

Jouw data, jouw keuze

Praktische gids voor een autonome en soevereine IT



Inleiding

Wanneer een softwareleverancier ineens zijn gebruiksvoorwaarden of hostingbeleid wijzigt, kunnen de gevolgen groot zijn. Plotseling heb je geen toegang meer tot cruciale klantdata, of blijkt tijdens een audit dat gevoelige informatie is opgeslagen op servers die onder niet-Europese wetgeving vallen. Dit klinkt misschien als een uitzonderlijk scenario. Het is in werkelijkheid een risico dat veel organisaties lopen omdat ze simpelweg geen volledige controle hebben over hun data en de juridische kaders waarin die worden beheerd. Zolang je niet zelf bepaalt waar je data worden opgeslagen, wie er toegang toe heeft en onder welk juridisch regime dat gebeurt, loop je het gevaar de controle onbedoeld uit handen te geven.

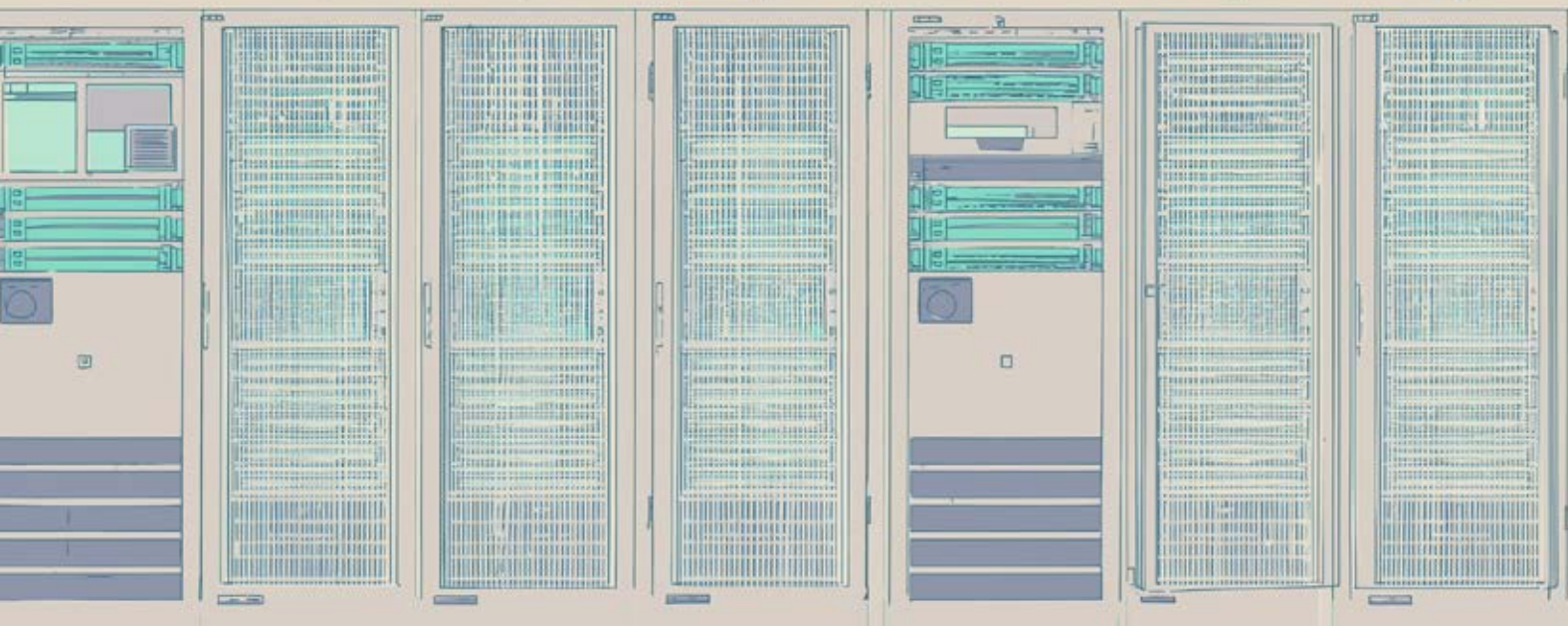
Digitale autonomie gaat niet alleen over waar data staan of wie ze host. Steeds meer organisaties, en ook de Europese Commissie, hanteren een bredere kijk. Dit zijn de drie lagen van controle die centraal staan:

- **Data-soevereiniteit:** zelf bepalen wie toegang heeft tot je data, waar die zich bevinden en onder welk juridisch regime ze vallen.
- **Infrastructuur-soevereiniteit:** controle over de fysieke en virtuele infrastructuur waarop je IT draait.
- **Technologische soevereiniteit:** autonomie over de technologieën, standaarden en software die je gebruikt.

In dit e-book laten we zien waarom autonomie geen abstract ideaal is, maar een strategische voorwaarde voor compliance, continuïteit en vertrouwen. Je ontdekt hoe je autonomie en soevereiniteit stap voor stap in balans brengt en hoe je dat vertaalt naar concrete keuzes in je datastrategie.

Wat je in dit e-book leest

- Wat digitale autonomie en soevereiniteit precies betekenen.
- Welke risico's en wetgeving daarbij komen kijken.
- Hoe je regie op je data behoudt.
- Hoe je met een hybride aanpak stappen kunt zetten richting digitale controle.



1. Wat is soevereine IT?

Van abstract begrip naar strategische noodzaak



De term 'soevereine IT' klinkt misschien abstract, maar gaat over iets heel concreets: zeggenschap over je digitale fundament. Dat betekent controle over je data, de infrastructuur waarop die draait én de software die je gebruikt. Het draait niet alleen om technologische keuzes, maar raakt aan compliance, leveranciersafhankelijkheid en het vermijden van vendor lock-in. Zonder die autonomie wordt het lastig om wendbaar te blijven in een speelveld waarin technologische en juridische kaders voortdurend veranderen.

In dit hoofdstuk duiken we dieper in de drie lagen van digitale autonomie: data-, infrastructuur- en technologische soevereiniteit. Wat houden ze precies in en waarom zijn ze essentieel voor organisaties die verantwoordelijkheid willen nemen over hun digitale toekomst?

1. Data-soevereiniteit

Data-soevereiniteit draait niet alleen om de fysieke locatie van data, maar vooral om grip en regie: wie mag er toegang toe krijgen, onder welke voorwaarden en binnen welk juridisch kader?

Het is een veelgehoorde aanname dat data die in Nederland of Europa zijn opgeslagen automatisch onder Nederlands of Europees recht vallen. In werkelijkheid spelen ook andere factoren mee zoals het land waarin je leverancier is gevestigd en de contractuele afspraken die je met die partij maakt. Daardoor is het mogelijk dat niet-Europese wetgeving van toepassing is, zelfs als de data nooit fysiek buiten de EU komen.

Initiatieven zoals EU Data Boundary van Microsoft, waarbij data worden verwerkt en opgeslagen binnen de EU, zijn een stap in de goede richting en bieden beleidsmatige garanties. Toch bieden ze niet altijd volledige juridische uitsluiting van buitenlandse claims. Het is daarom belangrijk om kritisch te blijven kijken naar de keuzes die je maakt op het gebied van dataverwerking, contracten en leveranciers, en om te zorgen dat die passen bij je eigen compliance-doelstellingen.

Impact op jouw business

Werk je met gevoelige klantdata of bedrijfskritische informatie? Dan is het cruciaal om stil te staan bij de juridische context waarin die data worden beheerd. Ook als data fysiek binnen de EU blijven, kan een leverancier die onder buitenlandse jurisdictie valt, toch wettelijk worden verplicht om gegevens te overhandigen aan buitenlandse autoriteiten. Zonder heldere afspraken over jurisdictie en toegang loop

je het risico dat je organisatie te maken krijgt met juridische claims of dataverzoeken die buiten het Europese rechtssysteem vallen. Dat raakt direct aan je compliance, reputatie én de continuïteit van je dienstverlening.

2. Infrastructuur-soevereiniteit

Digitale autonomie draait niet alleen om de locatie van je data, maar ook om de infrastructuur waarop je IT-omgeving draait. Wie beheert de netwerken, servers en virtuele lagen die jouw systemen in de lucht houden? En in hoeverre heb je daar zelf grip op?

Veel organisaties werken hiervoor samen met externe leveranciers. Dat is vaak efficiënt en soms onvermijdelijk, maar het betekent ook dat je afhankelijk bent van technologie, ondersteuning en beheer buiten je directe invloedssfeer. Denk aan firmware-updates, monitoring of beheer op afstand. Het zijn allemaal aspecten die invloed kunnen hebben op veiligheid, beschikbaarheid en compliance.

Infrastructuur-soevereiniteit vraagt daarom om inzicht in de keten. Om bewuste keuzes in leveranciers, architectuur en afspraken die passen bij je ambities en risicoprofiel.

Impact op jouw business

Zonder goed inzicht in de onderliggende infrastructuur kunnen er ongemerkt risico's ontstaan op het gebied van juridische verplichtingen, prestaties of compliance. Transparantie over hardware, netwerken en ondersteunende diensten helpt om tijdig bij te



"Wie beheert de netwerken, servers en virtuele lagen die jouw systemen in de lucht houden?"

sturen en grip te houden op databeveiliging en wet- en regelgeving.

3. Technologische soevereiniteit

Heb je als organisatie de vrijheid om je technologie zelfstandig te beheren, migreren, beveiligen en controleren? Of ben je afhankelijk van de kaders van één leverancier?

Echte technologische autonomie houdt in dat je zelf de encryptiesleutels beheert (BYOK/HYOK), toegang tot data en wijzigingen kunt loggen, én je data eenvoudig kunt exporteren of verwijderen in een open formaat. Werk je met een Trusted Execution Environment (TEE) waarbij je vertrouwt op een beveiligde verwerkingsomgeving, of ben je beperkt tot de standaardinterfaces van je IT-leverancier? De mate waarin je zelf zeggenschap hebt over je dataflows en verwerkingsprocessen bepaalt hoe wendbaar en toekomstbestendig je IT-landschap werkelijk is en hoe data-autonoom je daadwerkelijk bent.

Impact op jouw business

Beperkte technologische autonomie maakt het lastig om wendbaar te blijven. Zonder de mogelijkheid om zelfstandig te migreren, aanpassen of auditen, ben je sterk gebonden aan de keuzes van je leverancier. Dat kan innovatie vertragen, compliance bemoeilijken en ervoor zorgen dat je IT-landschap niet meegroeit met je strategische ambities.

Praktijktips

Evalueer je huidige infrastructuur

Breng in kaart welke delen van je IT-landschap je zelf beheert en waar je bent aangewezen op externe partijen. Kijk daarbij ook naar locatie, eigendom en toegang tot data.

Stel een soevereiniteitsprofiel op

Bepaal voor jouw organisatie welke datatypes strategisch, gevoelig of onderhevig zijn aan regelgeving, en leg vast welke eisen je stelt aan locatie, controle en compliance.

Formuleer beleidskaders

Stel richtlijnen op welke data en applicaties geschikt zijn voor de public cloud en welke thuishoren op Europese of eigen infrastructuur. Gebruik deze richtlijnen als kompas voor toekomstige keuzes.

Zet digitale autonomie op de strategische agenda

Betrek het bestuur en de directie bij het thema. Koppel autonomie aan thema's als risicobeheersing, digitale weerbaarheid en bedrijfscontinuïteit.

Maak het tastbaar met een eerste pilot

Start met één applicatie of datastroom en onderzoek hoe je die op een meer soevereine manier kunt inrichten. Denk aan alternatieve hosting, lokale opslag of aangepaste toegangsrechten. Gebruik de learnings voor het in kaart brengen van je gehele infrastructuur.



“Echte technologische autonomie houdt in dat je zelf de encryptiesleutels beheert”



2. Hoe beïnvloedt soevereiniteit jouw databeheer?

Zeggenschap over je IT begint bij hoe je data beheert. Wie toegang heeft, hoe gegevens worden opgeslagen, verwerkt, versleuteld en verwijderd: het zijn allemaal cruciale keuzes die bepalen in hoeverre je als organisatie controle houdt. Databeheer is dan ook geen puur technische aangelegenheid. Het raakt juridische, organisatorische en strategische aspecten van je bedrijfsvoering. In dit hoofdstuk verkennen we hoe digitale autonomie zich vertaalt naar concreet databeheer en waar je in de praktijk op moet letten.

Wetgeving en verantwoordelijkheden: Meer dan alleen GDPR

De wet stelt steeds hogere eisen aan hoe organisaties met data omgaan. De GDPR verplicht je al om precies aan te tonen waar data zich bevinden en hoe je die beschermt. Nieuwe regels zoals DORA, NIS2 en de AI Act gaan nog verder: ze leggen nadrukkelijk verantwoordelijkheden bij het bestuur en IT-management. Dat betekent dat organisaties niet langer kunnen volstaan met technische maatregelen alleen. Er moeten duidelijke strategieën worden ontwikkeld voor cybersecurity, datagovernance en operationele veerkracht. Zonder zo'n strategisch fundament wordt voldoen aan wetgeving niet alleen lastig, maar loopt je organisatie ook reëel risico op reputatieschade en boetes.

Zeker in internationale cloudomgevingen is juridische duidelijkheid essentieel. Niet alleen wáár data staan, maar ook met wie je samenwerkt en onder welke voorwaarden, bepaalt of je voldoet aan wet- en regelgeving. Wie het overzicht mist, loopt al snel kans op boetes of reputatieschade. Simpelweg omdat datastromen en verantwoordelijkheden niet helder zijn vastgelegd.

Wie mag wat en wanneer?

Toegang tot data is zelden eenduidig geregeld. Niet alleen externe leveranciers, maar ook interne afdelingen, partners of tijdelijke medewerkers kunnen toegang nodig hebben. Juist die variatie vraagt om fijnmazig toegangsbeheer, duidelijke rollen en realtime logging. Weet jij wie er toegang heeft tot welke gegevens en of dat nog actueel is? Zonder actief beheer verlies je niet alleen grip op je datastromen, maar loop je ook beveiligingsrisico's.

"Soeverein data-beheer gaat over inzicht, afweging en actie."

Het is zelden zwart-wit

In de praktijk werkt vrijwel niemand volledig soeverein of volledig buiten de EU. De meeste organisaties bevinden zich ergens in het midden: met data die deels in de public cloud staan, deels on-premises en deels bij Europese aanbieders. Juist daarom is het belangrijk om weloverwogen beslissingen te maken. Welke data bewaar je waar en waarom?

Soeverein databasebeheer gaat over inzicht, afweging en actie. Niet over alles afschermen, maar over gerichte controle houden. Jij bepaalt wat kritisch is, wat extern kan, en hoe je daarin wendbaar blijft.

Praktijktips

Voer een juridische risicoanalyse uit

Breng per leverancier en datalocatie in kaart onder welke jurisdictie jouw data vallen en controleer of dat in lijn is met je compliance-eisen.

Analyseer toegangsstructuren

Bekijk wie binnen en buiten je organisatie toegang heeft tot je data. Zorg voor duidelijke regels over wie toegang mag krijgen, onder welke voorwaarden en met welke registratie.

Definieer datalocatiebeleid

Leg vast waar verschillende soorten data idealiter worden opgeslagen (bijvoorbeeld binnen de EU) en toets leveranciers actief op deze eisen.

Werk realistische scenario's uit

Denk aan situaties als: "Wat als onze cloudprovider geen toegang meer geeft tot een kritieke dataset?" of "Wat als data plotseling onder een andere jurisdictie vallen?". Leg voor elk scenario vast wie wat doet, welke contractuele afspraken gelden en hoe je bedrijfscontinuïteit waarborgt.

Vergeet je netwerk niet

Als je controle wilt over je data, moet je ook grip houden op de routes waarlangs die data zich verplaatsen. Met een eigen glasvezelnetwerk of een beheerde verbinding bepaal jij zelf hoe gevoelige of bedrijfskritische datastromen lopen.

3. Internationale ontwikkelingen die je IT-keuzes beïnvloeden

Internationale cloudproviders, nieuwe Europese wetgeving en geopolitieke spanningen maken IT-keuzes complexer dan ooit. Het gaat allang niet meer alleen om kosten of prestaties, maar ook om compliance, continuïteit en zeggenschap.

1. Hyperscalers bieden regionale controle, maar geen volledige transparantie

Grote cloudaanbieders zoals Microsoft, AWS en Google bieden inmiddels soevereine clouddiensten aan: oplossingen waarbij data binnen een bepaalde regio blijven, met lokaal beheer en beperkte toegang. In theorie klinkt dat soeverein, maar in de praktijk zijn de garanties vaak minder sluitend.

Veel hyperscalers werken namelijk met een netwerk van subcontractors voor beheer, support en infrastructuur. Denk aan:

- Derde partijen die op afstand firmware beheren.
- Subverwerkers buiten de EU die toegang krijgen tot jouw omgeving.
- Supportteams die opereren vanuit landen met een andere juridische basis, zoals China of de VS.

Zonder volledig inzicht in deze keten kun je per ongeluk gevoelige data blootstellen aan buitenlandse wetgeving, zoals de Amerikaanse CLOUD Act. Hierbij kunnen de Verenigde Staten technologiebedrijven via een dagvaarding of bevelschrift dwingen gegevens van gebruikers te verstrekken. Ook als die op buitenlands grondgebied opgeslagen zijn. Daarnaast kunnen achterdeurtjes ontstaan in beheer- en updateprocessen, waardoor derde partijen alsnog toegang krijgen tot je gegevens.

Wat kun je doen?

Toets leveranciers op subverwerkers, logbeheer, toegangscontrole én datalocatie. Vraag om een volledig inzicht in de keten. Niet alleen op papier, maar ook operationeel.

2. Europese kaders helpen bij compliance

De EU biedt steeds meer handvatten om je infrastructuur juridisch, technisch en strategisch te onderbouwen.

Voorbeelden hiervan zijn:

- Het EU Cloud Services Scheme (EUCS) helpt bij het selecteren van veilige cloudleveranciers.
- GaiaX ontwikkelt interoperabele standaarden voor veilige datadeling in Europa. Eurofiber is als partner actief betrokken bij dit initiatief.

Deze kaders maken het opzetten van een compliance-by-design-architectuur gemakkelijker. Voorwaarde is wel dat je de juiste vragen stelt aan je leveranciers én dat je weet hoe je die standaarden vertaalt naar concrete keuzes.

3. Hybride IT is de standaard

Steeds meer organisaties kiezen ervoor om bedrijfskritische data niet (langer) toe te vertrouwen aan internationale cloudomgevingen. Lokale of Europese opslag wordt aantrekkelijker, mede dankzij:

- De groei van regionale datacenters.
- Open netwerken en vendor-neutrale infrastructuren.
- Lagere migratiebarrières door gestandaardiseerde APIs en dataservices.

Een hybride strategie, waarbij je workloads slim spreidt over meerdere omgevingen, is daarmee niet alleen realistischer geworden. Het is ook eenvoudiger te beheren en te beveiligen.

4. Ketenrisico's worden cruciaal door nieuwe regelgeving

Soms draait het niet om jouw systemen, maar om die van je leveranciers. Als die niet compliant of onvoldoende beveiligd zijn, beïnvloedt dat direct jouw risico's. Wetgeving zoals NIS2 en de aankomende CSRD scherpen dat bewustzijn aan:

- NIS2 verplicht organisaties in vitale sectoren tot het beheersen van ketenrisico's, inclusief rapportage over toeleveranciers.
- CSRD eist vanaf 2025 transparantie over duurzaamheid en governance, ook in je digitale processen.

Zonder keteninzicht en duidelijke afspraken kun je die verantwoordelijkheden simpelweg niet invullen.

5. Digitale autonomie wordt beleidsprioriteit

Van Brussel tot Den Haag groeit het besef dat Europa digitaal weerbaar moet worden. Niet alleen tegen cyberdreigingen, maar ook tegen economische afhankelijkheid. Overheidsprogramma's als Digital Decade en IPCEI-CIS investeren in een Europese infrastructuur waar openheid, controle en interoperabiliteit centraal staan.

Wat kun je verwachten? Toekomstige wetgeving gaat verder dan security of compliance alleen. Denk aan verplichte portabiliteit, strengere eisen aan auditbaarheid, en sancties voor niet-transparante ketens.

Praktijktips

Werk een hybride datastrategie uit

Analyseer welke applicaties je gebruikt en hoe de datastromen lopen. Bepaal vervolgens per workload welk type infrastructuur het beste past. Gebruik objectieve criteria zoals compliance-eisen, datakritikaliteit, latency of schaalbaarheid.

Leg leveranciers langs je soevereiniteitslat

Vraag leveranciers om transparantie over datalocatie, toegangsbeheer en compliance. Check of ze voldoen aan standaarden zoals EUCS of GaiaX en leg dit vast in je selectiecriteria.

Houd ketentransparantie structureel bij

Maak een overzicht van je digitale keten inclusief subleveranciers. Koppel dit aan je risicomanagement en governanceproces en actualiseer het minimaal één keer per jaar.

Ondersteun beleid met duidelijke kaders

Leg in je IT- en inkoopbeleid vast aan welke eisen leveranciers moeten voldoen op het gebied van autonomie, interoperabiliteit en repatriëring van data.

Test je exitstrategieën in de praktijk

Simuleer scenario's waarin je moet overstappen naar een andere leverancier of omgeving. Controleer of dataportabiliteit echt werkt en of je ketenverantwoordelijkheden helder blijven.

Contractuele borging met leveranciers

Leg in je SLA's en DPIA's vast waar data staan (datalocatie & jurisdictie), wie erbij kan (inclusief subverwerkers), wat er gebeurt bij exit (portabiliteit & verwijdering) en hoe je naleving controleert (auditrecht of toezicht).

Meer weten of direct aan de slag?

Eurofiber helpt je graag bij het opbouwen van een digitale infrastructuur die veilig, flexibel en toekomstgericht is. Neem vrijblijvend contact met ons op, we denken graag met je mee.

4. Eurofiber: het netwerk achter digitale autonomie



Wie écht grip wil op data en IT, moet beginnen bij de basis: de netwerkinfrastructuur. Want als je niet weet waar je data naartoe gaat, met wie het gedeeld wordt of onder welke wetgeving het valt, kun je ook geen bewuste keuzes maken. Een veilige, flexibele en transparante infrastructuur is daarom onmisbaar voor elke organisatie die inzet op digitale soevereiniteit. Eurofiber levert die basis, met open netwerken, regionale dekking en maximale keuzevrijheid.

1. Onafhankelijke infrastructuur als ruggengraat voor digitale autonomie

Autonomie vraagt om een infrastructuur die je kunt vertrouwen. Eurofiber combineert een vendor-neutraal glasvezelnetwerk met eigen datacenters en cloudoplossingen, zodat je altijd controle houdt over je digitale omgeving.

2. Eigen glasvezelnetwerk met open karakter

Eurofiber beheert een eigen open netwerk van meer dan 76.000 kilometer glasvezel in Nederland, België, Frankrijk en Duitsland. Dankzij de ondergrondse diepteligging van 60 centimeter biedt dit netwerk optimale veiligheid én maximale beschikbaarheid. Jij

bepaalt zelf welke cloudproviders, datacenters en IT-partners je aansluit. Zonder afhankelijkheid van één leverancier.

3. Krachtige combinatie van connectiviteit en colocation

Digitale autonomie vraagt om meer dan alleen een snelle verbinding of een fysieke serverlocatie. Eurofiber biedt een combinatie van hoogwaardige glasvezelconnectiviteit, eigen datacenters in Nederland en Frankrijk, én toegang tot meer dan 400 externe locaties via het DCspine-platform. Maar ook op het vlak van private cloud en maatwerkoplossingen biedt Eurofiber de bouwstenen voor een autonome IT-structuur.

Denk aan cloudopslag binnen de EU, private netwerken en hybride modellen waarbij je zélf bepaalt welke data lokaal, in een private cloud of juist in een publieke omgeving worden verwerkt. Zo houd je controle over je routes, je databeheer en bovenal: over de juridische context waarin je IT-omgeving opereert.

4. Netwerk als strategisch fundament onder compliance

In het streven naar digitale soevereiniteit is infrastructuur meer dan een technische randvoorwaarde. Het netwerk bepaalt:

- of je weet waar je data zijn;
- of je data kunt verplaatsen wanneer je wilt; en of dat gebeurt binnen Europese wet- en regelgeving.

Toch focussen veel organisaties nog te veel op software en te weinig op de onderliggende infrastructuur. Eurofiber helpt je om die compliance-eisen te vertalen naar een robuust en toekomstbestendig infrastructuurbeleid.

5. Flexibel, schaalbaar en juridisch transparant

Met Eurofiber's open netwerk behoud je keuzevrijheid, voorkom je lock-in en kun je IT-partners en diensten selecteren die passen bij jouw strategische en juridische kaders. Alle diensten worden geleverd onder duidelijke SLA's, met ondersteuning vanuit het Eurofiber Netwerk Monitoring Center en gegarandeerde hersteltermijnen van maximaal 8 uur (glasvezel) en 4 uur (actieve diensten).

6. Samen bouwen aan een soeverein digitaal Europa én aan jouw datastrategie

Digitale autonomie is niet alleen een strategisch doel van de Europese Unie, maar ook een praktische opgave voor iedere organisatie. Eurofiber werkt actief mee aan het versterken van digitale weerbaarheid

in Europa, met infrastructuur die keuzevrijheid, transparantie en interoperabiliteit centraal stelt. Als partner in initiatieven zoals GaiaX zet Eurofiber zich in voor open standaarden en eerlijke samenwerking tussen publieke en private partijen.

Maar dat is slechts de helft van het verhaal. Eurofiber biedt niet alleen de infrastructuur, maar ook de expertise om die op een echt autonome manier in te richten. Onze specialisten denken mee op alle drie de lagen van digitale autonomie: data, infrastructuur én technologie. We zijn een strategisch partner bij keuzes rondom datalocatie, het veilig repatriëren van data, of het vermijden van vendor lock-in.

We leveren geen generiek advies, maar maatwerk. Van private netwerken en cloudopslag tot hybride architecturen waarbij jij zelf de regie houdt over toegang, beheer en jurisdictie. Zo bouwen we samen aan een toekomstbestendige digitale omgeving. Europees waar nodig, maar bovenal: volledig onder jouw controle.

Praktijktips

Analyseer je netwerkstructuur met een expert

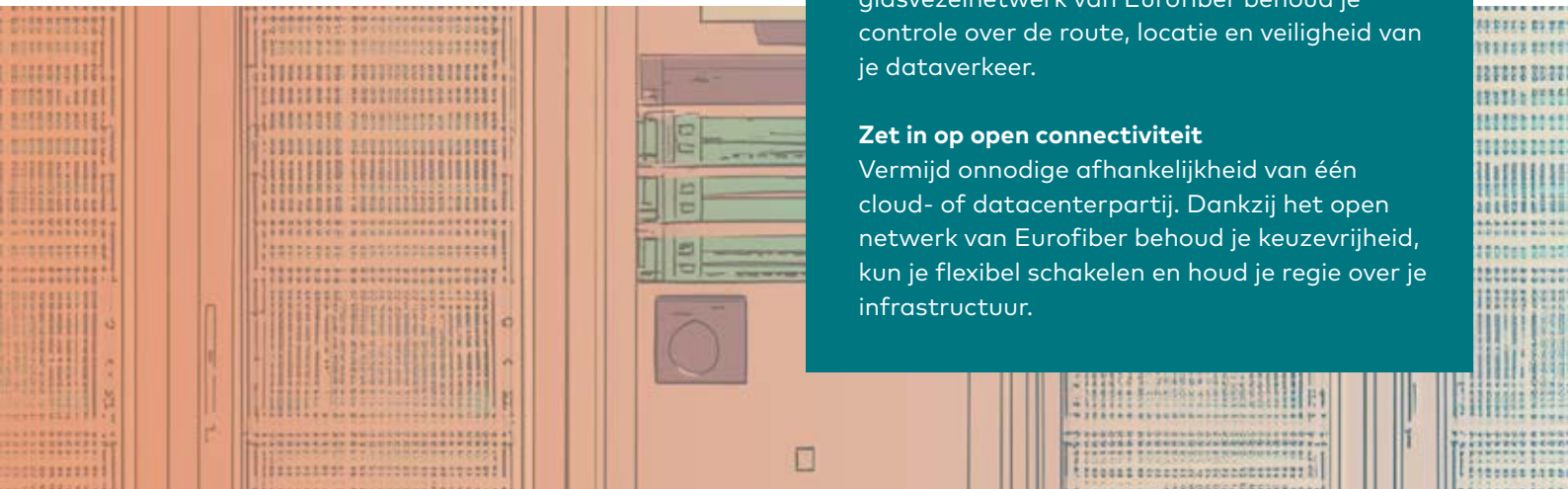
Laat doorlichten hoe jouw dataverkeer momenteel loopt, via welke knooppunten en welke risico's of afhankelijkheden dat oplevert. Eurofiber helpt bij het identificeren van optimalisatiekansen voor performance, compliance en wendbaarheid.

Verbind datastrategie met netwerk-architectuur

Zorg dat gevoelige of bedrijfskritische data worden verzonden via betrouwbare, transparante verbindingen. Met het glasvezelnetwerk van Eurofiber behoud je controle over de route, locatie en veiligheid van je dataverkeer.

Zet in op open connectiviteit

Vermijd onnodige afhankelijkheid van één cloud- of datacenterpartij. Dankzij het open netwerk van Eurofiber behoud je keuzevrijheid, kun je flexibel schakelen en houd je regie over je infrastructuur.





5. Conclusie

Je IT-omgeving is nooit af. Wet- en regelgeving veranderen, technologie ontwikkelt zich door en ook je eigen organisatie stelt voortdurend nieuwe eisen aan de infrastructuur en data. Daarom is digitale autonomie geen eindpunt, maar een manier van werken: je keuzes regelmatig heroverwegen, partners toetsen, beleid bijstellen.

Daarbij hoef je niet alles zelf te doen. Wel is het cruciaal dat je de juiste vragen stelt. Waar staan je data, en onder welk recht vallen ze? Is je infrastructuur flexibel genoeg om te blijven voldoen aan nieuwe regels? Wie die vragen kan beantwoorden, heeft een voorsprong.

Ben jij klaar om de volgende stap te zetten? Wil je verder praten over jouw datastrategie, netwerkarchitectuur of compliance-aanpak? Eurofiber helpt je graag verder. Neem contact met ons op, we denken graag met je mee.



Colofon

Meer weten?

Heb je vragen of wil je liever persoonlijke advies?
Neem dan [contact](#) op.

Eurofiber Nederland

Safariweg 25-31
3605 MA Maarssen
T +31 (0)30 242 87 00

