Ministerie van Binnenlandse Zaken
en Koninkrijksrelaties

Visie

Digitale autonomie en soevereiniteit van de overheid

Werken aan de basis. Van Nederland en ons Koninkrijk.

Inhoud

1 Inleiding 3

1.1 Beleidscontext en verankering visie 3

2 Een wenkend perspectief: naar een weerbare digitale overheid 5

2.1 Toekomstperspectief 5

3 Van definities naar gedeelde visie 7

3.1 Digitale open strategische autonomie - DOSA 7

3.2 Digitale soevereiniteit: zeggenschap en controle 7

3.3 Een gedeelde visie: autonomie en soevereiniteit in een veranderlijke wereld 8

4 Een realistische benadering 9

5 Strategische bouwstenen en leidende principes: de fundamenten van een toekomstbestendige digitale overheid 10

5.1 Leidende principes: het kompas voor een betrouwbare en toekomstbestendige digitale overheid 10

5.2 Strategische bouwstenen: het versterken van de fundamenten voor een digitale toekomst 11

6 Vervolg en slotwoord 13

1 Inleiding

De overheid is in toenemende mate afhankelijk van digitale systemen voor het uitvoeren van haar publieke taken. Deze afhankelijkheid brengt risico's met zich mee, zeker in een tijd van technologische versnelling en geopolitieke ontwikkelingen. Het behouden van zeggenschap over technologie, data, informatie en digitale processen is essentieel om publieke waarden, veiligheid en de democratie te waarborgen. De digitale infrastructuur van de overheid speelt een centrale rol in het functioneren van de samenleving. Zonder een goed beveiligde en toekomstbestendige digitale infrastructuur kan de overheid haar taken niet betrouwbaar uitvoeren. Het is belangrijk dat de overheid haar rol als beheerder van dergelijke systemen opnieuw overweegt, zodat de continuïteit en veiligheid van deze processen gewaarborgd blijven, ook in tijden van verhoogde dreiging.

Deze visie biedt richting aan de manier waarop de Nederlandse overheid haar digitale (open strategische) autonomie en haar digitale soevereiniteit[1] kan versterken. Zij legt uit wat deze concepten betekenen, waarom ze belangrijk zijn en hoe ze bijdragen aan een toekomstbestendige digitale overheid. Centraal staan het verminderen van ongewenste strategische afhankelijkheden, het vergroten van technologische zelfredzaamheid en het stimuleren van samenwerking binnen Europa. Om dat te bereiken kiest Nederland nadrukkelijk voor een Europese koers: we werken met onze partners aan soevereine oplossingen en dragen als betrouwbare speler bij aan het vormgeven van internationale standaarden en regelgeving. Zo positioneren we ons land én Europa sterker in de mondiale digitale economie, beschermen we onze economische en geopolitieke belangen en blijven onze publieke waarden leidend.

Tegelijk vraagt dit om een realistische en gefaseerde aanpak, waarbij strategische keuzes op organisatieniveau genomen moeten worden. Met deze visie wil de overheid een gedeeld perspectief creëren dat uitnodigt tot samenwerking tussen overheidsorganisaties, private partijen, internationale partners en kennisinstellingen. De visie is belangrijk omdat zij een gedeeld vertrekpunt biedt voor het versterken van de digitale weerbaarheid en autonomie van de overheid. Het is een uitnodiging om samen te bouwen aan een sterk en veerkrachtig digitaal fundament, waarin beheersing, zeggenschap en innovatie centraal staan.

1.1 Beleidscontext en verankering visie

De digitale autonomie en soevereiniteit van de Nederlandse overheid staan niet op zichzelf, maar maken deel uit van een bredere beweging binnen Europa en de wereld. Deze visie bouwt voort op nationaal en internationaal beleid, kaders en strategieën die met het thema samenhangen.

Rijksbreed beleid

De Agenda Digitale Open Strategische Autonomie (DOSA)[2] is het integraal beleidskader dat middels acties invulling geeft aan de Kamerbrief Open Strategische Autonomie[3] en de Kamerbrief kabinetsaanpak risicovolle strategische afhankelijkheden voor wat het digitale domein betreft.[4] Hierin staan ook de tien digitale technologieën (zoals cloud en kantoorsoftware) omschreven die vanuit het geopolitiek en geo-economisch perspectief het meest cruciaal zijn voor Nederland. De Kamerbrief OSA, de Agenda DOSA en het fundament voor het beleid over digitale (open strategische) autonomie. Deze visie concretiseert en verdiept de doelstellingen uit de Agenda DOSA voor de overheid, en vormt daarmee een belangrijke bouwsteen voor het overheidsbrede beleid rondom digitale autonomie.

Overheidsbreed beleid

De visie richt zich op de versterking van digitale autonomie en soevereiniteit voor de overheid. De visie richt zich niet op specifieke uitvoeringsvraagstukken, maar schetst de strategische contouren en stip op de horizon voor de Nederlandse overheid. Het beleid zal op een risico-gebaseerde aanpak gestoeld zijn. De verantwoordelijkheid voor de risicoafweging en de beslissing van (de impact van) de te nemen maatregelen ligt bij de organisatie zelf. Met het versterken van de digitale autonomie zijn naar verwachting inspanningen en investeringen gemoeid. Deze visie onderkent dat structurele veranderingen tijd en geld kosten en vragen om gezamenlijke, overheidsbrede inzet en een langdurige, gerichte aanpak. Strategisch gerichte investeringen zijn nodig om als overheid duurzame keuzes te maken die bijdragen aan meer zeggenschap over belangrijke digitale infrastructuur en diensten.

1 Waar in dit document 'digitale autonomie' staat, wordt 'digitale open strategische autonomie' (DOSA) bedoeld, in lijn met de in 2023 door het demissionair kabinet uitgebrachte Agenda DOSA. De verhouding tussen digitale autonomie en 'digitale soevereiniteit', een ander begrip waarvoor nog geen Nederlands beleidskader is, wordt uitgelegd in hoofdstuk 3.
2 Kamerstuk 36 259, nr. 23.
3 Kamerstuk 35 982, nr. 9.
4 Kamerstuk 30 821, nr. 181.

Waar samenwerking logisch en wenselijk is, ligt er een opgave om ambities en middelen te bundelen. Tegelijkertijd biedt deze koers kansen: het versterken van de digitale autonomie draagt bij aan het borgen van publieke waarden, het vergroten van weerbaarheid en een duurzame vermindering van ongewenste strategische afhankelijkheden. Op de langere termijn kunnen bovendien andere voordelen ontstaan, zoals meer samenhang in de inzet van publieke middelen en een stimulans voor een meer diverse markt die beter aansluit bij onze publieke waarden en belangen.

IT-Sourcingstrategie Rijk en overheid

Om de ambities uit de visie op digitale autonomie en soevereiniteit te realiseren, zijn concrete instrumenten nodig die deze strategische richting ondersteunen en vertalen naar handelingsperspectief. Een belangrijk voorbeeld daarvan is de IT-sourcingstrategie Rijk. De IT-sourcingstrategie Rijk bundelt, waar mogelijk, de inkoopkracht van het Rijk. Deze strategie maakt het mogelijk om risico-gebaseerd, verantwoord en uniform besluiten te nemen over IT-inkoop en leverancierskeuze. Dit draagt bij aan de continuïteit van de dienstverlening, verhoogt de digitale weerbaarheid en bevordert een efficiënt gebruik van IT-diensten. De organisatorische reikwijdte van de strategie wordt stapsgewijs uitgebreid, met als doel uiteindelijk toe te werken naar een overheidsbrede toepassing.

De visie op digitale autonomie en soevereiniteit biedt richting aan de strategische keuzes die binnen deze sourcingstrategie gemaakt worden. Ze onderstreept het belang van technologische keuzevrijheid, het voorkomen van lock-ins en het bewust beheersen van strategische afhankelijkheden. De sourcingstrategie vormt daarmee een belangrijk instrument om de visie te operationaliseren: door inkoopbeslissingen expliciet te toetsen op autonomie, soevereiniteit en publieke waarden, kan de overheid haar grip op kritieke digitale processen versterken. Zo helpt de sourcingstrategie niet alleen om kosten en risico's te beheersen, maar ook om vanuit gedeelde waarden toekomstbestendige digitale infrastructuur in te richten.

Rijksbrede cloudbeleid

Cloudtechnologie is een onmisbaar onderdeel van de digitale infrastructuur van de overheid, maar stelt ons ook voor keuzes die raken aan de digitale autonomie en soevereiniteit van de overheid. Dat perspectief onderstreept het belang van goede besluitvorming over waar digitale diensten van de overheid, haar beschikbaarheid en haar data worden opgeslagen en verwerkt onder welke garanties. Het Rijksbrede cloudbeleid vertaalt deze ambitie naar concrete richtlijnen voor het verantwoord gebruik van publieke clouddiensten. In de aanscherping van dit beleid wordt expliciet rekening gehouden met risico's rond marktconcentratie en ongewenste afhankelijkheden van enkele cloudleveranciers. Zo vormt het cloudbeleid tevens een belangrijk instrument om digitale autonomie te versterken en publieke waarden te borgen inxons ICT-landschap.

Europese kaders

De visie sluit aan op belangrijke EU-strategieën zoals de Digital Decade 2030, die inzet op technologische onafhankelijkheid en innovatie binnen Europa. De Algemene verordening gegevensbescherming (AVG) is het juridisch kader om persoonsgegevens te beschermen, een verantwoordelijkheid die de overheid hoog in het vaandel moet dragen bij het beheren van gevoelige data. De AVG benadrukt daarnaast het belang van Europese controle over data, wat aansluit bij de Nederlandse ambitie om datasoevereiniteit centraal te stellen. Daarnaast kunnen initiatieven zoals EuroStack en de Cloud and AI Development Act bijdragen aan het versterken van de Europese autonomie op het gebied van cloudtechnologie en AI, beide van belang voor een veerkrachtige digitale overheid.

Mondiale dimensie

Geopolitieke trends maken duidelijk dat samenwerking met gelijkgestemde landen essentieel is. Door actief bij te dragen aan internationale open standaarden en digitale governance, kan Nederland niet alleen haar eigen belangen beschermen, maar ook bijdragen aan een stabiel en open digitaal ecosysteem.

2 Een wenkend perspectief: naar een weerbare digitale overheid

Toegenomen geopolitieke ontwikkelingen en veranderde machtsverhoudingen in de wereld, vragen om een overheidsbrede aanpak in de waarborging van onze autonomie en soevereiniteit. Voor de Nederlandse overheid kunnen deze ontwikkelingen concrete risico's vormen voor het dagelijks functioneren, zoals bedreigingen voor de continuïteit van de dienstverlening en onze publieke waarden.

De overheid voert taken uit die van groot belang zijn voor de Nederlandse samenleving: van veilige dijken en schoon water tot rechtspraak, gezondheidszorg en nationale veiligheid. Veel van deze taken zijn volledig of grotendeels afhankelijk van digitale infrastructuur. Ze moeten altijd blijven functioneren, vooral in tijden van crisis of conflict.

Daarom zijn digitale autonomie en soevereiniteit voor de overheid essentieel. We willen controle over onze data en grip op de infrastructuur waarop de overheid draait. Niet alleen om continuïteit te waarborgen, maar ook om onze democratie en rechtsstaat te beschermen. De afhankelijkheid van niet-Europese technologieën maakt dit vraagstuk urgenter. De EU wil minder afhankelijk worden van externe partijen. De overheid heeft nu soms te weinig zicht op de risico's van digitale afhankelijkheden en kwetsbaarheden. Zonder dat inzicht kunnen we niet goed sturen op autonomie en soevereiniteit.

Daarbij is een realistische aanpak onmisbaar. De weg naar een versterking van onze digitale autonomie vraagt om een gefaseerde en pragmatische benadering, waarin bestaande leveranciers worden gecombineerd met Europese alternatieven en de inzet op overheidsbrede samenwerking centraal staat.

De oplossing ligt in een zorgvuldige balans: open waar het kan, beschermen waar het moet. Strategische keuzes bepalen wat we zelf doen en waar we afhankelijkheden bewust beperken. Zo verkleinen we risico's en benutten we kansen, met waarden als democratie, leiderschap, privacy en transparantie als kompas. De Nederlandse overheid wordt wendbaarder, weerbaarder en beter gepositioneerd in Europa en daarbuiten. Dit maakt het mogelijk om onze eigen koers te varen en zo onze publieke belangen te borgen.

2.1 Toekomstperspectief

Het toekomstbeeld voor de komende jaren bouwt voort op het hierboven geschetste wenkende perspectief en vertaalt de principes en bouwstenen naar concrete doelen en resultaten. De Nederlandse overheid heeft op termijn de volgende mijlpalen bereikt:

Autonomie door innovatie: Nederland vervult een leidende rol in de ontwikkeling van Europese oplossingen die digitale afhankelijkheden van de overheid verkleinen. Door in te zetten op open standaarden en samenwerking binnen Europa, heeft de overheid grip op kritieke digitale processen en versterkt zij haar technologische zelfbeschikking.

Soevereiniteit door leiderschap: Nederland biedt een veilige en robuuste digitale infrastructuur voor de overheid, met data-soevereiniteit als centraal uitgangspunt. Door te investeren in technologieën zoals quantum-veilige cryptografie en juridische en organisatorische kaders te ontwikkelen, is Nederland erkend als een veilige plek voor databeheer en digitale rechten.

Weerbaarheid door samenwerking: door Europese regelgeving, standaarden en gezamenlijke cybersecurity-strategieën te ondersteunen, draagt Nederland bij aan een weerbaar digitaal Europa. Internationale samenwerking versterkt niet alleen de Europese positie, maar biedt ook bescherming tegen grensoverschrijdende digitale dreigingen.

Waardengedreven technologieontwikkeling: Nederland heeft een ecosysteem ontwikkeld waarin innovatie samen gaat met maatschappelijke verantwoordelijkheid. AI en andere technologieën worden ontworpen met oog voor ethisch en verantwoord gebruik, wat Nederland internationaal tot voorbeeld maakt.

Versterking van democratische processen: technologie wordt gebruikt om democratische participatie te vergroten en transparantie te bevorderen. Burgers en bedrijven hebben meer inspraak, wat niet alleen het vertrouwen in de overheid versterkt, maar ook de legitimiteit van beleidsvorming verbetert.

Een wenkend perspectief: een weerbare en samenwerkende digitale overheid

Stel je een overheid voor die grip heeft op haar digitale infrastructuur, maar ook strategisch sterk en geopolitiek bewust opereert. Een overheid die strategische keuzes maakt: open waar het kan, beschermen waar het moet. Met die aanpak neemt Nederland een leidende positie binnen en met Europa, gebaseerd op gedeelde infrastructuren en waarden als privacy, veiligheid en democratie.

De Nederlandse overheid werkt toe naar een toekomst waarin zij zelfstandig, veilig en verantwoord digitale keuzes maakt. Dit doet zij door te investeren in technologie, Europese samenwerking en eigen controle over kritieke digitale processen. Een digitale infrastructuur voor de overheid die publieke waarden borgt, innovatie stimuleert en meebeweegt met technologische en geopolitieke ontwikkelingen vormt daarbij het fundament.

In dit toekomstbeeld trekken overheidslagen samen op met vertrouwde EU- en NAVO-partners. Ze bouwen aan een robuuste, veilige en toegankelijke digitale infrastructuur. Tegelijkertijd speelt Nederland internationaal een actieve rol in het versterken van weerbaarheid en het benutten van technologische kansen.

Dit is een overheid die risico's beheerst én kansen benut. Een organisatie die publieke waarden centraal stelt en werkt aan een toekomst waarin burgers en bedrijven kunnen vertrouwen op digitale veerkracht, wendbaarheid en innovatie.

3 Van definities naar gedeelde visie

Digitale autonomie en digitale soevereiniteit zijn fundamenten van een toekomstgerichte digitale overheid die kan opereren in een complexe en veranderlijke wereld. Deze begrippen bieden richting en helderheid in een tijd waarin technologie, geopolitiek en samenleving steeds meer met elkaar verweven raken. Omdat volledige onafhankelijkheid een onhaalbare ambitie is, vraagt de werkelijkheid om een realistische benadering. De overheid beweegt toe naar een aanpak waarbij autonomie en soevereiniteit een rol speelt bij de afweging voor de selectie van leveranciers van producten en diensten. Dit gebeurt op basis van operationalisatie van de begrippen, leidende principes en bouwstenen, zodat publieke waarden, veiligheid, weerbaarheid en continuïteit altijd gewaarborgd blijft en leveranciers een duidelijk beeld hebben van hoe de vraag vanuit de overheid er over een aantal jaar uit zal zien, zodat ze hier tijdig op in kunnen spelen.

3.1 Digitale open strategische autonomie - DOSA

Waar het gaat over autonomie, hanteert het kabinet de definitie, zoals beschreven in de Kamerbrief, omtrent Open Strategische Autonomie (OSA): *het vermogen van de EU om als mondiale speler, in samenwerking met internationale partners, op basis van eigen inzichten en keuzes publieke belangen te borgen en weerbaar te zijn in een onderling verbonden wereld.* Die belangen zijn onder meer de nationale veiligheid, het verdien- en concurrentievermogen, het vinden van oplossingen voor maatschappelijke uitdagingen, en de borging van de democratische rechtsstaat en fundamentele waarden. Met de agenda Digitale Open Strategische Autonomie (DOSA) heeft het destijds demissionaire kabinet in een integraal beleidskader voor open strategische autonomie binnen het digitale domein voorzien. In lijn met de Kamerbrief OSA en kabinetsbrede aanpak strategische afhankelijkheden wil Nederland hiermee een gebalanceerd narratief uitdragen op Europees en internationaal niveau.

Deze algemene Europese benadering van digitale open strategische autonomie (DOSA) wordt voor de Nederlandse overheid als volgt verder ingevuld:

3.1.1 Digitale autonomie van de overheid

Digitale autonomie van de overheid is gericht op het vermogen van de overheid om autonoom te handelen en beslissingen te nemen over haar digitale technologie. Het vormt de handelingsvrijheid van de overheid, niet alleen in het digitale domein, maar ook in andere domeinen zonder dat die kan worden belemmerd d.m.v. het digitale domein.

Binnen dit concept staan drie concepten centraal. De eerste is technologische keuzevrijheid. De overheid moet in staat zijn om technologie te kiezen, wijzigen of vervangen zonder onredelijke belemmeringen door lock-in-effecten of incompatibiliteit met bestaande systemen. Een tweede kernelement is kennisautonomie: de overheid beschikt over voldoende interne expertise om technologie te begrijpen, beheren en ontwikkelen. Het derde aspect betreft strategische afhankelijkheden, waarbij de overheid gericht bewust technologische afhankelijkheden mitigeert om risico's te beheersen:

- **Technologische keuzevrijheid:** de overheid behoudt de ruimte om weloverwogen keuzes te maken over technologieën en leveranciers. Bepaalde infrastructuur en systemen worden zodanig ingericht dat overstappen, aanpassen of combineren mogelijk blijft. Daarbij worden bestaande partijen aangevuld met autonome en Europese alternatieven, om afhankelijkheden te beheersen en strategische veerkracht te vergroten.
- **Kennisautonomie:** het vergroten van interne expertise over technologie en processen is essentieel. Dit omvat het vermogen om te beoordelen welke technologieën onder eigen beheer kunnen worden gebracht en waar samenwerking met derden de betere optie is.
- **Strategische afhankelijkheden mitigeren:** Als de overheid gebruik maakt van technologieën waarbij (risicovolle) strategische afhankelijkheden spelen kunnen hier risico's uit voortkomen, bijvoorbeeld voor de continuïteit voor de overheidsystemen. Dan kan de overheid inzetten op het mitigeren van de afhankelijkheid, bijvoorbeeld door het inzetten van haar inkoopkracht voor het opschalen van Europese alternatieven.

3.2 Digitale soevereiniteit: zeggenschap en controle

Digitale soevereiniteit heeft een fundamenteel andere focus dan autonomie: het gaat specifiek over juridische en bestuurlijke controle over digitale infrastructuren, data en systemen. Waar autonomie gaat over handelingsvrijheid, gaat soevereiniteit over zeggenschap. Daarbij is digitale autonomie een ruimer begrip dan digitale soevereiniteit: een staat die digitaal soeverein is (zeggenschap heeft over digitale infrastructuren, data en systemen), is ook digitaal autonoom (vrij om onafhankelijke keuzes te maken in het digitale domein). Omgekeerd is het niet zo: een digitale autonome staat hoeft niet per se volledige controle te hebben over de eigen digitale infrastructuren, data en systemen.

Juridische controle vormt een essentieel aspect van soevereiniteit, waarbij de overheid zekerheid heeft dat systemen en data enkel onder Nederlandse of Europese rechtsmacht vallen. Een tweede component is datasoevereiniteit, die volledige controle waarborgt over de locatie, verwerking en toegang tot overheidsinformatie. Het derde wezenlijke aspect betreft bestuurlijke zeggenschap: de mogelijkheid om democratische controle uit te oefenen over digitale systemen.

Door deze kenmerken te onderscheiden van autonomie, wordt helder dat soevereiniteit een juridisch-bestuurlijk karakter heeft en primair gericht is op controle en zeggenschap. Het gaat niet om de vrijheid om te handelen of het vermogen om te beschermen, maar om de formele en feitelijke controle over digitale middelen. Dit kan uiteraard sterk bijdragen aan de autonomie van de overheid. Dit omvat:

Juridische controle: zeggenschap over data, informatie en systemen vereist dat deze onder Nederlandse of Europese jurisdictie vallen. Waar volledige soevereiniteit niet haalbaar is, worden strenge contractuele en technische waarborgen toegepast om risico's te beperken en wordt gestreefd naar het opbouwen van alternatieven.

Data- en infrastructuurcontrole: Europese cloudoplossingen en technologieën voor de overheid krijgen prioriteit, maar bestaande leveranciers kunnen functioneren binnen duidelijke kaders die controle en zeggenschap garanderen. Dit wordt ondersteund door Europese certificering, zoals de EUCS, en initiatieven zoals Eurostack.

Digitale soevereiniteit maakt het mogelijk om publieke waarden, zoals privacy, veiligheid en transparantie, duurzaam te beschermen. Het biedt een basis om vertrouwen te behouden en verankeren in de digitale processen van de overheid.

3.3 Een gedeelde visie: autonomie en soevereiniteit in een veranderlijke wereld

De uitwerking van de begrippen digitale autonomie en soevereiniteit voor de overheid geeft houvast om gezamenlijk prioriteiten en uitgangspunten vast te stellen die richting geven aan beleid en uitvoering. Ze zijn nauw met elkaar verbonden en versterken samen de digitale weerbaarheid van de overheid. Autonomie en soevereiniteit zijn hierin geen doelen op zich, maar noodzakelijke voorwaarden om als overheid wendbaar, veilig en veerkrachtig te kunnen opereren in een steeds veranderende digitale en geopolitieke context.

Autonomie: zelfbeschikking en onafhankelijkheid

Autonomie stelt de overheid in staat strategische keuzes te maken zonder overmatige externe afhankelijkheden die de controle over systemen en processen beperken. Het vormt de basis voor zelfredzaamheid en innovatie, ook in tijden van geopolitieke of technologische druk. Daarbij behoudt de overheid de vrijheid om technologieën en infrastructuren onder eigen beheer te ontwikkelen of aan te sturen, terwijl samenwerking mogelijk blijft waar dat effectief is.

Soevereiniteit: zeggenschap en controle

Soevereiniteit is het vermogen om juridische en operationele controle te behouden over technologieën, systemen en data die essentieel zijn voor publieke dienstverlening en nationale veiligheid. Dit betekent dat vitale digitale processen zoveel mogelijk onder Nederlandse of Europese rechtsmacht vallen en worden beschermd tegen buitenlandse invloeden. Ook bij samenwerking met externe leveranciers blijft de overheid leidend, met heldere kaders die publieke waarden zoals privacy, veiligheid en transparantie beschermen.

Doel en resultaat: vergroten weerbaarheid van de overheid

Weerbaarheid is het vermogen om flexibel en proactief te anticiperen op risico's en adequaat te reageren op dreigingen zoals cyberaanvallen, technologische verstoringen of geopolitieke druk. Het garandeert de continuïteit en stabiliteit van overheidsdiensten, ongeacht de gekozen technologische of organisatorische aanpak. Autonomie en soevereiniteit dragen hieraan bij, door de handelingsruimte en controle te vergroten die nodig zijn om als overheid snel en doeltreffend te kunnen handelen.

4 Een realistische benadering

Het versterken van digitale autonomie en soevereiniteit is geen einddoel op zich. Het is een doorlopend proces van bewust kiezen, afwegen en samenwerken. De overheid wordt immers steeds afhankelijker van digitale infrastructuur om publieke taken goed te kunnen uitvoeren. Dat vraagt om meer grip op systemen, data en processen – zonder de illusie te hebben dat volledige autonomie haalbaar of wenselijk is. Veel afhankelijkheden zijn namelijk wederzijds en niet per se problematisch. Het categorisch uitsluiten van bepaalde dienstverleners past bovendien niet binnen het landenneutrale kabinetsbeleid. Sterker nog: dit kan het gelijke speelveld verstoren, de economische weerbaarheid schaden en de wederkerigheid op internationale markten onder druk zetten.

Maar: ambitie stuurt de verandering. De Nederlandse inzet is daarom gericht op verstandig omgaan met afhankelijkheden: open waar het kan, beschermen waar het moet. We zetten in op samenwerking met andere landen, behoud van een open economie en het versterken van Europese oplossingen. Tegelijkertijd nemen we meer verantwoordelijkheid waar onze kernbelangen op het spel staan.

Die balans is niet altijd makkelijk. Het is belangrijk te onderkennen dat deze verschuiving van focus niet van de ene op de andere dag gerealiseerd kan worden. Het versterken van autonomie en soevereiniteit vraagt langdurige investeringen in kennis, organisatie, infrastructuur en samenwerking en een duidelijke stip op de horizon. Ook vereist het dat we kritisch kijken naar de technologische fundamenten waarop onze digitale overheid rust. Legacy-systemen zijn daarin een kernvraagstuk: zij symboliseren het verlies aan wendbaarheid, de opbouw van afhankelijkheden, en de sluipende uitholling van publieke zeggenschap. In plaats van legacy te zien als last, moeten we het ook erkennen als strategisch knooppunt – en benutten als katalysator voor structurele modernisering op basis van publieke waarde.

De koers naar een meer autonomie en soevereine overheid zal onvermijdelijk gepaard gaan met dilemma's. Meer autonomie kan bijvoorbeeld betekenen dat er tijdelijk hogere kosten kunnen ontstaan, dat schaalvoordelen van bestaande leveranciers deels verloren gaan, of dat innovatie trager verloopt doordat men minder kan leunen op dominante marktpartijen. Deze visie onderkent deze spanningen en kiest nadrukkelijk voor een gefaseerde, realistische aanpak waarin de overheid bewust weegt waar directe zeggenschap cruciaal is, waar Europese oplossingen volstaan en waar afhankelijkheden acceptabel zijn. De Europese cloudmarkt is op dit moment nog niet volledig toegerust op de omslag naar meer Europese of nationale digitale autonomie en soevereiniteit. Tegelijkertijd zal die transformatie ook niet vanzelf plaatsvinden als wij als overheid de vraag aan de markt niet helder en richtinggevend formuleren. Om beweging te creëren is het van belang dat we onze strategische vraag expliciet maken en onze gezamenlijke inkoopkracht doelgericht inzetten naar een meer open ecosysteem. Alleen door als één overheid duidelijk te maken waar wij naartoe willen, kunnen wij de markt prikkelen en uitdagen om te investeren in soevereine en toekomstbestendige oplossingen die aansluiten op onze waarden en eisen.

Het gaat om het versterken van de interne basis, zodat de overheid niet alleen voorbereid is op uitdagingen, maar ook kansen kan benutten. Door de principes en bouwstenen in het volgende hoofdstuk intern te vertalen naar beleid, beheer en organisatie, legt de overheid een fundament voor een toekomst waarin zij met vertrouwen kan opereren in een complexe en steeds veranderende digitale wereld.

5 Strategische bouwstenen en leidende principes: de fundamenten van een toekomstbestendige digitale overheid

Om de digitale overheid van morgen te realiseren, zijn heldere leidende principes en strategische bouwstenen nodig die richting geven aan de inrichting en organisatie van de digitale infrastructuur van de overheid. De leidende principes definiëren de waarden en normen die als kompas dienen bij alle beslissingen en ontwikkelingen, terwijl de strategische bouwstenen de sleutelgebieden aangeven waarop de overheid zich richt om deze principes te realiseren. Samen vormen zij de basis voor een overheid die stevig grip heeft op haar digitale infrastructuur, haar processen en systemen beheerst, en effectief samenwerkt met partners binnen en buiten Nederland.

5.1 Leidende principes: het kompas voor een betrouwbare en toekomstbestendige digitale overheid

De digitale overheid van morgen vraagt om een stevig fundament van leidende principes die verder gaan dan louter technische inrichting. Deze principes geven richting aan de juridische, organisatorische, technische en semantische aspecten van de digitale infrastructuur en zorgen dat technologische vooruitgang in balans blijft met publieke waarden zoals vertrouwen, transparantie en legitimiteit.

Ze zijn ontwikkeld vanuit de unieke verantwoordelijkheid van de overheid in een digitaliserende samenleving: het waarborgen van zeggenschap, het beheersen van risico's, en het creëren van eenduidigheid in taal en standaarden. Met deze principes als kompas werkt de overheid aan een infrastructuur die niet alleen veilig en veerkrachtig is, maar ook juridisch verantwoord, bestuurlijk wendbaar en inhoudelijk helder.

1. Veerkracht en aanpassingsvermogen

De digitale infrastructuur van de overheid is bestand tegen veranderende ongunstige omstandigheden zoals verstoringen, faillissementen, cyberdreigingen en geopolitieke risico's. Veerkracht gaat verder dan alleen technische beveiliging: het omvat het vermogen om snel te herstellen, te leren van incidenten en flexibel in te spelen op nieuwe uitdagingen. Een essentieel onderdeel hiervan is portabiliteit – het vermogen om data, diensten en tooling los te koppelen van één specifieke aanbieder en over te brengen naar andere leveranciers. Dit versterkt niet alleen de handelingsvrijheid van de overheid, maar voorkomt ook langdurige ongewenste afhankelijkheden. Het bevorderen van de veerkracht en aanpassingsvermogen van de overheid vergroot de strategische flexibiliteit en waarborgt de continuïteit en betrouwbaarheid.

2. Democratische legitimiteit

De digitale infrastructuur van de overheid moet democratische processen en waarden ondersteunen. Het vertrouwen van burgers wordt gewaarborgd door transparantie, publieke controle en verantwoording. Besluitvorming over digitale systemen en technologieën zijn inzichtelijk en toetsbaar en sluiten aan bij publieke belangen en rechtvaardige afwegingen. Zo blijft de digitale overheid stevig verankerd in de democratische rechtsstaat.

3. Europese samenwerking en gedeelde waarden

De digitale infrastructuur van de overheid wordt ontwikkeld binnen en verbonden met een sterk Europees ecosysteem. Door nauwe samenwerking met Europese partners kan Nederland technologische afhankelijkheden verminderen, digitale autonomie versterken en collectieve weerbaarheid vergroten. Gedeelde uitgangspunten zoals privacy, veiligheid, weerbaarheid en rechtvaardigheid vormen de basis voor gezamenlijke oplossingen en standaarden die zowel nationaal als internationaal van waarde zijn. Daarnaast stelt samenwerking binnen Europa Nederland in staat om actief bij te dragen aan het vormgeven van internationale standaarden en regelgeving, waarin publieke waarden centraal staan. Zo versterken we niet alleen de strategische positie van Europa als geheel, maar ook die van Nederland als betrouwbare en invloedrijke partner in de mondiale digitale economie.

4. Risicobewust leiderschap

Digitale autonomie vraagt om een overheid die niet alleen risico's beheerst, maar ook risico's durft te nemen om digitale autonomie en soevereiniteit op te bouwen. Dit vereist een cultuur van 'risicobewust leiderschap' in plaats van risicomijdend leiderschap: leren van mislukkingen, sneller schakelen en ruimte geven aan experimenten. Binnen de overheid wordt vaak gekozen voor de veiligste weg, maar technologische en geopolitieke ontwikkelingen laten zien dat te veel terughoudendheid innovatie en weerbaarheid ondermijnt. Om deze reden moet de overheid strategische durf tonen, onder andere door pilotprojecten te faciliteren waarin innovatieve technologieën in de praktijk worden getest. Dit vraagt om bestuurlijke rugdekking en een kader waarin leren en bijsturen centraal staan.

5. Privacy en datasoevereiniteit als kern

De bescherming van persoonsgegevens en de zeggenschap over data en de verwerking daarvan staan centraal. De digitale infrastructuur wordt zodanig ontworpen dat informatie veilig wordt beheerd binnen Nederlandse of Europese jurisdictie. Privacy-by-design en dataminimalisatie vormen fundamentele uitgangspunten. Dit garandeert niet alleen juridische controle over data, maar versterkt ook het vertrouwen van burgers en bedrijven in de digitale overheid.

Deze leidende principes vormen een samenhangend en geïntegreerd kader. Democratische legitimiteit ligt aan de basis en waarborgt dat technologie in lijn is met publieke waarden en belangen. Dit versterkt privacy en datasoevereiniteit, die op hun beurt de grondslag leggen voor maatschappelijke betrokkenheid. Veerkracht en aanpassingsvermogen zorgen ervoor dat de infrastructuur robuust blijft in een dynamische wereld, terwijl Europese samenwerking niet alleen de autonomie versterkt, maar ook gedeelde waarden internationaal verankert.

5.2 Strategische bouwstenen: het versterken van de fundamenten voor een digitale toekomst

De strategische bouwstenen vormen de concrete focusgebieden waarop de overheid zich richt om de leidende principes te realiseren. Waar de principes het kompas bieden, geven de bouwstenen richting aan de uitvoering. Ze zijn specifiek ontworpen om de digitale infrastructuur van de overheid te versterken en toekomstbestendig te maken, met aandacht voor zelfbeschikking, samenwerking en maatschappelijke impact. Samen bieden deze bouwstenen een integraal kader dat de overheid in staat stelt om haar verantwoordelijkheid als betrouwbare dienstverlener en hoeder van publieke waarden waar te maken.

1. Grip op digitale autonomie

De overheid versterkt haar digitale autonomie ten aanzien van technologieën, informatie, systemen, processen en infrastructuren die van belang zijn voor haar functioneren. Dit houdt in dat zij bewuste keuzes maakt over waar investeringen (bijvoorbeeld in open source-technologieën), beschermende maatregelen of samenwerking (bijvoorbeeld met Europese partners) nodig zijn, of over waar het nodig is om digitaal soeverein te zijn. Digitale autonomie betekent niet alles zelf doen, maar wel grip houden op technologieën en processen die cruciaal zijn voor de nationale veiligheid en publieke waarden. Daarbij is het stapsgewijs uitfaseren van verouderde of beperkende legacy-systemen een belangrijke randvoorwaarde om ruimte te creëren voor duurzame, soevereine en toekomstbestendige alternatieven. De modernisering van legacy is daarmee niet enkel een technische operatie, maar een strategische opgave die raakt aan de kern van digitale autonomie.Het juist omgaan met legacy vormt daarmee een blijvende opgave.

2. Datasoevereiniteit

Volledige zeggenschap over data is een noodzakelijke voorwaarde voor het functioneren van een betrouwbare overheid. Datasoevereiniteit wordt gerealiseerd door data enkel binnen Nederlandse en/of Europese jurisdictie te houden, juridische controle te waarborgen en veilige infrastructuren te ontwikkelen voor opslag, verwerking en analyse. Door datasoevereiniteit te versterken, beschermt de overheid niet alleen de privacy van burgers, maar wordt ook de digitale autonomie gewaarborgd.

3. Cyberveiligheid en weerbaarheid

De overheid bouwt aan een robuuste eigen digitale infrastructuur die bestand is tegen cyberdreigingen en geopolitieke risico's. Cyberveiligheid omvat preventie, detectie en snelle respons op aanvallen, terwijl weerbaarheid betekent dat systemen flexibel enxveerkrachtig genoeg zijn om te herstellen van verstoringen. Deze bouwsteen vraagt om nauwe samenwerking met internationale partners, private sectoren en kennisinstituten om de Nederlandse overheid als een van de meest veilige digitale omgevingen ter wereld te positioneren.

4. Digitaal vakmanschap

Een autonome en soevereine overheid vereist voldoende kennis en kunde over het digitale domein. Zij heeft voldoende I-professionals met actuele kennis en expertise nodig om publieke waarden in een technologisch landschap te verankeren. Daarbij gaat het niet alleen om technische competenties, maar ook om strategisch en ethisch handelingsvermogen in een complex digitaal speelveld. Daarnaast is flexibele capaciteit nodig om snel te kunnen inspelen op technologische ontwikkelingen en digitale dreigingen. Alleen met voldoende kennis, kunde en aanpassingsvermogen kan de overheid grip houden op haar digitale toekomst.

5. Waardengedreven technologieontwikkelingen

Bij het ontwikkelen en toepassen van technologie zet de overheid ethiek en publieke waarden centraal. Dit houdt in dat nieuwe technologieën vooraf worden getoetst op maatschappelijke impact en rechtvaardigheid. De overheid stelt richtlijnen op om ervoor te zorgen dat innovatie niet alleen functioneel is, maar ook mensgericht en verantwoord. Door dit actief uit te dragen, positioneert Nederland zich als koploper in waardengedreven innovatie.

6. Digitale democratie

De overheid zet digitale technologie strategisch in om democratische processen te versterken en maatschappelijke betrokkenheid te vergroten. Transparante besluitvorming, toegankelijke digitale participatie en mensgerichte technologie vormen de kern. Innovatie draagt bij aan technologische autonomie en positioneert de overheid als koploper in verantwoorde digitale ontwikkeling.

Deze bouwsteen richt zich op het duurzaam versterken van vertrouwen in democratische instellingen in een digitaliserende samenleving.

7. Open innovatie en autonome voorzieningen

Door het inzetten van haar inkoopkracht stimuleert de overheid stimuleert technologische innovatie die bijdraagt aan digitale autonomie en soevereiniteit. Daarbij blijft zij ook gebruikmaken van de innovatiecapaciteit van marktpartijen, met waarborgen op het gebied van zeggenschap, transparantie en publieke waarden. Door in te zetten op open standaarden, open source en leveranciers-onafhankelijke interoperabele oplossingen en Europese alternatieven wordt de afhankelijkheid van gesloten, niet-Europese technologieën verkleind. Succesvolle toepassing hiervan vraagt ook aanvullende inzet om de implementatie door alle overheidslagen heen te borgen.

Overheidsopdrachten worden innovatiegericht ingericht om een open ecosysteem te stimuleren, waarin onderdelen zoals beheer, productie en onderhoud van elkaar zijn losgekoppeld en waarin Europese en publieke alternatieven kunnen floreren. Daarbij richt de overheid zich niet alleen op de markt van vandaag, maar versterkt zij stap voor stap de strategische basis door onderdelen uit trans-Atlantische clouds waar mogelijk over te brengen naar Europese (soevereine) oplossingen die publieke waarden borgen – ook als dat vraagt om het combineren van meerdere cloudomgevingen. Deze bouwsteen onderstreept het belang van gerichte investeringen, publiek-private samenwerking en experimenteerruimte binnen de overheid om technologische vernieuwing in lijn met publieke waarden te versnellen. Zo wordt autonomie een motor voor van innovatie.

6 Vervolg en slotwoord

Digitale autonomie en soevereiniteit zijn geen eindbestemmingen, maar voorwaarden om als overheid wendbaar, veilig en rechtvaardig te kunnen blijven opereren in een veranderlijke wereld. In een tijd waarin technologie zich snel ontwikkelt en veranderende geopolitieke verhoudingen elkaar opvolgen, is het essentieel dat de overheid strategische keuzes maakt die publieke waarden verankeren in de digitale infrastructuur van morgen.

Deze visie biedt daarvoor een gemeenschappelijk referentiepunt. Het biedt richting voor keuzes over infrastructuur, samenwerking, leveranciers en investeringen – keuzes die niet altijd eenvoudig zijn, maar wel noodzakelijk. Daarbij is consistent leiderschap nodig, eengedeeld handelingsperspectief en de bereidheid om samen, op nationaal en Europees niveau, te bouwen aan voorzieningen die passen bij onze publieke opdracht.

Om dit te realiseren, is voortdurende inzet nodig op het versterken van onze kennis, kunde en capaciteit, het ontwikkelen van standaarden en kaders, en het opzetten van duurzame samenwerkingen binnen Europa. De uitvoering vraagt om een flexibele aanpak waarin wordt geleerd, bijgestuurd en aangepast op basis van nieuwe inzichten, technologische ontwikkelingen en risicoafwegingen. Zo groeit de overheid mee met de opgaven van deze tijd, zonder haar koers op publieke waarden en zeggenschap te verliezen.

Het succes van deze koers hangt af van gezamenlijke inzet – van overheidsorganisaties, partners en marktpartijen. Alleen zo kunnen we komen tot een digitaal ecosysteem dat niet alleen functioneel en veilig is, maar ook recht doet aan onze democratische waarden, maatschappelijke doelen en internationale positie.

Met deze visie markeren we het begin van een koersvaste en waardengedreven inzet op digitale autonomie en soevereiniteit voor de overheid. De uitdaging is groot, maar de noodzaak en het momentum zijn helder. Nu is het moment om te handelen.

Deze brochure is een uitgave van:

Ministerie van Binnenlandse Zaken

Juni 2025