ONLINE TRUST COALITIE

Hoe hou je grip in een woelige wereld?

Een whitepaper over bestuurlijke, tactische en operationele digitale soevereiniteit

SEPTEMBER 2026

Managementsamenvatting

Digitale soevereiniteit klinkt snel groot en abstract. In de praktijk gaat het om een heel concrete bestuurlijke vraag: houdt de organisatie voldoende grip op kritieke data, diensten en digitale ketens als de wereld om u heen verandert? Deze whitepaper vertaalt dat vraagstuk naar keuzes die bestuurders, directies en interne toezichthouders vandaag kunnen maken.

Het vertrekpunt is digitale weerbaarheid. Organisaties moeten weten waar zij kwetsbaar zijn, welke afhankelijkheden zij accepteren en welke maatregelen nodig zijn om de continuïteit van hun IT, en daarmee steeds vaker ook de continuïteit van de organisatie, de vertrouwelijkheid van data en de operationele controle aantoonbaar te versterken. Dat is geen theoretische exercitie meer. Geopolitieke spanningen, sancties, concentratie van technologieaanbieders en complexe digitale ketens maken de risico's van digitale afhankelijkheid tot een bestuursvraagstuk.

De kernboodschap van dit paper: impliciet vertrouwen is niet langer genoeg. Organisaties kunnen er niet meer vanzelfsprekend van uitgaan dat hun leveranciers in digitale ketens zich onder alle omstandigheden aan contracten, afspraken, wetten en regels blijven houden, of altijd in het belang van hun afnemers zullen handelen. Afhankelijkheidsrisico's horen daarom thuis in reguliere governance, in risicobeheer, leverancierssturing, assurance en dus in intern toezicht.

Digitale soevereiniteit is daarmee geen streven naar volledige autonomie. Het gaat niet om alles weer zelf gaan doen, of om afscheid nemen van internationale technologie. Het gaat om bestuurbare afhankelijkheid: weten waar de organisatie afhankelijk van is, begrijpen wat er kan misgaan en voorbereid zijn als juridische, geopolitieke of operationele omstandigheden veranderen.

Voor directie en toezicht zijn vooral de volgende aandachtspunten van belang:

- **Maak digitale soevereiniteit onderdeel van goed bestuur.** Het is geen louter technische- of IT-kwestie. Behandel soevereiniteitsrisico's als continuïteits-, veiligheids- en compliancevraagstukken en veranker die expliciet in governance, risicobeheer, interne beheersing en toezicht.
- **Maak digitale afhankelijkheden expliciet.** Breng lock-in, concentratierisico's en zeggenschapsrelaties in beeld en betrek deze bij leverancierskeuzes, architectuur, risicobeoordelingen en strategische besluitvorming.
- **Wees voorbereid op geopolitieke ontwikkelingen.** Houd rekening met scenario's waarin zulke ontwikkelingen ertoe leiden dat partijen zich niet langer kunnen of willen houden aan contracten en aan de principes van de rule of law. Beoordeel daarom ook de gevolgen van sancties, politieke druk en beïnvloeding via eigendom, bestuur en digitale ketens.
- **Organiseer wendbaarheid en exit-vermogen voordat deze nodig zijn.** Gebruik waar mogelijk open standaarden en kies architecturen die interoperabiliteit en vervangbaarheid ondersteunen, zodat kritieke digitale processen niet onnodig afhankelijk worden van één leverancier of rechtsgebied.
- **Borg vertrouwen actief.** Ook als de beheersing op orde is, kan geopolitieke onzekerheid het vertrouwen in digitale dienstverlening onder druk zetten. Werk daarom met de OTC-principes Criteria, Controle en Communicatie: bepaal het gewenste beheersingsniveau, laat dit onafhankelijk toetsen en communiceer helder over uitkomsten en restrisico's.
- **Ook de overheid heeft een belangrijke rol.** Zij kan digitale weerbaarheid en vertrouwen versterken door transparantie over digitale afhankelijkheden te bevorderen, open standaarden en interoperabiliteit te stimuleren en beheersing van soevereiniteitsrisico's expliciet onderdeel te maken van toezicht en bestaande weerbaarheidskaders.

Inhoud

Inleiding

Dit document benadert digitale soevereiniteit niet als eindbeeld maar als discipline: het vermogen om kritieke afhankelijkheden en risico's in digitale ketens te begrijpen en te toetsen, vervolgens maatregelen te nemen om het geheel bestuurbaar en beheersbaar te houden.

De urgentie van digitale soevereiniteit is de afgelopen jaren sterk toegenomen. Geopolitieke spanningen, economische sancties, exportrestricties en de inzet van digitale middelen als geopolitiek instrument laten zien dat digitale afhankelijkheden niet langer alleen technische of economische vraagstukken zijn. Digitale infrastructuur is onderdeel geworden van economische veiligheid, nationale veiligheid en strategische autonomie.

Jarenlang werd mondiale sourcing van digitale diensten vooral gezien als een bron van efficiëntie, innovatie en schaalvoordeel. Dat beeld is te beperkt geworden. Concentratie van marktmacht en diepe internationale digitale ketens maken duidelijk dat afhankelijkheid van technologie en technologieaanbieders ook een kwetsbaarheid kan zijn.

Voor veel organisaties is die kwetsbaarheid inmiddels direct relevant. Zij zijn voor communicatie, dataopslag, identiteitsbeheer, softwareontwikkeling en operationele processen afhankelijk van leveranciers, platforms en onderliggende ketens. Over die ketens hebben zij zelden directe controle. Vaak berust die controle vooral op het vertrouwen dat partijen zich aan contracten, afspraken en wet- en regelgeving blijven houden.

Die vanzelfsprekendheid staat onder druk en dat vraagt om een ander perspectief. Digitale soevereiniteit gaat niet over autarkie of volledige directe zeggenschap over alle diensten, mensen en middelen. Dat is zelden operationeel of economisch haalbaar. Digitale afhankelijkheden zijn en blijven een gegeven. Het accent ligt daarom op het vermogen van organisaties om voldoende grip te houden op de beschikbaarheid, integriteit, vertrouwelijkheid, privacy en continuïteit van hun digitale voorzieningen in een wereld die minder voorspelbaar is dan voorheen.

De opbouw van dit paper volgt die vraag stap voor stap. Eerst bakenen we het begrip digitale soevereiniteit af. Daarna bespreken we digitale ketens en toetsingsinstrumenten. Vervolgens volgt de juridische context en ten slotte werken we concrete maatregelen uit voor overheid, organisaties en serviceproviders.

Het accent ligt daarom op het vermogen van organisaties om voldoende grip te houden op de beschikbaarheid, integriteit, vertrouwelijkheid, privacy en continuïteit van hun digitale voorzieningen in een wereld die minder voorspelbaar is dan voorheen.

1. Wat is digitale soevereiniteit?

In veel literatuur wordt digitale soevereiniteit breed gedefinieerd. Het begrip soevereiniteit wordt meestal besproken op het niveau van staten. In een digitale samenleving hangt die soevereiniteit echter steeds meer af van technologie. Een moderne economie kan nauwelijks functioneren zonder betrouwbare digitale infrastructuur voor communicatie, betalingen, zorg, overheid, logistiek en bedrijfsvoering. Die infrastructuur is daarmee even vitaal geworden als elektriciteit of water. Als een land of organisatie onvoldoende grip heeft op zulke digitale basisvoorzieningen, komt niet alleen de continuïteit van de IT zelf onder druk te staan, maar uiteindelijk ook de bestuurlijke en maatschappelijke zelfstandigheid.

In dit whitepaper sluiten we aan bij het perspectief van de OTC: digitale technologie moet zó worden beheerst dat het vertrouwen in een goed functionerende digitale samenleving behouden blijft. In gewone taal betekent dit dat organisaties moeten weten waar zij afhankelijk van zijn, welke risico's daarbij horen en welke maatregelen nodig zijn om het geheel bestuurbaar te houden.

Digitale soevereiniteit definiëren we daarom als de mate waarin organisaties risico's voor beschikbaarheid, continuïteit, integriteit, vertrouwelijkheid, privacy en bestuurbaarheid kunnen begrijpen en expliciteren, en vervolgens effectieve maatregelen voor beheersing kunnen implementeren. In dit whitepaper gaat het specifiek om risico's door ingrepen in leveringsketens als gevolg van geopolitieke ontwikkelingen of acties in of vanuit andere jurisdicties.

Digitale soevereiniteit gaat dus niet alleen over de beschikbaarheid van IT-systemen. Het gaat ook over de vraag of gegevens vertrouwelijk blijven, of processen betrouwbaar blijven functioneren en of organisaties zelf kunnen bepalen wie toegang heeft tot data, systemen en beheeromgevingen.

In het publieke debat wordt digitale soevereiniteit vaak benaderd vanuit drie invalshoeken: strategisch, tactisch en operationeel. Voor dit whitepaper is vooral van belang dat deze drie invalshoeken geen losse werelden zijn. Ze beschrijven hetzelfde vraagstuk op verschillende niveaus en werken door in concrete bestuurlijke, tactische en operationele keuzes voor IT-beheersing.

- **Strategisch:** het vermogen om afhankelijkheden op langere termijn te verminderen en te kunnen schakelen wanneer geopolitieke of marktomstandigheden veranderen. Dat vraagt om wendbaarheid, gebruik van open standaarden, beperking of voorkoming van lock-in en beschikbare alternatieven.
- **Tactisch:** de inrichting van governance, risicobeheer, compliance, leveranciersturing en assurance. Op dit niveau wordt bepaald welke eisen gelden voor digitale ketens, welke restrisico's aanvaardbaar zijn, hoe toetsing plaatsvindt en welke maatregelen nodig zijn om aan wet- en regelgeving en eigen beleidsdoelen te voldoen.
- **Operationeel:** de feitelijke beheersing van toegang, beheer, logging, encryptie, continuïteit, herstel en doorwerking van beleidskeuzes in de keten. Hier wordt zichtbaar of een organisatie in de praktijk voldoende grip heeft op haar data, systemen en kritieke afhankelijkheden.

2. Digitale ketens

Moderne digitale toepassingen bestaan uit diepe en brede ketens van leveranciers en diensten, en kennen dus veel afhankelijkheden. Achter een ogenschijnlijk eenvoudige dienst gaan vaak vele lagen schuil: hardware, firmware, besturingssystemen, open source- en proprietary componenten, identity en access management, netwerken, datacenters, beheer- en monitoringtools, package repositories, licentieservers, certificate authorities en domeinregistrars, en zo voorts. Veel van die schakels zijn diensten (digital services), die allemaal goed moeten functioneren om het geheel beschikbaar, veilig en beheersbaar te houden.

Een belangrijk soevereiniteitsrisico vormt concentratie van afhankelijkheden. Organisaties zijn steeds vaker afhankelijk van een beperkt aantal cloudproviders, identiteitsdiensten, softwareplatforms, beheerdienstverleners, certificaatautoriteiten en open source-componenten. Deze worden in grote delen van de economie gebruikt. Uitval, verstoring of beïnvloeding van zulke partijen kan daardoor gevolgen hebben die veel verder reiken dan één organisatie.

Digitale soevereiniteit vraagt daarom niet alleen aandacht voor individuele leveranciers, maar ook voor concentratierisico's binnen gehele digitale ecosystemen. Organisaties hebben vaak redelijk zicht op hun directe leverancier, maar aanzienlijk minder zicht op onderliggende softwarecomponenten, beheerdienstverleners, open source-afhankelijkheden en operationele ketens. Juist in deze diepere lagen kunnen afhankelijkheden ontstaan die pas zichtbaar worden wanneer een verstoring optreedt. Het expliciet in kaart brengen en doorgronden van deze first-tier en onderliggende afhankelijkheden is daarom een belangrijk onderdeel van tactische digitale soevereiniteit.

ESSENTIËLE DIENSTEN

Juist daarom is digitale soevereiniteit geen abstract begrip. Waar ketens diep, ondoorzichtig of geconcentreerd zijn en het om veel schakels gaat, neemt de feitelijke beheersing door afnemers af. Dat geldt des te sterker wanneer het gaat om diensten die essentieel zijn voor bedrijfsvoering, publieke taken of vitale maatschappelijke processen. De dimensie cloud voegt daaraan toe dat de effecten van falen en ingrepen onmiddellijk voelbaar zijn, wat de risicoperceptie verder beïnvloedt.

Recente Europese wetgeving benoemt specifiek die effecten op ketens en de maatschappij en verplicht betrokken organisaties en hun bestuurders expliciet om die keteneffecten in hun beleid te adresseren. Dat betekent dat digitale soevereiniteit ook onderdeel is van de implementatie van die wet- en regelgeving in zulke organisaties.

3. Toetsingsinstrumenten voor bepaling van soevereiniteitsrisico's

Als soevereiniteitsrisico's niet adequaat worden beheerst erodeert dat vertrouwen. We benadrukken daarom opnieuw het OTC-perspectief: soevereiniteitsvraagstukken zijn geen apart thema, maar zijn onderdeel van bestaande IT governance- en beheerskaders, zoals BIV+P, COSO en COBIT. Zij passen ook binnen wettelijke verplichtingen uit cyber- en weerbaarheidswetgeving zoals de Cyberbeveiligingswet, CER, DORA en andere kaders. Het proces van risicobeoordeling en mitigatie verandert daardoor niet fundamenteel door soevereiniteit, maar wordt wel specifieker: het omvat explicieter de risico's van mondiale sourcing van IT.

De risk-based insteek betekent niet dat diensten van niet-Europese aanbieders altijd bruikbaar zijn zolang er interne beheersmaatregelen bestaan. Sommige situaties vragen om een zeer hoog beheersingsniveau en/of een laag acceptatieniveau van restrisico. Dat niveau kan soms niet, of niet langer, met bestaande aanbieders worden gerealiseerd. Ook de risicoperceptie van externe stakeholders kan doorslaggevend zijn. Voor vitale, staatskritieke of hoog-gerubriceerde processen kan het daarom noodzakelijk zijn afhankelijkheden van specifieke jurisdicties, eigendomsstructuren of leverancierscategorieën volledig uit te sluiten. In zulke situaties volstaan aanvullende beheersmaatregelen niet langer. Architectuurkeuzes, leverancierskeuzes en locatiekeuzes worden dan onderdeel van het risicobeheer en vragen om strategische keuzes.

In de context van digitale soevereiniteitsrisico's bespreken we twee specifieke toetsingsinstrumenten die kunnen helpen bij het ontwerp van de beheersing. Het vertrekpunt voor inzet van één of beide instrumenten is de vraag in welke mate soevereiniteitsrisico's voor een specifieke toepassing moeten worden beheerst of uitgesloten. Beide frameworks bieden deelonderwerpen en vragen die helpen bij het bepalen van het gewenste ambitieniveau voor risicobeheersing. Zij spreken beide over gradaties, niet over absolute zekerheden, en evenmin over soevereiniteit als binair begrip.

Vervolgens kan met de vragen, onderwerpen en toetsing uit de frameworks worden bepaald of een specifieke inrichting van leveranciers, diensten en aanvullende mitigerende maatregelen dat ambitieniveau kan halen.

HET EU CLOUD SOVEREIGNTY FRAMEWORK

Het eerste toetsingsmodel voor het identificeren en mitigeren van soevereiniteitsrisico's in organisaties is het EU Cloud Sovereignty Framework (Europese Commissie, 2025). Dit framework werd in 2025 door de Europese Commissie gepubliceerd en biedt een beoordelingskader voor de risico's van clouddiensten. Het doel is organisaties te helpen de afhankelijkheid van buitenlandse IT-aanbieders in kaart te brengen, zodat de beheersing van strategische, juridische, operationele en technologische aspecten van cloudgebruik binnen de EU kan worden versterkt.

Het framework onderscheidt de volgende risico's:

- **Extraterritoriale wetgeving** (bv. CLOUD Act, FISA 702): kan leiden tot ongewenste toegang tot data door niet-EU autoriteiten.
- **Technologische lock-in**: blokkades om snel van provider te wisselen door afhankelijkheid van (niet-EU) leveranciers met gesloten ecosystemen.
- **Supply chain kwetsbaarheid**: risico dat levering van hardware en software wordt onderbroken.
- **Operationele afhankelijkheid**: onvoldoende **beheersing** over voorzieningen in de keten (beheer en onderhoud).
- **Juridische ambiguïteit**: onduidelijkheid over afdwingbaarheid van EU-rechten bij internationale conflicten.
- **Strategische afhankelijkheid**: sterke machtsconcentratie van digitale infrastructuur bij een klein aantal niet-EU-hyperscalers.
- **Compliance gaps**: disconnectie tussen cybersecurity-certificering (bijv. EUCS) en soevereiniteitscriteria.
- **Duurzaamheidsrisico's**: energie-intensieve infrastructuur zonder robuuste lange termijn strategie.

Deze risico's raken uiteindelijk BIV+P: beschikbaarheid, integriteit, vertrouwelijkheid en privacy. BIV+P correspondeert met de internationale CIA+P-indeling: availability, integrity, confidentiality en privacy.

- **Vertrouwelijkheid**: kan worden aangetast door de potentiële effecten van extra-territoriale wetgeving, bijvoorbeeld wanneer toegang tot data mogelijk wordt voor onbevoegde partijen dieper in de digitale keten.
- **Integriteit**: kan in gevaar komen wanneer onbevoegden of gecompromitteerde hard- of software dieper in de keten data wijzigen.
- **Beschikbaarheid**: kan worden verstoord door denial-of-service, het onbeschikbaar maken van diensten, verstoringen in energievoorziening of uitval van apparatuur dieper in de keten.
- **Privacy**: kan onder druk komen te staan door juridische onzekerheid of tekortkomingen in compliance.

Het framework bevat een ratingmodel met vier niveaus, waarbij niveau 4 de hoogste mate van soevereiniteit aangeeft. Hiermee benadrukt ook de Europese Commissie dat soevereiniteit geen binair begrip is, maar een gradueel spectrum.

Ook duurzaamheid wordt in dit framework als een continuïteitsrisico beschouwd: een te grote energievraag kan leiden tot druk op energievoorziening in andere kritieke sectoren.

HET DICTU TOETSINGSINSTRUMENT CLOUDDIENSTEN

Ook in Nederland bestaat een toetsingsinstrument voor soevereiniteit van clouddiensten van DICTU, de Dienst ICT Uitvoering van het ministerie van Economische Zaken. Dit instrument maakt het mogelijk om de mate van soevereiniteit van een aanbieder te bepalen aan de hand van vijf dimensies:

- **Juridisch:** Aan welk juridisch en politiek systeem is de aanbieder uiteindelijk verantwoording schuldig?
- **Data en AI:** In welke mate zijn gegevens aantoonbaar beschermd, in zowel juridische als technische zin?

- **Technologie:** Biedt de technologie autonomie, inzichtelijkheid, weerbaarheid en portabiliteit voor de klant?
- **Operationeel:** Wie heeft de controle over de operationele omgeving van de dienst?
- **Mens:** In hoeverre is er zichtbaarheid en controle over wie toegang heeft tot systemen en data, en beschikt het personeel over de kennis en vaardigheden om soevereine, duurzame, veilige en innovatieve clouddiensten te ontwikkelen en te beheren?

Bij de ontwikkeling van het toetsingsinstrument heeft DICTU overigens gebruik gemaakt van het EU Cloud Sovereignty Framework. Daarmee sluit het goed aan op de kern van dit white-paper: digitale soevereiniteit moet concreet toetsbaar worden gemaakt in keuzes over leveran-ciers, architectuur, toegangsbeheer, beheerprocessen en de inzet van mensen.

Conclusie

Beide instrumenten helpen organisaties om soevereiniteitsrisico's systematisch te duiden en expliciet te maken. Daarmee worden zij bruikbaar als onderdeel van reguliere governance, leveranciersbeoordeling, architectuurkeuzes en interne beheersing.

Het moeilijkste punt blijft de bestuurlijke weging van risico's: welke afhankelijkheden zijn aanvaardbaar en welke niet? En welke maatregelen zijn nodig als juridische, politieke of ope-rationele omstandigheden verslechteren? Die bepaling is geen exacte wetenschap. Risico-in-schattingen kunnen sterk verschillen tussen stakeholders, en voor publieke organisaties speelt ook de perceptie van eindgebruikers en het maatschappelijke discours een belangrijke rol. Kortom, het gaat er niet alleen om dat de organisatie zelf van mening is dat de beheersing ade-quaat is, ook andere stakeholders zullen vertrouwen moeten krijgen dat er voldoende grip is.

Daarom is de aanbeveling om naast de genoemde kaders, ook de OTC-kerngedachte uit het eerdere whitepaper *Vertrouwen in de cloud* in de afwegingen mee te nemen: vertrouwen ont-staat door een samenhang van Criteria, Controle en Communicatie.

Criteria maken expliciet welk niveau van beheersing nodig is voor beschikbaarheid, integriteit, vertrouwelijkheid en privacy.

Controle zorgt voor onafhankelijke, kwalitatief hoogstaande beoordeling van de feitelijke werking op basis van standaarden en normen.

Communicatie vertaalt criteria en controle-uitkomsten naar de informatiebehoefte van specifieke doelgroepen, zodat duidelijk wordt waar vertrouwen op gebaseerd is en welke restrisico's blijven bestaan.

4. De juridische context

Het juridische debat over digitale soevereiniteit is relevant omdat het laat zien dat controle over data en dienstverlening niet alleen technisch wordt bepaald, maar ook door jurisdictie, rechtskeuze en de vraag welke wetgeving in conflictsituaties de doorslag geeft. Voor organisaties is het minder relevant om elk juridisch detail te doorgronden, maar om te begrijpen welke juridische kwesties risico's zijn en waarom die bestuurlijke en operationele maatregelen vereisen.

LAWFUL VERSUS LAWFARE

Voor de duiding van die risico's helpt een onderscheid tussen twee uitersten: **lawful** en **lawfare**.

In een **lawful**-scenario handelen staten en organisaties in hoofdzaak binnen de grenzen van geldende wetgeving, verdragen en rechtsbescherming. Conflicten tussen rechtsstelsels zijn dan lastig, maar in beginsel juridisch adresseerbaar. Dat was lange tijd het impliciete uitgangspunt onder de mondiale digitale economie.

In een **lawfare**-scenario wordt wetgeving of juridische druk ingezet als geopolitiek instrument. Dan verschuift het risicobeeld. Het gaat niet meer alleen om de vraag wat formeel rechtmatig is, maar ook of bedrijven en bestuurders onder politieke of juridische druk bereid zijn en/of gedwongen worden te handelen in strijd met belangen, verwachtingen of zelfs wetgeving in het land van levering. Voor risicobeheersing is lawfare daarom geen theoretische kwestie meer, maar een serieus ontwerpscenario.

Het is duidelijk dat in de mondiale digitale economie van vandaag een verschuiving zichtbaar is van het lawful-scenario naar situaties waarin elementen van lawfare een grotere rol spelen.

Recente geopolitieke ontwikkelingen laten zien dat economische sancties, exportbeperkingen, investeringsrestricties en nationale veiligheidsmaatregelen steeds vaker worden ingezet als instrument van buitenlands beleid. Voor organisaties betekent dit dat scenario's waarin digitale diensten of technologie om geopolitieke redenen beperkt beschikbaar raken niet langer theoretisch zijn, maar onderdeel moeten worden van regulier risicobeheer.

We bespreken eerst het **lawful**-scenario. Daarbij maken we onderscheid tussen internationaal recht en de extraterritoriale werking van nationale wetgeving. Vervolgens analyseren we het **lawfare**-scenario en de mogelijke gevolgen daarvan voor digitale infrastructuur en diensten.

HET LAWFUL-SCENARIO

Soevereiniteit en internationaal recht

In het internationaal recht geldt in beginsel dat staten soeverein zijn en dat hun rechtsorde leidend is op eigen grondgebied. Binnen de EU betekent dit bovendien dat Europese en nationale regels gelden voor entiteiten die hier diensten leveren. In een rechtsstatelijk scenario hoort die rechtsorde dus leidend te zijn voor vertrouwelijkheid, continuïteit en bescherming van gegevens en diensten in de EU.

De praktijk is echter weerbarstiger. Extraterritoriale wetgeving, buitenlandse bevelen en sanctieregimes kunnen druk zetten op aanbieders en bestuurders die onderdeel zijn van internationale ketens. Dat verklaart waarom in het soevereiniteitsdebat zoveel aandacht uitgaat naar rechtskeuze, locatie, eigendomsstructuren en bestuurlijke loyaliteit.

Europese wetgeving

De Europese Unie heeft de afgelopen jaren veel wet- en regelgeving aangenomen voor het digitale domein. Veel van deze wet- en regelgeving bevat elementen die van belang zijn voor de bescherming van de digitale weerbaarheid van de Unie en haar lidstaten. Soevereiniteit speelt daarin een steeds grotere rol. Belangrijke wetten zijn onder meer:

- De General Data Protection Regulation (GDPR, in Nederland de Algemene Verordening Gegevensbescherming – AVG) voor de bescherming van persoonsgegevens
- De Digital Operational Resilience Act (DORA) voor de financiële sector
- De Cyber Security Act (CSA)
- De Cyber Resilience Act (CRA)
- De Network and Information Security Directive (NIS2, in Nederland de Cyberbeveiligingswet – Cbw)
- De Critical Entities Resilience Directive (CER, in Nederland de Wet weerbaarheid kritieke entiteiten – Wwke)

Al deze wetten bevatten maatregelen om de digitale weerbaarheid te beschermen. Hieronder vallen onderwerpen zoals beveiliging van de toeleveringsketen en de zorgplicht van bestuurders. Vooral die verantwoordelijkheid en aansprakelijkheid van bestuurders is aangescherpt. Bestuurders moeten voldoende kennis hebben van het digitale domein om dit effectief te kunnen besturen. In sommige gevallen kunnen zij persoonlijk aansprakelijk zijn als hun organisatie niet voldoet aan EU-wetgeving of bij incidenten. Het sanctiebeleid is stevig en kan variëren van schorsing tot boete, ontslag en persoonlijke aansprakelijkheid.

Het EU- en NL-recht biedt hiermee voldoende aanknopingspunten om organisaties en bestuurders te verbieden om uitvoering te geven aan opdrachten die de vertrouwelijkheid of continuïteit van systemen kunnen schaden, zeker als het om specifieke, essentiële diensten gaat. In de AVG staat zelfs een passage die organisaties en hun bestuurders expliciet verbiedt om uitvoering te geven aan opdrachten die gebaseerd zijn op niet-Europese wet- en regelgeving en strijdig zijn met de criteria van de AVG.

Dat neemt niet weg dat er aan de andere kant van het spectrum wetten en sancties bestaan die bestuurders kunnen raken als gevolg van wetgeving die geldt in het moederland van de organisatie.

Wetgeving met extraterritoriale effecten op EU-IT-diensten

Voor de praktijk is vooral van belang dat bepaalde niet-Europese wettelijke regimes extra-territoriale effecten kunnen hebben. In het debat over digitale soevereiniteit wordt daarom vaak verwezen naar instrumenten als de US CLOUD Act, FISA 702, Executive Order 12333 en IEEPA[1]. Het precieze juridisch-technische verschil tussen die instrumenten is relevant voor specialisten, maar voor bestuur en risicobeheer is vooral van belang welk type risico zij kunnen veroorzaken.

Samengevat kunnen zulke instrumenten leiden tot drie soorten druk: gerichte vorderingen tot verstrekking van gegevens, ruimere vormen van inlichtingenvergaring en economische of sanctieregimes die dienstverlening of leveringen kunnen raken. Daarbij is het wel van belang scherp te blijven op de aard van die instrumenten. In een regulier *lawful*-scenario bieden de CLOUD Act en Executive Order 12333 geen zelfstandige basis om bedrijven op te dragen complete diensten generiek uit te zetten voor hele landen of organisaties. Zij zien primair op toegang tot gegevens, inlichtingenvergaring en daarmee samenhangende bevoegdheden, niet op een algemene opdracht tot digitale uitsluiting of algehele denial of service.

In de genoemde wetten vinden we onder meer:

- gerichte vorderingen tot verstrekking van gegevens,
- ruimere vormen van inlichtingenvergaring en
- economische of sanctieregimes die dienstverlening of leveringen kunnen raken.

Zij maken ook duidelijk dat locatie van data of een contractuele verwijzing naar EU-recht op zichzelf geen immuniteit biedt tegen de mogelijkheid dat zulke opdrachten een organisatie kunnen bereiken.

Effecten op veiligheid en continuïteit in het lawful-scenario

In een overwegend lawful-scenario zijn veel van deze risico's juridisch begrensd en gedeeltelijk mitigeerbaar. Gerichte gegevensvorderingen en toezichtmechanismen zijn niet hetzelfde als willekeurige bulktoegang of het uitzetten van complete diensten. Dat onderscheid is belangrijk: instrumenten als de CLOUD Act en EO 12333 rechtvaardigen in dat scenario niet zonder meer een algemene opdracht aan bedrijven om diensten voor een land, sector of individuele organisatie integraal uit te schakelen. De IEEPA biedt wat dat betreft meer mogelijkheden. Ook in dit lawful-scenario blijft gelden dat Europese bescherming van persoonsgegevens, vertrouwelijkheid en rechtsbescherming niet altijd volledig samenvallen met de bescherming die in derde landen wordt geboden. Juridisch comfort is dus geen beheersmaatregel.

HET LAWFARE-SCENARIO

In een lawfare-scenario verandert de afweging wezenlijk. Dan nemen de voorspelbaarheid van rechtsbescherming, de waarde van contractuele afspraken en de betrouwbaarheid van impliciete aannames af. Juist daarom moeten organisaties niet alleen kijken naar formele compliance, maar ook naar afhankelijkheden, concentratierisico's, fallbackopties, exitvermogen en feitelijke operationele beheersing.

[1] IEEPA staat voor International Emergency Economic Powers Act — het is Amerikaanse wetgeving waarmee de VS economische maatregelen kan nemen, waaronder controle over technologie en data toegang.

Rechtskeuze en locatie

Rechtskeuze en locatie blijven daarbij belangrijk. Voor kritieke ketens is het niet verdedigbaar om impliciet of expliciet niet-EU-recht leidend te laten zijn. Tegelijk geldt dat exclusieve EU-rechtskeuze en datalocatie wel noodzakelijke, maar geen voldoende voorwaarden zijn. Ook dan blijven operationele afhankelijkheden, eigendomsstructuren, inmenging, toeleveringsketens en bestuurlijke druk relevante risicofactoren.

Daarmee is de juridische hoofdles niet dat elk risico volledig juridisch kan worden uitgesloten, maar dat organisaties hun beheersing niet mogen baseren op aannames over welwillendheid, stabiliteit of vanzelfsprekende loyaliteit in internationale digitale ketens.

Lawfare: de erosie van de rule of law

De kern is daarom eenvoudig: lawful en lawfare vragen niet om twee totaal verschillende denkwerelden, maar wel om een ander ambitieniveau in risicobeheer. In beide gevallen moeten organisaties afhankelijkheden verkleinen, single points of failure beperken en alternatieven voorbereiden. In een lawfare-scenario worden die maatregelen alleen urgenter en minder vrijblijvend.

Daarmee is de juridische hoofdles niet dat elk risico volledig juridisch kan worden uitgesloten, maar dat organisaties hun beheersing niet mogen baseren op aannames over welwillendheid, stabiliteit of vanzelfsprekende loyaliteit in internationale digitale ketens.

Conclusie juridische impact

De juridische context maakt dus vooral duidelijk waarom digitale soevereiniteit thuishoort in reguliere governance, risicobeheer en operationele beheersing. Niet omdat elk juridisch risico exact voorspelbaar is, maar omdat afhankelijkheden, rechtskeuze, concentratie en bestuurlijke druk directe gevolgen kunnen hebben voor vertrouwelijkheid, continuïteit en beheersing.

Daarom is de volgende vraag beslissend: welke concrete maatregelen zijn nodig om die risico's vandaag expliciet te maken, te verkleinen en bestuurlijk beheersbaar te houden?

DE ZEGGENSCHAPSROUTE ALS JURIDISCH EN OPERATIONEEL CRITERIUM

Een gevoelig punt in het soevereiniteitsdebat is de perceptie dat organisaties of leveranciers alsnog uitvoering kunnen geven aan niet-Europese wetgeving. Dat kan bijvoorbeeld via aandeelhouderschap, moedermaatschappijen, bestuurdersbenoemingen of andere zeggenschapslijnen. Artikel 48 AVG onderstreept dat besluiten van autoriteiten uit derde landen niet automatisch in de EU kunnen worden erkend of afgedwongen. Toch neemt dat de zorg niet volledig weg. Lawfare kan via concernstructuren, bestuurders of operationele ketens een feitelijk aangrijpingspunt vormen. Zo'n zorg kan alleen worden weggenomen als het uitsluiten van zulke routes onderdeel is van expliciete criteria.

In eerdere versies en discussies rond het EUCS werd voor het hoogste zekerheidsniveau in vergelijkbare termen gesproken over zulke eisen. Het doel was uit te sluiten dat niet-EU-jurisdicties werking konden hebben via aanbieder, eigendom of controle. Daarmee werd juridische soevereiniteit niet alleen behandeld als compliancevraag, maar ook als zelfstandig criterium voor vertrouwen. Ook in de Cloud and AI Development Act (CADA) wordt soevereiniteit als voorwaarde voor het hoogste zekerheidsniveau voorgeschreven. Zowel EUCS als CADA zijn overigens nog in ontwikkeling.

Daar zit echter meteen praktische spanning. Een criterium dat volledige uitsluiting van een theoretische aangrijpingsmogelijkheid vraagt, is buitengewoon lastig toetsbaar. Een auditor kan vaststellen welke juridische entiteiten, contracten, beheerrollen, datastromen, toegangspaden en escalatielijnen bestaan. Maar bewijzen dat nergens in een complexe internationale keten een aangrijpingspunt voor niet-EU-wetgeving kan bestaan, lijkt al snel op een bewijs uit het ongerijmde. Hoe dieper de keten, hoe moeilijker het wordt om niet alleen bekende risico's, maar ook onbekende of indirecte beïnvloedingsroutes uit te sluiten.

Ook de proportionaliteitsvraag blijft noodzakelijk: wegen de kosten, complexiteit en uitvoeringsrisico's van het volledig vervangen van diensten, organisaties, onderaannemers en personeel die theoretisch onder buitenlandse invloed zouden kunnen vallen, op tegen de extra zekerheid die daarmee wordt bereikt? Voor sommige vitale of staatskritieke toepassingen kan het antwoord ja zijn. Voor veel andere toepassingen zal een combinatie van transparantie, onafhankelijke controle, contractuele waarborgen, technische segmentatie, sleutelbeheer, logging, exitvermogen en gerichte communicatie over restrisico's een realistischer en beter verdedigbaar beheersingsniveau opleveren.

5. Wat kunnen we doen om de risico's te verkleinen?

Voor de EU is de strategische richting helder: afhankelijkheden moeten worden verminderd, de eigen digitale slagkracht moet worden vergroot en er moet sterker EU-aanbod komen. Maar organisaties kunnen niet wachten tot die strategische opgave volledig is gerealiseerd. Zij moeten nu handelen. De vraag voor hen is niet of volledige digitale soevereiniteit morgen haalbaar is, maar welke maatregelen vandaag nodig zijn om continuïteits-, vertrouwelijkheids- en controlerisico's bestuurlijk en operationeel beheersbaar te maken.

Dat handelingsperspectief ligt op drie niveaus. Strategisch gaat het om het verminderen van lock-in, het wegnemen van niet langer acceptabele afhankelijkheden en het organiseren van alternatieven. Tactisch gaat het om governance, toetsing, leverancierssturing, assurance en besluitvorming over restrisico's. Operationeel gaat het om toegangsbeheer, logging, encryptie, herstelvermogen, fallback en de praktische uitvoerbaarheid van exit- en continuïteitsmaatregelen.

In de rest van dit hoofdstuk werken we maatregelen uit op verschillende niveaus. Daarbij komen achtereenvolgens de volgende onderwerpen aan bod:

- **Strategische soevereiniteit:** het verminderen van lock-in, het vergroten van keuzevrijheid en het versterken van wendbaarheid.
- **Overheidsbeleid:** de rol van wetgeving, toezicht, transparantie en open standaarden bij het versterken van digitale weerbaarheid.
- **Risicobeheer en governance:** het expliciet meenemen van soevereiniteitsrisico's in governance, leverancierssturing en reguliere risicoprocessen.
- **Juridische en geopolitieke risico's:** aandacht voor rechtskeuze, lawfare, zeggenschapsrelaties en scenario's waarin juridische of geopolitieke omstandigheden veranderen.
- **Wendbaarheid en continuïteit:** exitstrategieën, vervangbaarheid, interoperabiliteit en herstelvermogen.
- **Operationele beheersing:** assurance, toegangsbeheer, logging, zero trust en andere maatregelen die de feitelijke grip op systemen en data versterken.
- **Verantwoordelijkheden van serviceproviders:** maatregelen om ongewenste beïnvloeding, management overrule en onrechtmatige beheeracties te voorkomen en aantoonbaar te beheersen.

INZET OP STRATEGISCHE SOEVEREINITEIT

In alle scenario's vraagt strategische soevereiniteit om structurele vermindering van lock-in, gebruik van open standaarden, stimulering van Europees aanbod en meer keuzemogelijkheden in de digitale markt. Dat is essentieel, maar biedt organisaties vandaag nog geen vrijbrief om bestaande afhankelijkheden te negeren. Juist daarom moeten kortetermijnmaatregelen expliciet en bestuurbaar worden gemaakt. Daarbij is er een ondersteunende taak voor de overheid en een praktische invulling voor organisaties.

OVERHEIDSBELEID

Zet ook voor soevereiniteitsrisico's in op de risk-based toepassing van wetgeving. Overheidsbeleid moet digitale soevereiniteit niet behandelen als een apart debatspoor naast bestaande weerbaarheidswetgeving, maar als een directe invulling daarvan. Nieuwe incidentgedreven verboden of ad-hocmaatregelen zijn minder effectief dan het consequent toepassen en aanscherpen van bestaande risk-based kaders. Dat vraagt vooral om expliciete normstelling, toezicht en handhaving.

Benoem soevereiniteitsrisico's expliciet in toezicht. Toezichthouders moeten soevereiniteitsrisico's expliciet binnen toezicht trekken. Het beheersen van afhankelijkheden, concentratie, rechtskeuze, fallback en operationele beheersing hoort geen vrijblijvende best practice te zijn, maar een toetsbaar onderdeel van reguliere IT-beheersing en weerbaarheid.

Bevorder transparantie over digitale afhankelijkheden. Overheden kunnen organisaties ondersteunen door meer transparantie te stimuleren over digitale afhankelijkheden, concentratierisico's en kritieke ketens. Organisaties kunnen risico's alleen effectief beheersen wanneer voldoende inzicht bestaat in onderliggende leveranciersrelaties, eigendomsstructuren, beheerketens en afhankelijkheden van kritieke diensten.

Bevorder interoperabiliteit en open standaarden Overheden kunnen digitale soevereiniteit tevens versterken door interoperabiliteit, open standaarden en portabiliteit actief te stimuleren. Deze vergroten de keuzevrijheid van organisaties, verminderen lock-in en maken het eenvoudiger om digitale diensten te vervangen wanneer risico's, marktomstandigheden of geopolitieke ontwikkelingen daartoe aanleiding geven.

RISICOBEHEER EN GOVERNANCE IN ORGANISATIES

Digitale afhankelijkheden zijn geen uitsluitend technisch vraagstuk meer. Bestuurders dragen verantwoordelijkheid voor de continuïteit van kritieke processen en moeten daarom expliciet inzicht hebben in de belangrijkste digitale afhankelijkheden van hun organisatie. Het identificeren, beoordelen en beheersen van soevereiniteitsrisico's behoort daarmee tot de reguliere bestuursverantwoordelijkheid.

Maak soevereiniteit onderdeel van risicobeheer. Voor organisaties geldt één hoofdregel: digitale soevereiniteit mag niet impliciet blijven. Bestuurders en interne toezichthouders moeten dit onderwerp expliciet opnemen in hun governance: in besluitvorming, risicobeheer en intern toezicht. Afhankelijkheden zonder inzicht, toetsing of exitstrategie zijn bestuurlijk onvolwassen en in kritieke ketens niet langer verdedigbaar.

Breng strategische afhankelijkheden expliciet in kaart. Bepaal welke keuzes snel schakelen verhinderen, waar concentratierisico's zitten, welke leveranciers of diensten single points of failure vormen en welke alternatieven werkelijk beschikbaar zijn.

Neem soevereiniteitsrisico's expliciet mee in BIV+P/CIA+P-classificatie en reguliere riskcycli. Daarmee worden analyse, periodieke herbeoordeling, mitigatie en verantwoording onderdeel van bestaande wettelijke en bestuurlijke kaders.

Maak de zeggenschapsroute expliciet in leverancierscriteria. Beoordeel niet alleen welke technische controls aanwezig zijn. Kijk ook naar eigendoms-, bestuurs-, personeels- en onderaannemersrelaties die in theorie een aangrijpingspunt kunnen vormen voor niet-EU-wetgeving of druk. Leg vast welk restrisico aanvaardbaar is en waar volledige uitsluiting proportioneel en noodzakelijk is. Zeggenschap over leveranciers en hun leveringsketen is niet statisch. Bewaking daarvan vraagt daarom om een doorlopend proces.

Voeg scenario- en faalwijzeanalyse toe aan risicobeheer. Organisaties moeten niet alleen vragen óf een verstoring waarschijnlijk is, maar vooral wat zij doen áls een kritieke leverancier, beheerroute, juridische waarborg of operationele keten faalt. FMEA kan daarbij een bruikbare methode zijn, maar in essentie gaat het om expliciete analyse van faalwijzen, gevolgen, detectie en herstelmaatregelen.

JURIDISCHE EN GEOPOLITIEKE RISICO'S

Maak expliciete of impliciete niet-EU-rechtskeuze in kritieke digitale ketens zichtbaar en behandel die als urgent risico. Voor kritieke processen is het niet verantwoord om afhankelijk te zijn van diensten waarbij EU-recht niet ondubbelzinnig leidend is.

Benoem lawfare en de verplichting om conflicterende opdrachten te weigeren. Benadruk wet- en regelgeving die expliciet benoemt dat organisaties en bestuurders opdrachten uit andere jurisdicties die strijdig zijn met EU-recht, contractuele verplichtingen of maatschappelijke continuïteit niet mogen uitvoeren. Maak ook duidelijk dat lawfare niet buiten de scope van digitale weerbaarheid valt, maar juist binnen de kern van bestuurlijke verantwoordelijkheid en interne beheersing.

WENDBAARHEID EN CONTINUÏTEIT

Organiseer wendbaarheid en exitvermogen. Organisaties die niet snel kunnen overschakelen bij onvoorziene juridische, operationele of geopolitieke verstoringen lopen disproportionele risico's. Wendbaarheid is daarom geen efficiëntiethema, maar een kernvoorwaarde voor continuïteit en bestuurlijke beheersing.

Exitstrategieën mogen daarbij niet uitsluitend op papier bestaan. Voor kritieke diensten moet periodiek worden getoetst of migratie, herstel of vervanging binnen acceptabele termijnen daadwerkelijk uitvoerbaar is. Een exitplan dat niet praktisch uitvoerbaar blijkt, biedt geen effectieve beheersing van afhankelijkheden.

Organisaties die niet snel kunnen overschakelen bij onvoorziene juridische, operationele of geopolitieke verstoringen lopen disproportionele risico's.

Gebruik open standaarden en ontkoppel waar mogelijk.
Wie afhankelijkheid wil verkleinen moet technische en organisatorische keuzes maken die vervangbaarheid bevorderen. Dat betekent: minder gesloten ecosystemen, meer portabiliteit, expliciete architectuurkeuzes voor uitwisselbaarheid en waar passend inzet op containerisatie of andere vormen van abstrahering van onderliggende platformen.

Technieken zoals containerisatie en orkestratie kunnen bijdragen aan sneller herstel en eenvoudiger verplaatsing van workloads tussen omgevingen. Ze zijn geen wondermiddel, maar wel een concreet voorbeeld van hoe architectuurkeuzes direct kunnen bijdragen aan tactische en operationele soevereiniteit.

Daarmee krijgt ook het strategische doel van wendbaarheid praktische inhoud: systemen worden zo ontworpen dat verstoringen opgevangen kunnen worden zonder dat kritieke diensten direct uitvallen of alleen via één leverancier herstelbaar zijn.

OPERATIONELE BEHEERSING

Hanteer waar mogelijk een zero-trustbenadering. Zero trust vertrekt vanuit het uitgangspunt dat toegang nergens impliciet wordt vertrouwd, maar telkens opnieuw wordt geverifieerd. Dat helpt om operationele soevereiniteit te versterken, omdat toegang, gebruik en beheer van gevoelige informatie nauwer en explicieter worden gecontroleerd.

Zero trust is niet overal volledig toepasbaar, zeker niet in bestaande omgevingen. Maar het principe blijft breed relevant: beperk impliciet vertrouwen, versleutel waar mogelijk, scheid bevoegdheden en houd sleutelbeheer, logging en toegangscontrole zo dicht mogelijk bij de eigen organisatie.

Waar het restrisico in externe ketens ondanks adequate maatregelen onaanvaardbaar blijft, kan verdergaande eigen beheersing nodig zijn. Ook dan geldt echter dat eigen beheer geen automatische garantie is voor veiligheid of continuïteit; het is alleen zinvol als de organisatie die beheersing ook daadwerkelijk kan waarmaken.

Vraag om aantoonbare werking van beheersmaatregelen. Certificeringen alleen zijn onvoldoende. Vraag, zeker in kritieke ketens, om assurance over feitelijke effectiviteit van controls, leveranciersbeheersing, logging, toegangsbeheer, continuïteitsmaatregelen en waar relevant expliciet ook over weerbaarheid tegen lawfare en management overrule.

Overweeg een beoordeling van de kwaliteit van de IT-beheersing. Juist hier is het van groot belang dat alle bij IT betrokken aspecten goed en evenwichtig vanaf de directietafel worden gemanaged, en goed bij interne toezichthouders op tafel komen. Het laten maken van een IDRS-rapportage kan hierbij helpen.

VERANTWOORDELIJKHEDEN VAN SERVICEPROVIDERS

Ook serviceproviders moeten explicieter worden. Zij zijn immers het onderwerp van eroderend vertrouwen als gevolg van soevereiniteitsrisico's. Wie actief is in kritieke digitale ketens moet meer doen dan compliant willen lijken. Zo'n aanbieder moet aantoonbaar maken hoe weerbaarheid tegen juridische druk of management overrule, admin-toegang, logging en escalatiepaden zijn ingericht. Diensten die dit niet inzichtelijk kunnen of willen maken, bieden onvoldoende basis voor vertrouwen.

Blokkeer door lawfare gemotiveerde pressie. Aanbieders met aandeelhouders, moedermaatschappijen of andere zeggenschapslijnen buiten de EU moeten expliciet maken hoe wordt voorkomen dat via inmenging of druk wordt gehandeld in strijd met wetten, regels en contracten in het land van levering. Dat vraagt om aantoonbaar beleid, heldere escalatieregels en verifieerbare controls.

Van aanbieders mag daarom worden verwacht dat zij vooraf duidelijk maken hoe zij omgaan met lawful-verzoeken, maar ook met lawfare-scenario's en conflicterende opdrachten, en dat zij de effectiviteit van hun maatregelen aantoonbaar laten toetsen.
Daarbij hoort ook dat niet alleen formele rechtmatigheid wordt beoordeeld, maar ook proportionaliteit, subsidiariteit en de verenigbaarheid van opdrachten met de rechtsorde en contractuele verplichtingen in de EU.

Blokkeer onrechtmatige opdrachten in de lijn. Aanbieders moeten besluitvormings- en beheerprocessen zo inrichten dat opdrachten die strijdig zijn met lokale wet- en regelgeving nooit eenzijdig of informeel kunnen worden afgedwongen. Het risico op management overrule en op uitvoering van dubieuze opdrachten buiten reguliere beheersing om moet worden uitgesloten. Daarbij kan tevens worden vastgelegd dat aandeelhouders en interne toezichthouders het management van de entiteit niet mogen vervangen door bestuurders of managers uit het land van de eigenaar.

Richt beheertoegang zodanig in dat onrechtmatige opdrachten expliciet worden uitgesloten. Voor hoog-risico handelingen kan worden gedacht aan streng gescheiden bevoegdheden, vier-ogen-principes, multi-party approval en technische beperkingen op admin-acties die direct tot uitval, gegevensverstrekking of onomkeerbare wijzigingen kunnen leiden.

Detecteer management overrule en sysadmin acties. Volledige logging en detectie van beheeracties, escalaties en afwijkingen zijn daarbij essentieel. Wat niet aantoonbaar zichtbaar is, is ook niet aantoonbaar beheerst.

6. Conclusies

Digitale soevereiniteit behoort voor organisaties geen abstract debat over geopolitiek te zijn, maar een direct vraagstuk van continuïteit, vertrouwelijkheid, bestuurlijke verantwoordelijkheid en operationele beheersing. Afhankelijkheden, concentratie, rechtskeuze en beperkte grip in digitale ketens zijn geen neutrale omstandigheden maar risico's die expliciet moeten worden gemaakt en actief moeten worden beheerst.

De kernboodschap van dit whitepaper is daarom eenvoudig: digitale soevereiniteit is een verdieping van beheersing van digitale risico's en organisaties mogen soevereiniteitsrisico's niet langer impliciet laten voortbestaan. Met andere woorden: impliciet vertrouwen dat iedereen in digitale ketens zich altijd aan contracten, afspraken, wetten en regels zal houden, is geen acceptabele basis meer voor compliance en beheersing. Het benoemen en beheersen van risico's op verstoring in ketens hoort thuis in reguliere governance, risicobeheer, leveranciersturing, assurance en toezicht.

Dat vraagt om drie dingen: minder afhankelijkheid van single points of failure, meer wendbaarheid en vervangbaarheid in digitale ketens, en meer feitelijke operationele grip op toegang, beheer, logging, herstel en escalatie. Bestuurders kunnen dit niet delegeren als louter IT-vraagstuk. Het is een kernonderdeel geworden van goed bestuur en van maatschappelijke weerbaarheid.

De discussie over digitale soevereiniteit gaat uiteindelijk niet over de vraag of volledige autonomie haalbaar is. Zij gaat over de vraag hoeveel afhankelijkheid organisaties bereid zijn te accepteren voor essentiële processen. Dat kan gaan om hun maatschappelijke taak, economische positie of publieke verantwoordelijkheid. Ook gaat het om de vraag hoe zij met onvermijdelijke afhankelijkheden omgaan.

Digitale soevereiniteit is daarmee geen doel op zichzelf. Het is een instrument voor weerbaarheid, bestuurbaarheid en vertrouwen. De uitdaging voor bestuurders is niet om alle afhankelijkheden uit te sluiten. Zij moeten bewust bepalen welke afhankelijkheden acceptabel zijn en welke niet. Dat vormt de basis voor duurzame digitale weerbaarheid.

We sluiten af met de OTC-kerngedachte: de digitale economie kan alleen goed functioneren als er voldoende vertrouwen is. De soevereiniteitskwestie laat zien dat beheersing van risico's meer dan ooit nodig is. Dat vraagt om heldere criteria, onafhankelijke controle en gerichte communicatie. Daarbij moet duidelijk worden in welke mate beheersing aantoonbaar is gerealiseerd en welke restrisico's van het werken met digitale technologie bewust worden aanvaard.

De digitale economie kan alleen goed functioneren als er voldoende vertrouwen is.

Bronnen

- EU. (2023). Verordening (EU) 2023/1543 betreffende Europese bevelen tot verstrekking en Europese bevelen tot bewaring van elektronisch bewijsmateriaal in strafprocedures. EUR-Lex.
- Europese Commissie. (2025). Cloud Sovereignty Framework.
- DICTU. (z.j.). Toetsingsinstrument Soevereiniteit Clouddiensten v1.0.1.
- FMEA. Failure mode and effects analysis - Wikipedia.
- Haven+. (z.j.). Haven+ overview / documentatie.
- Microsoft. (z.j.). Government Requests for Customer Data Report: Transparency reporting.
- NCSC Pas zero trust toe en bescherm je bedrijf.
- WRR / Wetenschappelijke Raad voor het Regeringsbeleid. (2020). Voorbereiden op digitale ontwrichting.
- Van de van der Schueren, M. (z.j.). Digitale soevereiniteit.
- Online Trust Coalitie. (2021). Vertrouwen in de cloud.
- Cyber Security Raad. (2025). Handreiking cybersecurity voor bestuurders en bedrijfseigenaren.

Colofon

Titel: Digitale Soevereiniteit - OTC 2026
Ondertitel: Een whitepaper over bestuurlijke, tactische en operationele digitale soevereiniteit
Versie / datum: 1 september 2026
Redactie: Online Trust Coalitie

Gebruik: Dit document is bedoeld als inhoudelijke verkenning en handelingsperspectief voor bestuurders, directies, interne toezichthouders en professionals die betrokken zijn bij digitale weerbaarheid, IT-governance, risicobeheer en leverancierssturing.

Disclaimer: Dit whitepaper biedt een bestuurlijke en praktische duiding van digitale soevereiniteit. Het document is niet bedoeld als juridisch advies. Organisaties blijven zelf verantwoordelijk voor hun eigen risicoanalyse, besluitvorming en naleving van toepasselijke wet- en regelgeving.