samenwerking.</li> <li>- Uitvoeren van onderzoeken naar best practices en kennisuitwisseling.</li> </ul> | Internationale samenwerking versterkt de positie van Nederland binnen Europa en bevordert gedeelde kennis en middelen voor een robuustere digitale infrastructuur  |
| Doorontwikkeling Generieke Digitale Infrastructuur (GDI). | <ul style="list-style-type: none"> <li>-Versterken van beveiligingsmaatregelen voor toegangssystemen zoals DigiD en eHerkenning.</li> <li>-Implementeren van geavanceerde beveiligingsmaatregelen voor platforms zoals Digimelding en Digipoort.</li> <li>- Versterken van beveiligingsmaatregelen voor infrastructuurcomponenten zoals Diginetwerk en PKIoverheid.</li> <li>- Bevorderen van samenwerking tussen verschillende overheidslagen voor een uniforme implementatie van digitale autonomie</li> </ul>  | Een robuuste en moderne digitale infrastructuur zorgt ervoor dat overheidsdiensten efficiënt en veilig kunnen opereren, terwijl afhankelijkheid van buitenlandse technologieën en leveranciers wordt vermindert. Door te investeren in de nieuwste technologieën, beheer- en onderhoudsprocessen, en capaciteitsopbouw, versterkt de Rijksoverheid haar positie en weerbaarheid in de digitale wereld. |
| Doorontwikkeling inzet Open Source                        | <ul style="list-style-type: none"> <li>-Bevorderen van het gebruik van open source software binnen overheidsdiensten om vendor lock-in te voorkomen.</li> <li>- Investeren in open source projecten om innovatie en samenwerking te Bevorderen.</li> <li>- Verhogen van de veiligheid en transparantie van IT-systemen door gebruik te maken van open source oplossingen.</li> <li>- Organiseren van trainingen en workshops om overheidsmedewerkers vertrouwd te maken met open source technologieën en tools.</li> </ul>  | Open source software speelt een cruciale rol in het versterken van de digitale autonomie van de Rijksoverheid. Door gebruik te maken van open source technologieën, kan de overheid onafhankelijker opereren van grote, buitenlandse technologiebedrijven. Dit bevordert de controle over kritieke   |

|  |  |   |
|--|--|---|
|  | - Bevorderen van kennisuitwisseling en samenwerking tussen verschillende ministeries en overheidsorganisaties met betrekking tot open source initiatieven. | digitale infrastructuur en vermindert de afhankelijkheid van propriëtaire software. Open source software biedt transparantie, waardoor de beveiliging en integriteit van systemen beter kunnen worden gewaarborgd. Dit alles draagt bij aan een veerkrachtigere, veiligere en zelfvoorzienende digitale overheid. |
|--|--|---|

### Bijlage – Overzicht DOSA-activiteiten BZK

| Actie  | Eigenaar     | Samenwerkende partijen | Planning                                  |
|--|--------------|------------------------|---|
| Realisatie Rijksbreed cloudbeleid  | BZK          | Rijksbreed             | 2022                                      |
| Evaluatie Rijksbreed cloudbeleid   | BZK          | Rijksbreed             | 2023-2024                                 |
| Onderzoeken of de duur van overeenkomsten voor de levering van cybersecuritydiensten kan worden verlengd   | BZK          | NCSC, EZK              | 2023-2024                                 |
| Onderzoeken hoe de doorstroming van cybersecuritypersoneel tussen overheid en bedrijfsleven kan worden verbeterd   | BZK          | NCSC, EZK              | 2023-2024                                 |
| Verkennen of vanuit de NAVO DIANA Challenge 'Secure Information Sharing' in Nederland een high assurance en cryptographic accelerator kan worden gevestigd | BZK/Defensie | NCSC, EZK              | 2023-2024                                 |
| Inrichting Open Source Program Office (OSPO) binnen BZK  | BZK          | -                      | Kwartiermaker gestart 1-8-2023            |
| Scenarioverkenning nut en noodzaak van een OSPO Rijk   | BZK          | CIO-beraad             | Ter bespreking in het CIO-beraad Sept/Okt |

|   |          |                                   |                         |
|---|----------|-----------------------------------|-------------------------|
| Vergroten adoptie 'open, tenzij' afwegingskader   | BZK      | Forum Standaardisatie             | Sept 2022 t/m eind 2024 |
| Uitvoering geven aan strategisch communicatieplan t.b.v. vergroten bewustzijns- en kennisniveau t.a.v. opensource-werken  | BZK      | Forum Standaardisatie             | Sept 2020 t/m dec 2023  |
| Verkennen van open source software als alternatief voor kantoorsoftware in kader van strategie voor open source   | BZK      | EZK, Forum Standaardisatie        | Vanaf 2023              |
| Blijvend aandacht vestigen op naleving van de verplichtingen van Forum Standaardisatie voor het gebruik van software binnen de overheid   | BZK      | Rijksbreed, Forum Standaardisatie | Doorlopend              |
| Inventariseren van strategische afhankelijkheid van individuele kantoorsoftwareproducten in gebruik door Rijksoverheid  | BZK      | Rijksbreed, EZK                   | N.t.b.                  |
| Onder de Nationale Cryptostrategie (NCS) een marktanalyse uitvoeren van de high assurance-markt in Nederland  | BZK      | EZK                               | 2023-2024               |
| Onderzoeken op welke wijzen barrières bij aanbestedingen vanuit de Rijksoverheid ten aanzien van open source weggenomen kunnen worden   | BZK      | Rijksbreed                        | N.t.b.                  |
| Implementatie van Europese wetgevingstrajecten Data Act en Data Governance Act  | BZK      | J&V, BZK, ACM, AP                 | 2023 -2025              |
| Onderzoek verrichten naar mogelijke mitigerende maatregelen voor vermindering Cloudafhankelijkheid Nederland, waaronder mogelijkheid en haalbaarheid soevereine Nederlandse cloud | BZK, EZK | Rijksbreed, NCSC                  | N.t.b.                  |