

Visiepaper Kenniscentrum Data & Maatschappij

Digitale Soevereiniteit als richting voor een veerkrachtige onderneming

Verklarende woordenlijst



Adequaatheidsbesluit Een beslissing van de Europese Commissie die vaststelt dat een land buiten de EU een “passend beschermingsniveau” biedt voor persoonsgegevens, waardoor data naar dat land mag stromen.

Air-gapped Volledig afgesloten van het internet of andere netwerken, zodat een systeem fysiek geïsoleerd is en niet extern benaderbaar is.

AI Factories Europese/Vlaamse initiatieven die rekenkracht (zie *compute*) ter beschikking stellen om AI-modellen te trainen en te gebruiken, als alternatief voor buitenlandse cloud-GPU's.

AVG (Algemene Verordening Gegevensbescherming) De Europese privacywet (ook bekend als GDPR) die regelt hoe organisaties persoonsgegevens mogen verzamelen, bewaren en verwerken.

Broligarchy Informele term voor de groep invloedrijke Amerikaanse techmiljardairs met nauwe banden tot de Amerikaanse politiek.

CLOUD Act Amerikaanse wet die Amerikaanse politie- en veiligheidsdiensten toelaat om data op te vragen bij bedrijven onder Amerikaans recht, ook als die data op servers in Europa staat.

Compute (rekenkracht) De reken- en verwerkingscapaciteit die nodig is om AI-modellen te trainen en te gebruiken.

Data Act Europese verordening met regels over eerlijke toegang tot en overdracht van data.

Dataportabiliteit Het gemakkelijk kunnen overzetten van je data naar een andere leverancier.

Datasoevereiniteit De keuze voor je cloudserver en -leverancier, en de bijhorende voorwaarden voor opslag en (her)gebruik van je data – een deelaspect van het bredere begrip digitale soevereiniteit.

De-skilling Het verlies van interne technische capaciteit binnen een organisatie doordat taken (zoals serveronderhoud) uitbesteed worden aan externe leveranciers.

Digital Commons (EDIC) Een gedeelde, gemeenschappelijke digitale infrastructuur van meerdere Europese lidstaten, gebouwd op opensourcesoftware, open standaarden en open data.

Digitalemarktenverordening (DMA) Europese wet die regels uitschrijft voor een eerlijke en concurrerende digitale markt, en bepaalde marktpraktijken van grote techbedrijven ("poortwachters") moet tegengaan.

Digitaledienstenverordening (DSA) Europese wet die regels stelt aan online platformen, bijvoorbeeld rond illegale inhoud, transparantie en verslavend ontwerp.

Egress fees (overstapkosten) Kosten die een leverancier aanrekent om data uit zijn platform te halen en naar een andere leverancier te verplaatsen.

Executive Order 14086 Een Amerikaans presidentieel besluit dat de juridische basis vormt voor het EU-VS Data Privacy Framework.

FISA (Foreign Intelligence Surveillance Act) Amerikaanse wet die het kader vormt voor buitenlandse inlichtingensurveillance door de VS.

FOSS (Free and Open Source Software) / vrije en opensourcesoftware Software waarvan de broncode vrij bekeken en aangepast kan worden. Vrije software volgt daarbij de "vier vrijheden": gebruiken, bestuderen/aanpassen, delen en verspreiden.

Frontier AI Verzamelnaam voor de meest geavanceerde, best presterende AI-modellen.

GAFAM Afkorting voor Google, Apple, Facebook, Amazon en Microsoft – de grote Amerikaanse techbedrijven.

Inferentiedata De data die een AI-model verwerkt op het moment dat het gebruikt wordt (in tegenstelling tot trainingsdata).

Interoperabiliteit De mate waarin systemen of software met elkaar en met andere toepassingen kunnen samenwerken en data uitwisselen.

Kill switch Een verborgen mechanisme waarmee een apparaat of systeem op afstand kan worden uitgeschakeld.

NIS2-richtlijn Europese richtlijn die organisaties in essentiële en belangrijke sectoren verplicht om maatregelen te nemen voor risicobeheer van hun netwerk- en informatiesystemen (cybersecurity-eisen).

One throat to choke Uitdrukking voor het voordeel van één verantwoordelijke leverancier aanspreken bij problemen, in plaats van meerdere leveranciers.

Open Strategische Autonomie Het EU-beleidsprincipe (sinds 2016) om overal en altijd autonoom te kunnen handelen met gelijkgezinde partners, volgens eigen waarden en belangen – de bredere beleidscontext waaruit digitale soevereiniteit voortkomt.

Percelen (aanbesteding in percelen) Het opdelen van een overheidsopdracht in kleinere, afzonderlijke deelopdrachten (bv. hosting, onderhoud, support apart), wat kleinere aanbieders meer kans geeft.

Propriëtaire software / propriëtaire standaarden Software of technische standaarden waarvan de broncode niet vrij beschikbaar is en waarvoor bindende gebruiksregels gelden (tegenovergestelde van open source).

SaaS (Software as a Service) Een model waarbij een gebruiker een licentie op software afneemt via het internet, in plaats van de software zelf te installeren en beheren.

Single point of failure Eén onderdeel van een systeem waarvan alles afhangt: valt dit uit, dan valt de hele organisatie of dienst stil.

Sovereignty washing Een clouddienst of technologie “soeverein” noemen zonder dat deze werkelijk aan de vereiste soevereiniteitscriteria voldoet.

Status quo bias De neiging van organisaties of mensen om verandering te vermijden en vast te houden aan de bestaande situatie.

Sunk cost fallacy De neiging om vast te houden aan eerdere investeringen of keuzes, ook als een verandering objectief voordeliger zou zijn.

Telemetry Het automatisch doorsturen van gebruiksdata door een digitale toepassing naar de producent of andere partijen.

Too big to regulate Uitdrukking voor grote techbedrijven die zo machtig zijn dat regelgeving moeilijk af te dwingen valt.

Trainingsdata De data waarmee een AI-model ontwikkeld en “getraind” wordt.

Vendor lock-in De situatie waarin een organisatie zo afhankelijk wordt van één leverancier dat overstappen naar een andere leverancier moeilijk of duur wordt.

Inhoud

	Verklarende woordenlijst	→ 2
1	Inleiding	→ 6
2	Wat is digitale soevereiniteit?	→ 7
3	Waarom is digitale soevereiniteit belangrijk?	→ 8
	3.1 Geopolitiek	→ 9
	3.2 Economie	→ 11
	3.3 Flexibiliteit en veerkracht	→ 12
	3.4 Cybersecurity	→ 13
	3.5 Databeheer en -veiligheid	→ 14
	3.6 Mensenrechten	→ 16
4	Hoe kwam digitale soevereiniteit op de (politieke) voorgrond in Europa?	→ 17
5	Maakt Europa nu de omslag?	→ 20
6	Vaak gestelde vragen over digitale soevereiniteit	→ 23
7	Visie en Aanbevelingen	→ 27
8	Addendum	→ 31
	8.1 Verdiepend: Soevereiniteit in cyberspace?	→ 31
	8.2 Verdiepend: Vrije en opensourcesoftware, en digitale soevereiniteit	→ 32
9	Bronnenlijst	→ 34

¹ 'Life without US tech,' The Big Read Technology Sector 11 May 2026: https://www.ft.com/content/4c3aad70-e0cb-46a2-95d5-15d11b6bf818?accessToken=zWAAAZ4btMHkc9MOq1w4MtGotOV1RXRG2v4GA.MEUCIBZdUjV-5o32TCmhxNupummvRy/YAE4rq6ZEMBj78rs_AiEApl5GAgh9yaZLFwdEQ-6ZiVo_3JD7W_WYtndeaY6-aAw&sharetype=gift&token=44588b15-7506-4d5d-98c7-bb8038aafb83&syn-25a6b1a6=1

² E. Bruford et al. (2020). Guidelines for human gene nomenclature. Nature Genetics 52: 754–758.

³ Gebaseerd op een prompt aan Microsoft Copilot voor een mediaonderzoek op Nederlandstalige, Engels en Franse nieuwsartikelen. Het aantal steeg van ongeveer 210 vermeldingen in het eerste kwartaal van 2024 naar ongeveer 720 in het eerste kwartaal van 2026.

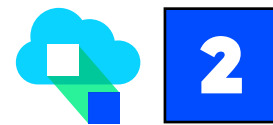
⁴ Doordat de term 'digitale soevereiniteit' alsnak vaker wordt gebruikt, merken we ook vaker tegenstrijdigheden in hoe de term in verschillende registers wordt gebruikt. Zie: S. Repetto (2025). 'Concept 'Stretching' or Concept Innovation? A Review of the Usages of Sovereignty in the Digital Sovereignty Literature,' Policy & Internet: <https://onlinelibrary.wiley.com/doi/full/10.1002/poi.3.70011>

Probeer eens een werkdag voor te stellen zonder Google, Microsoft of ChatGPT? Kan je eigenlijk nog werken? De impact van deze techgiganten op ons dagelijks leven is onmiskenbaar, ook waar je het niet meteen zou verwachten.¹ Wist je, bijvoorbeeld, dat in 2020 de HUGO Gene Nomenclature Committee (HGNC) de richtlijnen wijzigde voor het benoemen van genen omwille van Microsoft Excel? De reden: sommige genen werden (frustrerend vaak) als een opdracht of datum geïnterpreteerd!²

Tegelijk komt er alsnak meer kritiek op de grote Amerikaanse techbedrijven. Diverse bezorgdheden spelen een rol, zoals geopolitieke spanningen, monopolievorming en te grote afhankelijkheid van een bepaalde leverancier (*vendor lock-in*), privacy-issues (bijvoorbeeld door conflicterende wetgevingen) en de lijst gaat door. Het antwoord op deze bezorgdheden komt meestal in twee woorden: digitale soevereiniteit. Dit alomtegenwoordig begrip – het werd in het eerste kwartaal van 2026 drie keer zo vaak gebruikt in nieuwsartikelen vergeleken met het eerste kwartaal van 2024³ – wordt hier verduidelijkt.⁴ Na het lezen van deze tekst heb je een antwoord op de volgende vragen:

- Wat betekent digitale soevereiniteit?
- Waarom is digitale soevereiniteit belangrijk; of: waarom zijn sommige digitale afhankelijkheden problematisch?
- Welke (politieke) evoluties hebben zich afgespeeld rond digitale soevereiniteit?
- Wat zijn vaak gehoorde vragen over digitale soevereiniteit?
- Wat zijn de aanbevelingen van het Kenniscentrum Data & Maatschappij rond digitale soevereiniteit?

Wat is digitale soevereiniteit?



⁵ Er bestaat heel wat onduidelijkheid over de exacte definitie van soevereiniteit. Zie: S. Couture & S. Toupin (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media & Society 21; 2305–2322.

⁶ Deze "iemand" kan op vele wijzen ingevuld worden: het kan gaan over nationale staten, over kleine en grote marktspelers, maar ook over individuen. Zie: J. Pohle & T. Thiel (2020), 'Digital sovereignty', Internet Policy Review, 9(4).

⁷ Europese Unie (2022). Declaration for European Digital Sovereignty. Brussels. Hier beschikbaar: [Declaration for European Digital Sovereignty](#)

⁸ S. Fratini et al. (2024), 'Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models,' Digital Society 3: 1–27. Zie ook: K. O'Hara & W. Hall (2018). Four Internets: The Geopolitics of Digital Governance. Hier beschikbaar: <https://www.cigionline.org/static/documents/documents/Paper%20no.206web.pdf> J. Pohle et al. (2024), 'Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices,' Policy & Internet 16: 666–671.

⁹ F. Burwell & K. Propp (2026), 'Digital sovereignty: Europe's declaration of independence?' Atlantic Council 14 januari 2026: <https://www.atlanticcouncil.org/in-depth-research-reports/report/digital-sovereignty-europes-declaration-of-independence/>; D. Di Marco et al. (2023). Open but not powerless: Towards a common understanding of EU Digital Sovereignty. Publications Office of the European Union. JRC open but not powerless: towards a common understanding of EU Digital Sovereignty

Digitale soevereiniteit gaat over zelfbepaling in het digitale domein; het is **het vermogen om controle te hebben en houden over data en digitale technologieën**.⁵ Deze controle laat iemand⁶ toe om niet alleen digitale technologie volgens de eigen belangen en waarden te gebruiken, maar ook veerkrachtig om te gaan met (plotse) technologische, economische of geopolitieke schokken.⁷ Deze definitie kan je zien als een Europese interpretatie van digitale soevereiniteit, eentje die schippert tussen andere interpretaties, zoals het Amerikaanse model dat focust op de overmacht van nationale marktspelers en het Chinese of Russische model waarbij de voornaamste controle bij de staat ligt.⁸

Digitale soevereiniteit is **een breder verhaal** dan enkel datasoevereiniteit. Datasoevereiniteit gaat over de keuze voor jouw cloudserver en -leverancier, en de daarbij horende voorwaarden voor de opslag en (her)gebruik van jouw data. Digitale soevereiniteit gaat daarnaast ook over:

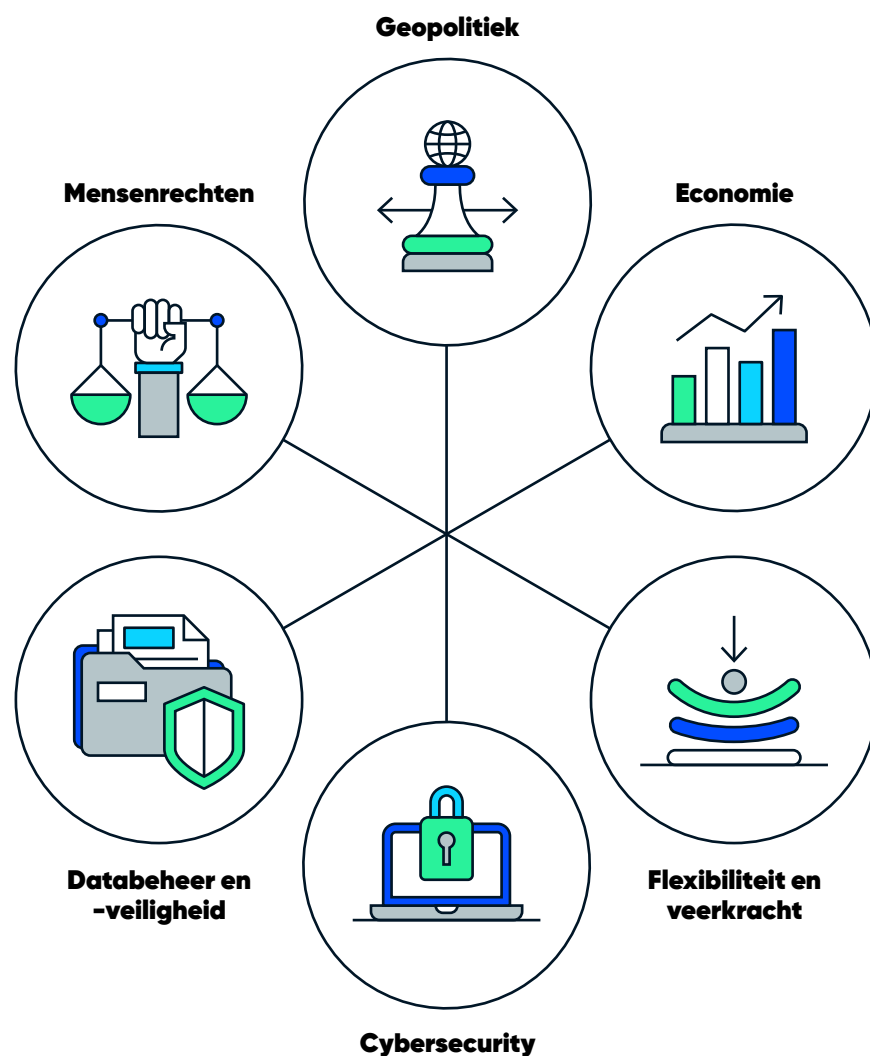
- De mogelijkheid om digitale technologieën volgens de eigen normen, waarden en regels in te zetten.
- Eigenaarschap van digitale toepassingen om deze maximaal aan jouw concrete, lokale noden aan te passen en zo technologisch te innoveren naar eigen inzicht.
- Het opbouwen van menselijk kapitaal om niet afhankelijk te (moeten) zijn voor het beheer en onderhoud van jouw digitale toepassingen.
- De eigen controle over de cyberveiligheid van jouw digitale toepassingen, en dus geen kwetsbaarheden bij contractpartijen te hoeven dulden.⁹

Deze digitale soevereiniteit uit zich in een complex kluwen van digitale infrastructuur, software en menselijk kapitaal. Het gaat over keuzes van leveranciers (of om iets zelf te bouwen), de voorwaarden die horen bij die leveranciers en de regelgeving waaronder een leverancier valt. Sommige keuzes staan garant voor meer flexibiliteit en eigenaarschap, maar kunnen samengaan met minder gebruiksgemak (bijvoorbeeld door een beperkte integratie met andere toepassingen) of een hogere kostprijs. Daarom weeg je soevereiniteit niet af in een vacuüm, maar samen met alle relevante factoren.

Waarom is digitale soevereiniteit belangrijk?



Organisaties kunnen uiteenlopende redenen hebben om meer controle over hun data en digitale technologieën te willen verkrijgen of behouden. Hieronder lijsten we de zes meest voorkomende redenen op.





¹⁰ '8 in 10 Europeans don't trust US, Chinese firms with data,' Politico 10 april 2026; <https://www.politico.eu/article/8-in-10-europeans-dont-trust-us-chinese-firms-with-data/#:~:text=The%20European%20Pulse%20survey%20was,includin%20age%2C%20gender%20and%20geography>

¹¹ Synergy Research Group (2026), 'Cloud Market Share Q1 2026: AWS, Microsoft, Google Battling In AI Era.' Hier beschikbaar: <https://www.crn.com/news/cloud/2026/cloud-market-share-q1-2026-aws-microsoft-google-battling-in-ai-era>

¹² Resonate (2026), 'HubSpot Market Share 2026: CRM Share, Revenue & Customers.' Hier beschikbaar: <https://www.resonatehq.com/blog/hubspot-market-share>

¹³ Datanyze (2026), 'Office Suites Software Market Share.' Hier beschikbaar: <https://www.datanyze.com/market-share/office-suites--370>

¹⁴ Market.us Scoop (2026), 'Video Conferencing Statistics By Connecting Technology (2026).' Hier beschikbaar: <https://scoop.market.us/video-conferencing-statistics/>

Geopolitieke spanningen zorgen voor een verminderd vertrouwen in bedrijven uit China of de Verenigde Staten. Zo wantrouwen respectievelijk 93% en 87% van de Belgen technologiebedrijven uit China en de Verenigde Staten.¹⁰ Dit heeft er deels mee te maken dat technologie ingezet kan worden in geopolitieke conflicten. Dit zien we vooral met betrekking tot sommige Amerikaanse techbedrijven (de zogenaamde hyperscalers), vooral omdat hun wereldwijd marktaandeel zeer groot is. Zij zetten de toon voor clouddiensten en andere digitale technologieën:

- Tweederde van clouddiensten wereldwijd worden geleverd door Amazon (AWS), Microsoft (Azure) en Google (GCP).¹¹
- Meer dan de helft van tools voor Human Resource Management (HRM) worden wereldwijd geleverd door Amerikaanse bedrijven zoals Salesforce, Adobe en Hubspot; het Duitse SAP bedient ongeveer 6% van de markt.¹²
- Meer dan 90% van de wereldwijde markt voor productiviteitssuites (zoals Microsoft Office) worden geleverd door Microsoft en Google.¹³
- Zo'n tweederde van de wereldwijde markt voor digitale communicatiemiddelen wordt bediend door Zoom, Microsoft en Google.¹⁴

¹⁵ A. Michelotti (2025), 'Concentration of Power in the Broligarch Era,' Tech Policy Press: <https://www.techpolicy.press/concentration-of-power-in-the-broligarch-era/>

¹⁶ Microsoft benadrukt dat er geen kwaad opzet was, maar dat de maatregel genomen werd als een geautomatiseerde cybeveiligingsactie omdat het Strafhof slachtoffer was van cyberaanvallen. Toch communiceerde Microsoft hierna over een serie van Europese of 'soevereine' maatregelen zodat Europese klanten vertrouwen kunnen hebben in de continuïteit van de dienst. 'Microsoft expands its Sovereign Cloud as Europe demands greater data control,' Windows Central News 17 juni 2025: <https://www.windowscentral.com/microsoft/microsoft-expands-its-sovereign-cloud-as-europe-demands-greater-data-control>

¹⁷ She Spoke Out About Gaza. Now She Can't Use a Credit Card,' Politico 30 maart 2026: <https://www.politico.com/news/magazine/2026/03/30/gaza-israel-un-criticize-us-sanction-00850477>

¹⁸ 'Statement on the US government directive to suspend access to Fable 5 and Mythos 5,' Anthropic website 12 juni 2026: <https://www.anthropic.com/news/fable-mythos-access>

¹⁹ SpaceX curbed Ukraine's use of Starlink internet for drones -company president,' Reuters 9 februari 2023: <https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09/>. Zie ook: B. Gur (2024), 'Resilient Connectivity: SpaceX's Stellar Solution for Gaza's Internet Amid Conflict.' Hier beschikbaar: <https://directionsblog.eu/resilient-connectivity-spacexs-stellar-solution-for-gazas-internet-amid-conflict/>

Binnen Europa is het marktaandeel van Europese aanbieders relatief groter, maar – met uitzondering van HRM-tools – blijft het marktoverwicht van Amerikaanse techbedrijven. Dit overwicht wordt alsmaar vaker ervaren als problematisch omdat deze bedrijven een nauwe band hebben met de (administratie van de) Amerikaanse president Donald Trump, of de zogenaamde *broligarchy*.¹⁵ Hierdoor kunnen deze bedrijven ingezet worden in politieke conflicten. Bijvoorbeeld:

- De voormalige hoofdaanklager en andere medewerkers van het Internationaal Strafhof konden plots niet meer hun Microsoft e-mail gebruiken. Dat gebeurde nadat onderzoek was begonnen naar bepaalde Israëlische politici.¹⁶
- VN-Speciale rapporteur voor de mensenrechten in de Palestijnse gebieden Francesca Albanese kon plots niet langer gebruik maken van haar kredietkaart.¹⁷
- De Amerikaanse president Donald Trump kondigde exportverboden aan voor bepaalde AI-modellen van het Amerikaanse bedrijf Anthropic. Deze zouden de nationale veiligheid in het gevaar brengen.¹⁸
- Het internetsatellietnetwerk *Starlink* is essentieel voor de Oekraïense strijdmachten, maar de beschikbaarheid ervan is sterk afhankelijk van de *goodwill* van SpaceX en de Amerikaanse administratie.¹⁹



²⁰ Europese Commissie: Directorate-General for Research and Innovation (2025), *Open for startups & scaleups – EU startup and scaleup strategy making Europe a startup powerhouse*. Publications Office of the European Union: <https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/86a3cca9-4023-11f0-b9f2-01aa75ed71a1/language-en>

²¹ European Investment Bank (2024). *The scale-up gap Financial market constraints holding back innovative firms in the European Union*. Hier beschikbaar: <https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/86a3cca9-4023-11f0-b9f2-01aa75ed71a1/language-en>

²² Zie: <https://www.vlaio.be/nl/begeleiding-advies/digitalisering/artificiele-intelligentie/advies-begeleiding-en-financiele-steun/financiele-steun-voor>

²³ OECD (2022), *OECD Handbook on Competition Policy in the Digital Age*, <https://www.oecd.org/daf/competition-policy-in-the-digital-age>

Het bovenvermelde overzicht van Amerikaanse bedrijven en technologie levert de Europese economie een globaal concurrentieel nadeel op. Europa is sterk in fundamenteel onderzoek en heeft een groot aandeel aan start-ups in nieuwe digitale technologieën, maar wanneer deze opschalen, verhuizen ze vaak naar het buitenland.²⁰ Zo zit slechts 8% van de wereldwijde scale-ups in Europa.²¹ In reactie hierop wil Europa bedrijven ondersteunen met investeringsprogramma's om eigen technologieën te ontwikkelen, zoals Europese Cloud (e.g. SAP Cloud) of Europese AI (e.g. de AI Factories). Dergelijke programma's zijn er ook in Vlaanderen via VLAIO en bedrijven kunnen gebruik maken van lokale *European Digital Innovation Hubs* (EDIHs), zoals [Flanders.AI](#) of [sustAI.n.Brussels](#), voor ondersteuning.²² Zo kan het economisch voordelig zijn om in te zetten op lokale, Europese digitale technologieën omdat deze van lokale ondersteuning kunnen genieten. Een meer diverse markt – met realistische Europese alternatieven – heeft ook een positieve uitwerking op kostenbeheersing. Zo kunnen bedrijven en overheden zich beter wapenen tegen stijgende licentiekosten door een sterkere onderhandelingsmacht.²³

Flexibiliteit en veerkracht



²⁴ "The Invisible Cage: How Cloud Vendor Lock-In Threatens European Digital Sovereignty," *Sovereign Sky* blog z.d.: https://www.sovereign-sky.net/vendor-lock-in?utm_source=copilot.com

²⁵ Art. 29 van Verordening (EU) 2023/2854 van het Europees Parlement en de Raad van 13 december 2023 betreffende geharmoniseerde regels inzake een eerlijke toegang tot en gebruik van data (Data Act), Pb.L. 2023, L 2854.

²⁶ I. Vignoli (z.d.), *FOSS and Open Standards for Digital Sovereignty*. Hier beschikbaar: <https://www.scribd.com/document/489531856/FOSS-and-Open-Standards-for-Digital-Sovereignty>

²⁷ Kenniscentrum Data & Maatschappij (2026), 'Data Act: Vijf vragen die elke onderneming zich moet stellen.' Hier beschikbaar: https://data-en-maatschappij.ai/uploads/Data-Act_5_vragen_KDM.pdf

²⁸ F. Mbuba et al. (2014), 'Software as a Service Adoption: Impact on IT Workers and Functions of IT Department Software as a Service Adoption: Impact on IT Workers and Functions of IT Department,' *Journal of Internet Technology* 15: 103-114; R.-K. Penttinen, et al (2023). 'The Vicious Circles of Skill Erosion: A Case Study of Cognitive Automation,' *Journal of the Association for Information Systems* 24: 1378-1412.

Door vooral gebruik te maken van één of enkele leveranciers van digitale technologieën, wordt een organisatie minder flexibel en veerkrachtig. Zo is men minder in staat om plotse veranderingen te verdragen, zoals geopolitieke, technologische of economische schokken. Dit heeft te maken met:

- **Vendor Lock-In.** Hoe meer diensten je bij één leverancier afneemt, hoe groter de afhankelijkheid van die partij. Daardoor wordt het steeds moeilijker om van leverancier te veranderen, zelfs wanneer dat voordeliger zou zijn.²⁴ Soms worden ook bepaalde overstapkosten aangerekend ('egress fees') om data uit een cloudplatform te halen en naar een andere leverancier te verplaatsen (deze overstapkosten zouden binnenkort, dankzij de *Data Act*, moeten verdwijnen)²⁵.
- **Propriëtaire standaarden.** Sommige aanbieders van digitale diensten leveren hun software als een dienst (SaaS), waarbij een afnemer een licentie op een bepaalde softwaredienst via het internet afneemt. Hierdoor heb je slechts beperkt zeggenschap over hoe de dienst werkt, hoe je data wordt opgeslagen, gestructureerd of soms zelfs uitgewisseld. Dit maakt dat de data van de organisatie minder herbruikbaar zijn, veranderen van aanbieder moeilijker is en de toegankelijkheid van data op langere termijn niet gegarandeerd is.²⁶ Dit bemoeilijkt compliance met bepaalde Europese regels, zoals de *Data Act*.²⁷
- **De-skilling.** Sterke afhankelijkheden van externe aanbieders van in het bijzonder SaaS-diensten zorgen voor herschikkingen in de eigen interne IT-diensten. Omdat heel wat aspecten van softwarebeheer (zoals serveronderhoud, updates, troubleshooting, etc.) uitbesteed worden, zien we in deze context ook een verlies aan interne capaciteit. Zo verlies je als organisatie de capaciteit om zelf problemen op te lossen of flexibel om te gaan met nieuwe technologieën.²⁸

Cybersecurity



²⁹ 'Iran Targets Big Tech, Expands War Beyond Battlefields,' *Analytics Insight* 1 april 2026: <https://www.analyticsinsight.net/news/iran-targets-big-tech-expands-war-beyond-battlefields>

³⁰ Insikt Group (2025), 'H1 2025 Malware and Vulnerability Trends.' Beschikbaar hier: <https://assets.recordedfuture.com/insikt-report-pdfs/2025/cta-2025-0828.pdf>

³¹ Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn). Deze richtlijn is in België omgezet via de De wet van 26 april 2024 Wet tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid ('wet NIS2').

Grote techbedrijven hebben meestal de grootste capaciteit om in te zetten op cyberveiligheid en kunnen zich het best wapenen tegen DDoS-aanvallen, *data breaches* en ransomware. Tegelijk zijn deze bedrijven ook het vaakst doelwit van cyberaanvallen, deels omdat ze aanzien worden als bondgenoten van de Amerikaanse staat.²⁹ Kwetsbaarheden in Microsoft en Apple worden wereldwijd het vaakst gebruikt voor cyberaanvallen.³⁰

Daaraan verbonden verplicht de NIS2-richtlijn³¹ aan organisaties die essentiële (e.g. energievoorziening, bankwezen, etc.) of andere belangrijke diensten (e.g. postdiensten, afvalbeheer) leveren om maatregelen te nemen voor risicobeheer van hun netwerk- en informatiesystemen (art. 21 NIS2). Afhankelijk van de dienst en de betrokken risico's, kan dit betekenen dat dergelijke organisaties meer eigen controle moeten behouden of verwerven over hun cyberveiligheid.

Databeheer en -veiligheid



³² Zie, in het bijzonder, artikel 28 van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Algemene Verordening Gegevensbescherming, AVG)

³³ Hof van Justitie van de EU, Case C-362/14 Schrems v Data Protection Commissioner EU:C:2015:650. EU:C:2020:559; Hof van Justitie van de EU, Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems

³⁴ S. Battle, A. van Waeyenberge (2024), 'EU-US Data Privacy Framework: A First Legal Assessment,' *European Journal of Risk Regulation* 15:191-200.

³⁵ B. Clifton (2025, 'Schrems III – how likely is it and how to be prepared.' Hier beschikbaar: <https://briancclifton.com/blog/2025/05/19/schrems-iii-how-likely-and-how-to-prepare/>

³⁶ 'EU-US Data Privacy Framework in 2026: What Organizations Need to Know,' GlobalDataShield 27 maart 2026; <https://globaldatashield.com/blog/eu-us-data-privacy-framework-2026>

Data van Europese organisaties worden vaak bewaard op cloudservers van Amerikaanse bedrijven. Voor persoonsgegevens blijven de Europese organisaties verantwoordelijk voor de verwerking hiervan en moeten zij ervoor zorgen dat deze verwerkingen alle gegevensbeschermingsprincipes van de Algemene Verordening Gegevensbescherming naleven (zie art. 5 AVG). De laatste jaren nemen alarmsignalen toe over de dataveiligheid en gegevensbescherming van vele niet-Europese cloudservers.³²

Het grootste alarmsignaal doet zich voor met betrekking tot de mogelijkheid die de Europese commissie heeft om een zogenaamd adequaatsbesluit vast te stellen met betrekking tot de privacyregelgeving in een derde land. Concreet betekent zo'n besluit dat dit derde land, in dit geval: de Verenigde Staten, een "een passend beschermingsniveau waarborgt" voor de bescherming van de persoonsgegevens (art. 45 AVG). De Europese Commissie heeft al verscheidene malen zo'n kader gemaakt, maar dit werd al tweemaal vernietigd door de arresten Schrems I en II van het Hof van Justitie van de EU.³³

Sinds 2023 bestaat het *EU-VS Data Privacy Framework* (DPF).³⁴ De laatste tijd doen zich alarmsignalen voor omdat de DPF te nauw verbonden is met de uitvoerende macht in de Verenigde Staten. Zo is dit goedgekeurd onder een besluit van de uitvoerende macht (*Executive Order 14086*) en bevat het weinig garanties rond de proportionaliteit van het gebruik van de *Foreign Intelligence Surveillance Act* (FISA).³⁵ De voornaamste toezichthoudende commissie – de *Data Protection Review Court* – lijkt ook onvoldoende onafhankelijk omdat het zich binnen de uitvoerende macht bevindt, waardoor de leden door de overheid worden benoemd en de commissie slechts beperkte transparantieplichtingen heeft.³⁶

Op 30 juni stuurde Max Schrems, hoofd van Noyb – European Center for Digital Rights, een open brief naar de Europese Commissie, om gefaseerd uit het DPF te stappen. Aanleiding hiervoor was het oordeel van het Amerikaanse Hooggerechtshof in *Trump v. Slaughter*, waarin geoordeeld wordt dat uitvoerende instanties als de *Federal Trade Committee*, maar dus ook de DPRC, geen onafhankelijkheid hebben van de Amerikaanse administratie. Hiermee zou de DPRC niet volstaan als een onafhankelijk rechtsmiddel voor EU-burgers.

³⁷ EPDS (2024), *Decision of the European Data Protection Supervisor following its investigation into the European Commission's use of Microsoft 365*. Hier beschikbaar: https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/european-commissions-use-microsoft-365-infringes-data-protection-law-eu-institutions-and-bodies_en. Deze problemen zouden, in principe, sinds 11 juli 2025 opgelost moeten zijn: EPDS (2025), 'Letter to Commission of July 11th, 2025.' Hier beschikbaar: https://www.edps.europa.eu/system/files/2025-07/25-07-11-letter-to-commission_2021-0518_en.pdf

³⁸ 'What the CLOUD Act Really Means for EU Data Sovereignty,' *Wire* 15 Juli 2025; https://wire.com/en/blog/cloud-act-eu-data-sovereignty?utm_source=copilot.com

³⁹ 'Microsoft admits it 'cannot guarantee' data sovereignty,' *The Register* 25 juli 2025.

⁴⁰ Homeland Security (2020), *Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China*. Hier beschikbaar: https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf

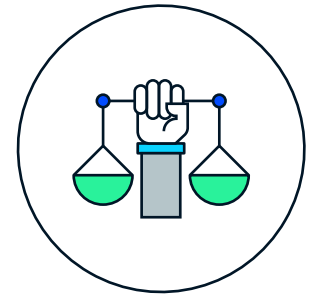
⁴¹ "Chinese 'kill switches' found in Chinese-made power inverters in US solar farm equipment that could let Beijing remotely disable power grids in a conflict." *Security Affairs* 18 Mei 2025: <https://securityaffairs.com/178005/hacking/rogue-devices-in-chinese-made-power-inverters-used-worldwide.html>

⁴² Het gaat over: COM(2026) Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)

Een ander probleem doet zich voor met betrekking tot *telemetry* van bepaalde digitale toepassingen, waarbij deze toepassing automatisch bepaalde data doorsturen naar de producent of andere partijen. Hierdoor kunnen ernstige privacydiscussies ontstaan.³⁷

Een laatste heikel punt met Amerikaanse bedrijven is de Amerikaanse CLOUD act. Deze voorziet de mogelijkheid voor Amerikaanse politiediensten om bedrijven die in de VS gevestigd zijn te dwingen data over te dragen, zelfs als deze data op Europese servers staat.³⁸ Antoine Carniaud, directeur publieke en juridische zaken van Microsoft France, verklaarde in het Franse parlement dat hij geen garanties kon bieden over de datasoevereiniteit van data van Franse burgers indien de Amerikaanse overheid die data opvraagt onder de CLOUD Act.³⁹ Deze regelgeving is van toepassing op alle bedrijven die onderworpen zijn aan de Amerikaanse wetgeving, wat ook Europese bedrijven kunnen zijn als zij – door een 'minimum contact' – onderhevig zijn aan de jurisdictie van de VS.

Deze bezorgdheden zijn er natuurlijk niet alleen met betrekking tot Amerikaanse bedrijven. Ook de Chinese Nationale Inlichtingenwet (2017) voorziet dat Chinese bedrijven – in het geheim – moeten meewerken aan nationale inlichtingen.⁴⁰ Andere ontwikkelingen met betrekking tot Chinese technologie zijn eveneens zorgwekkend. Zo vonden onderzoekers een 'kill switch' in Chinese stroomomvormers voor zonnepanelen, waardoor deze ingezet zou kunnen worden in politieke conflicten.⁴¹ Vanaf mei 2026 drong de Europese Commissie er sterker op aan bij de lidstaten om Huawei en ZTE te weren uit telecomnetwerken.⁴²



⁴³ Rechtbank Amsterdam, afdeling privaatrecht, Stichting Bits of Freedom tegen Facebook Netherlands, Meta Platforms Ireland LTD. en Meta Platforms Inc, zaaknummer C/13/774725/KG ZA 25-687 MK/JD.

⁴⁴ 'Meta negeert uitspraak Nederlandse rechter over algoritme,' VPN Nederland 24 oktober 2025: <https://www.vpnnederland.nl/blog/meta-negeert-uitspraak-nederlandse-rechter>.

⁴⁵ 'Berichten-app Telegram komt in Europa onder Belgisch toezicht,' VRT NWS 6 mei 2024: <https://www.vrt.be/vrtnws/nl/2024/05/06/bipt-gaat-in-ons-land-toezicht-houden-op-berichten-app-telegram/>

⁴⁶ 'EU Moves Against TikTok's 'Addictive Design,' The European Times 10 april 2026: https://europeantimes.news/2026/02/eu-moves-against-tiktoks-addictive-design/?utm_source=copilot.com

⁴⁷ 'Commission fines X EUR 120 million under the Digital Services Act.' Hier beschikbaar: https://digital-strategy.ec.europa.eu/en/news/commission-fines-x-eu120-million-under-digital-services-act?utm_source=copilot.com

⁴⁸ 'X appeals \$140M penalty from the EU Commission,' Social Media Today 22 februari 2026: https://www.socialmediatoday.com/news/x-formerly-twitter-challenges-eu-commission-dsa-penalty-fine/812791/?utm_source=copilot.com

Verscheidene Europese wetgevende kaders – zoals het Europees Verdrag voor de Rechten van de Mens en het Handvest voor de Grondrechten van de Europese Unie – bieden een bindend moreel kompas hoe wetgeving en technologie moet worden ontwikkeld en gebruikt. Voor digitale technologieën geeft de *Europese verklaring voor digitale rechten en beginselen* (2022) een niet-bindende richtsnoer hoe deze rechten te vertalen naar digitale technologieën. Deze regels worden verder geconcretiseerd in verplichtingen in Europese Verordeningen zoals de digitaaldienstenverordening en de AI-Verordening. Het handhaven van deze regels, vooral bij grote bedrijven die buiten Europa gevestigd zijn, blijkt niet evident. De vrees leeft dat deze bedrijven *too big to regulate* (aan het worden) zijn, en zich niet zullen schikken naar Europese normen en waarden. Enkele voorbeelden:

- Het Amerikaanse Meta (het moederbedrijf van Facebook) geeft volgens een Nederlandse rechtbank gebruikers niet blijvend de keuze om algoritmes uit te schakelen of aan te passen. Hierdoor wordt hun de controle ontnomen over hoe informatie wordt gepresenteerd.⁴³ Meta liet weten de aanpassingen voorlopig niet uit te voeren en stelde beroep in.⁴⁴
- Het oorspronkelijk Russische Telegram (nu gevestigd in Dubai) staat reeds meer dan twee jaar onder verscherpt Europees toezicht omdat grote hoeveelheden illegale inhoud erop circuleert, zoals uitkleedapps, beelden van seksueel kindermisbruik, terroristische inhoud, etc.⁴⁵
- De Europese Commissie oordeelde voorlopig dat de app TikTok een verslavend ontwerp heeft en – omdat het zich hoofdzakelijk richt naar kinderen en jongeren – hiermee in overtreding is met de digitaaldienstenverordening. TikTok vecht dit oordeel aan.⁴⁶
- Het Amerikaanse X werd veroordeeld voor het verspreiden van illegale inhoud, desinformatie, misleidende interface-ontwerpen en geen toegang geven tot data voor onderzoekers.⁴⁷ De eigenaar van X heeft fel gereageerd door de Europese Commissie te vergelijken met het naziregime en vecht de boete aan.⁴⁸

De voorgaande argumenten geven aan dat er veel goede redenen zijn voor Europese bedrijven en overheden om (meer) in te zetten op digitale soevereiniteit. Sommige van deze argumenten zijn relatief nieuw, andere zijn al langer relevant. *Wat zorgt ervoor dat digitale soevereiniteit plots zo hoog op de (Europese) agenda staat?*

Hoe kwam digitale soevereiniteit op de (politieke) voorgrond in Europa?



⁴⁹ Europese Commissie (2020), 'Europe's moment: Repair and Prepare for the Next Generation?' COM(2020) 456 final; <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0456&from=en>

⁵⁰ Europese Commissie (2013). Towards a more competitive and efficient defence and security sector. Communication from the Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions; European External Action Service (2016). Shared vision, common action: a stronger Europe. A global strategy for the European Union's foreign and security policy. Beschikbaar hier: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf. Voor verdere discussie: E. Michaels & M. Sus (2024). '(Not) Coming of age? Unpacking the European Union's quest for strategic autonomy in security and defence,' European Security 33:3: 383-405.

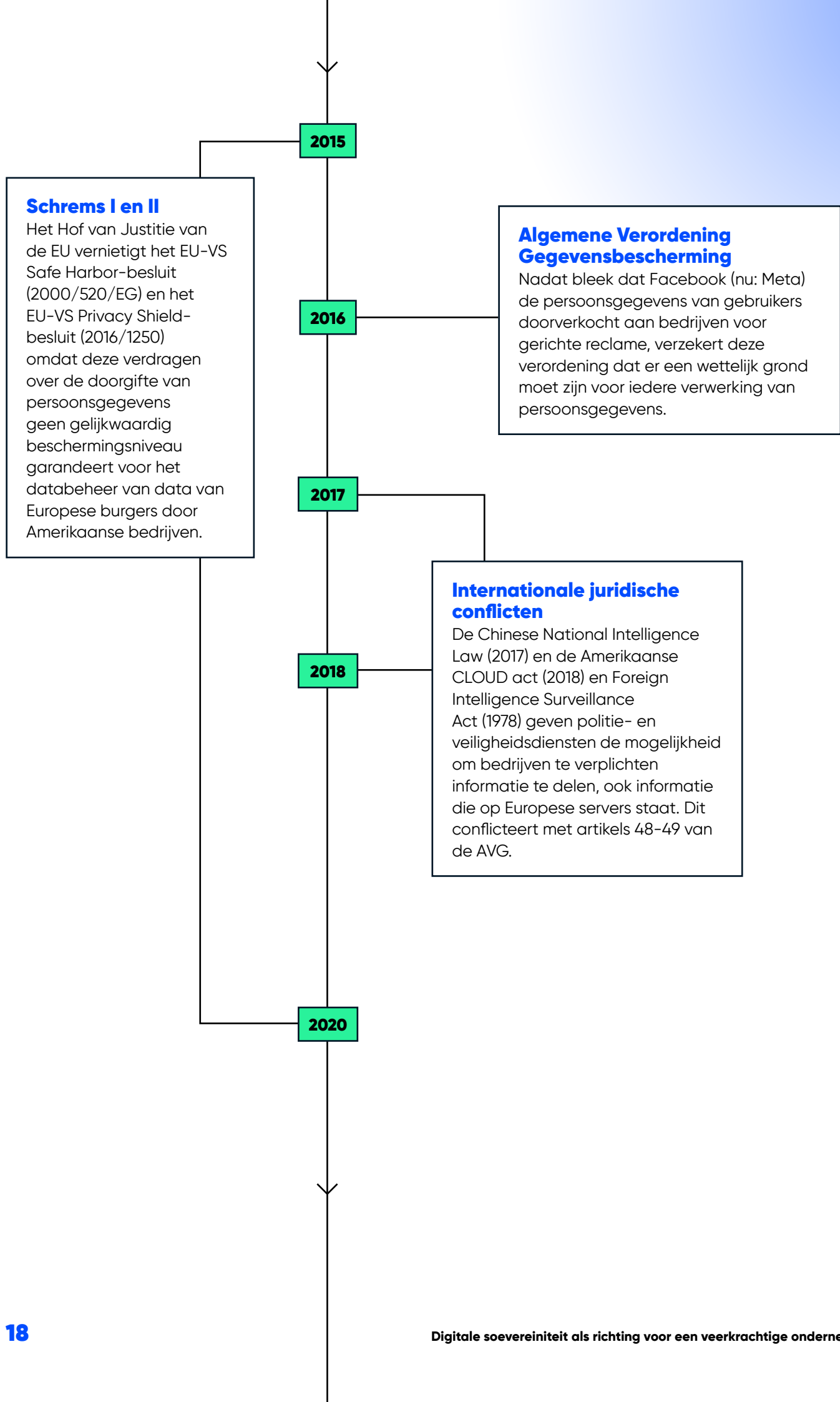
⁵¹ Europese Commissie (2021). Trade Policy Review – An Open, Sustainable and Assertive Trade Policy (COM(2021) 66 final). Brussels, 18 February 2021; C. Cagnin et al. (2021). Shaping and securing the EU's Open Strategic Autonomy by 2040 and beyond. Publications Office of the European Union, Luxembourg, 2021: https://data.europa.eu/doi/10.2760/414963_JRC125994. S. Mariotti (2025). "Open strategic autonomy" as an industrial policy compass for the EU competitiveness and growth: The good, the bad, or the ugly?. Journal of Industrial and Business Economics 52: 1-26.

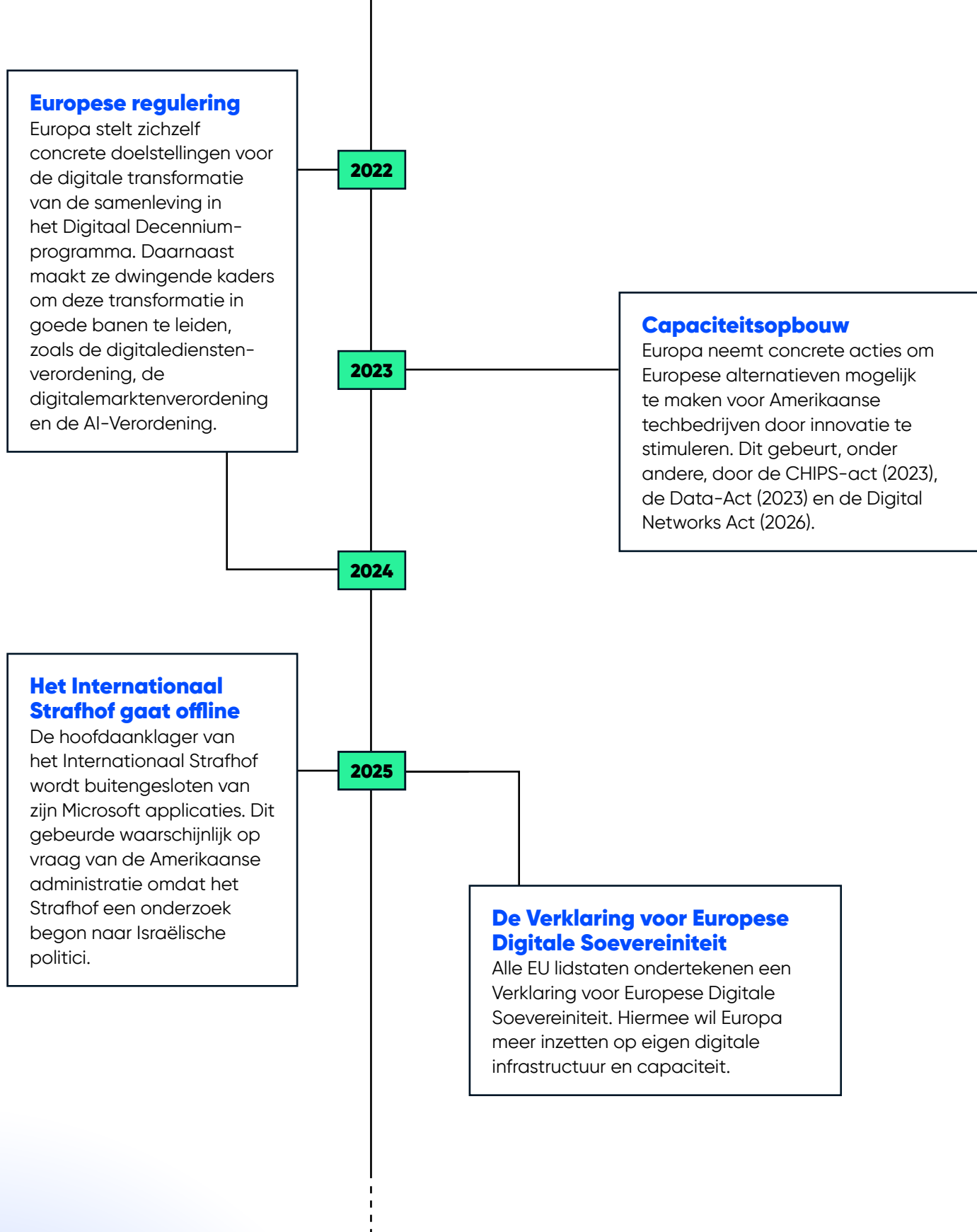
Digitale soevereiniteit is een logische vervolgstap in de Europese zoektocht naar **'Open Strategische Autonomie.'** Sinds de *EU Global Strategy* (2016) is dit een centraal element in de buitenlandstrategie van de EU als *de mogelijkheid om overal en altijd autonoom te kunnen handelen met gelijkgezinde partners volgens de eigen waarden en belangen.*⁴⁹ Belangrijke triggers voor deze strategische keuze waren de Russische inval op de Krim, de vluchtelingencrisis en terreuraanvallen van IS.⁵⁰ Deze gebeurtenissen legden een aantal structurele kwetsbaarheden voor Europa bloot, vooral inzake militaire autonomie, interne veiligheid en grensbewaking. Door andere gebeurtenissen zoals onthullingen over spionage (Snowden), ontwrictingen in waardeketens (coronapandemie) of energielevering (de Russische invasie in Oekraïne) verbreedde de beleidskeuze voor open strategische autonomie naar andere sectoren.⁵¹ Dit gebeurde ook met betrekking tot digitale technologieën, met als belangrijkste kantelpunten:

2013

Snowden-onthullingen

Edward Snowden onthulde dat de Amerikaanse National Security Agency (NSA) via surveillance-programma's (PRISM, XKeyscore) toegang had tot Europese data beheerd door Amerikaanse techbedrijven.





Maakt Europa nu de omslag?



⁵² European Union. (2022). *Declaration for European Digital Sovereignty*. Brussels. Hier beschikbaar: *Declaration for European Digital Sovereignty*

⁵³ European Union. (2022). *Declaration for European Digital Sovereignty*. Brussels. Hier beschikbaar: *Declaration for European Digital Sovereignty*

⁵⁴ Elysée (2025, November 18). *Summit on European Digital Sovereignty Delivers Landmark Commitments for a More Competitive and Sovereign Europe*. <https://www.elysee.fr/en/emmanuel-macron/2025/11/18/summit-on-european-digital-sovereignty-delivers-landmark-commitments-for-a-more-competitive-and-sovereign-europe>

⁵⁵ 'Commission fines Google €890 million for breaches of the Digital Markets Act,' European Commission News 23 juli 2026: https://digital-markets-act.ec.europa.eu/commission-fines-google-eur890-million-breaches-digital-markets-act-2026-07-23_en

⁵⁶ European Commission, Directorate-General for Digital Services. (2025, October 20). *Cloud sovereignty framework (Version 1.2.1)*. Publications Office of the European Union. https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en

⁵⁷ Zie: *European Digital Infrastructure Consortium - EDIC*

Deze voorgeschiedenis culmineert in november 2025 in een fundamentele beslissing van de Europese lidstaten om sterker in te zetten op hun digitale soevereiniteit. Het symbolische ankerpunt van deze beslissing kwam op initiatief van Frankrijk en Duitsland, namelijk de **Verklaring voor Europese Digitale Soevereiniteit**.⁵² Deze verklaring is richtinggevend voor het traject dat Europa de komende jaren wenst te lopen, met als leidend principe dat digitale soevereiniteit de voorwaarde is om, enerzijds, economische veiligheid, competitiviteit, weerbaarheid en vertrouwen te versterken en, anderzijds, om Europese democratische waarden te beschermen in de digitale wereld.⁵³

Op een Europese top in november 2025 werden hiertoe zeven prioritaire doelstellingen geïdentificeerd.⁵⁴

- **Vereenvoudiging en stroomlijning** van Europese **regelgeving**. Europa heeft de laatste jaren heel wat wetgeving geproduceerd rond digitale technologieën. Wanneer deze regels onvoldoende op mekaar afgestemd zijn, is dit nefast voor innovatie. De pakketten van maatregelen onder de digitale omnibus dienen om deze regels beter op elkaar af te stemmen en – waar mogelijk – overbodige regulering te verwijderen.
- **Eerlijkere digitale markten**. De Europese Commissie gaat een versnelling hoger schakelen om de Digitaalemarktenverordening (DMA) af te dwingen van de Amerikaanse grote techbedrijven. Een gevolg hiervan is, bijvoorbeeld, dat in juli 2026 Google veroordeeld werd tot een boete van in totaal 890 miljoen euro. De reden was dat het zijn eigen producten stelselmatig bevoordeelde via de zoekfunctie.⁵⁵
- **Datasoevereiniteit**. De Europese Commissie heeft via het Cloud Sovereignty Framework criteria opgesteld om datasoevereiniteit concreet te kaderen. Dit kader laat toe om het soevereiniteitsniveau van een technologie in te schatten; gebruikers moeten nog wel zelf inschatten welk soevereiniteitsniveau noodzakelijk is voor de digitale technologie die zij gebruiken.⁵⁶
- Het oprichten van **digitale gemeenschappelijke ruimtes** (*Digital Commons*), een gemeenschappelijk gebruikte digitale infrastructuur. Deze infrastructuur draait op opensourcesoftware, open standaarden en open data. De *Digital Commons EDIC* is opgericht door Frankrijk, Duitsland, Nederland en Italië. In de toekomst kan deze verder uitbreiden naar andere lidstaten.⁵⁷
- Meer gebruik van **opensource software** in publieke administraties. Dit werd recent verder geduid in de opensourcestrategie van de EU.

- Een **taskforce** wordt opgericht om een instrument uit te werken om digitale soevereiniteit concreet te **meten**. Hieraan is nog geen eenduidig gevolg gegeven.
- Concrete maatregelen om **Frontier AI** te ondersteunen. Frontier AI is een verzamelnaam voor de meest performantie, beste AI-modellen. Deze ambitie krijgt vooral vorm onder het AI Continent Action Plan.

Concrete initiatieven die uitdrukkelijk Europese leveranciers zouden verplichten liggen gevoelig in de context van Amerikaanse handelsovereenkomsten.⁵⁸ Afhankelijk van de verdere uitwerking kan dit vorm krijgen onder de recent voorgestelde Cloud and AI Development Plan.

Enkele **andere relevante initiatieven** op Europees niveau:

Gaia-X

Is een federatief data-infrastructuurproject. Vooral een afsprakenkader en infrastructuurmodel om clouddiensten veilig en eerlijk te laten samenwerken. Hier werken vele aanbieders van clouddiensten samen volgens dezelfde standaarden opdat die standaarden interoperabel zijn.

EU Sovereign Tech Fund (EU-STF)

Is een investeringsfond om kritieke open-source software te onderhouden, beveiligen en versterken. De meeste softwaretoepassingen gebruiken open source bestanddelen als fundamentele bouwstenen

DNS4EU

Levert een Europese DNS-resolverdienst (een soort telefoonboek waarmee IP-adressen gevonden worden) die werkt volgens de Europese privacy- en cybersecurityregels

Tech Sovereignty Package

Is een bundel initiatieven gericht op to de capaciteit van Europa om digitale infrastructuur zelf te ontwikkelen, controleren en opereren. Zoals: Cloud and AI Development Act (CADA) en Chips Act 2.0. Het initiatief werd enkele malen uitgesteld, maar krijgt concrete vorm sinds juni 2026.

⁵⁹ 'Gartner reveals top technologies shaping government AI adoption,' 9 september 2025: <https://www.gartner.com/en/newsroom/press-releases/2025-09-09-gartner-reveals-top-technologies-shaping-government-ai-adoption>

Deze evolutie richting soevereiniteit geen louter Europees fenomeen. Gartner voorspelt dat tegen 2028 zo'n 65% van overheden wereldwijd technologische soevereiniteitsvereisten zullen instellen.⁵⁹

Enkele voorbeelden van recente initiatieven:

Verenigde Staten

America's AI Action Plan

China

Semiconductor policy 2026

Zuid-Korea

NEXT Strategic Technologies Roadmap

Rusland

Sovereign Internet Law

Brazilië

PIX Instant Payments System

Afrikaanse Unie

Data Policy Framework

Australië

Whole-of-Government Cloud Computing Policy

Vaak gestelde vragen over digitale soevereiniteit



⁶⁰ KPMG (2025), 'Cloud Monitor 2025: Digital sovereignty begins in the cloud – how companies create innovation, security and trust.' Hier beschikbaar: <https://assets.kpmg.com/content/dam/kpmg/tr/pdf/2025/10/kpmg-cloud-monitor-2025-consulting.pdf>

⁶¹ Cisco (2026), 'A Shifting Paradigm: Governance in the Age of AI.' Hier beschikbaar: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2026.pdf

⁶² McKinsey & Company, 'Sovereign AI: Building ecosystems for strategic resilience and impact.' Hier beschikbaar: <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/sovereign-ai-building-ecosystems-for-strategic-resilience-and-impact>

⁶³ Volgens de jaarlijkse analyse van het Magic Quadrant for Strategic Cloud Platform Services zijn de clouddiensten van Amazon, Google en Microsoft de meest performante en toekomstbestendige. Zie: Gartner (2025), 'Magic Quadrant for Strategic Cloud Platform Services.' Hier Beschikbaar: https://www.gartner.com/doc/reprints?id=1-2LM5HTYC&ct=250805&st=sb&trk=59e09e9f-ef2e-4f08-9d0c-fce0d64139c7&sc_channel=el

⁶⁴ C. Stolwijk et al. (2023), 'Digital Sovereignty: How Europe Takes Back Control. The Opinion of European Digital Leaders.' Hier beschikbaar: <https://publications.tno.nl/publication/34640695/aPvPww/TNO-2023-digital.pdf>

Is digitale soevereiniteit niet gewoon een politieke ideologie?

Streven naar digitale soevereiniteit is inderdaad vaak politiek gekleurd, vooral omdat het thema op de voorgrond treedt nu politieke spanningen tussen de Europese Unie en de Verenigde Staten hoog oplopen. Bedrijven worden daarentegen niet primair gedreven door politieke ideologie, maar door winstmaximalisatie, kostenoptimalisatie en risicobeheersing. Streven naar digitale soevereiniteit kan eerder overkomen als een protectionistische, politieke reflex die niet strookt met een innovatie- of marktlogica. Tegelijk zijn er – zoals hierboven aangegeven – goede redenen om in te zetten op meer controle over data en digitale toepassingen. Dit vertaalt zich reeds naar het bedrijfsleven: 44% van bedrijven zijn bereid om tot 20% extra te betalen voor soevereine clouddiensten.⁶⁰

Zal digitale soevereiniteit zorgen voor een financiële meerwaarde?

Een direct verband tussen winst en digitale soevereiniteit is er niet meteen, vooral omdat digitale soevereiniteit erg veel vormen en gradaties heeft. Vendor lock-in zorgt er alleszins voor dat organisaties weinig controle hebben over kostprijs en minder mobiel zijn wanneer de dienstverlening of een product in kwaliteit afneemt. Soevereiniteit maakt dan alleszins weerbaarder en minder kwetsbaar voor plotse prijsstijgingen.

Soms wordt geopperd dat soevereiniteit extra kosten met zich meebrengt; soms wordt er gesteld dat (minstens op termijn) de kosten wel zullen meevallen. Dat heeft te maken met hoe doordacht en doelgericht strategieën voor digitale soevereiniteit worden ingezet. Daarnaast is het ook niet eenvoudig om in te schatten wat de langetermijnswinsten zijn. Sommige studies wijzen hierbij op:

- Meer controle over data maakt een bedrijf wendbaarder, verhoogt klantenvertrouwen en operationele efficiëntie.⁶¹
- Toenemend gebruik van AI zorgt ervoor dat meer en meer bedrijven belang hechten aan soevereiniteit.⁶² Naarmate AI dieper verweven raakt in bedrijfsprocessen, neemt ook de afhankelijkheid van die externe aanbieders toe. Wie op dat moment onvoldoende controle heeft over zijn data en systemen, ziet zijn strategische keuzes steeds meer bepaald worden door de logica (en het kostenplaatje) van de aanbieder in plaats van de eigen bedrijfsdoelstellingen.

⁶⁵ C. Stolwijk et al. (2023), 'Digital Sovereignty: How Europe Takes Back Control. The Opinion of European Digital Leaders.' Hier beschikbaar: <https://publications.tno.nl/publication/34640695/aPvPww/TNO-2023-digital.pdf>

⁶⁶ Bythepulse (2026), 'European vs US SaaS Tools 2026: Privacy-First Wins Complete Analysis.' Hier beschikbaar: <https://bythepulse.io/european-vs-us-saas-2026/>

⁶⁷ M. Diependaele, Vraag om uitleg 2113 (2025_2026) in Vlaams Parlement (Commissie Algemeen Beleid, Financiën, Begroting, Justitie en Onroerend Erfgoed). Hier beschikbaar: <https://www.vlaamsparlement.be/nl/parlementair-werk/commissies/commissievergaderingen/1998524/verslag/2004212>

⁶⁸ R. Bapna et al. (2022), 'Single-Sourcing vs. Multisourcing: An Empirical Analysis of Large Information Technology Outsourcing Arrangements' Information Systems Research 34: 1109-1130.

⁶⁹ Cisco (2017), 'Single versus multiple vendors: Asking the right questions.' Hier beschikbaar: https://www.cisco.com/c/dam/m/en_sg/cisco-start/asset/pdfs/ia_bob_single_vs_multiple_vendors_asking_the_right_questions.pdf

⁷⁰ OECD (2025), 'OECD Supply Chain Resilience Review: Navigating Risks.' Beschikbaar hier: https://www.oecd.org/en/publications/oecd-supply-chain-resilience-review_94e3a8ea-en.html

⁷¹ 'What leaders need to know about building tech resilience amid geopolitical risk,' McKinsey Blog 20 Februari 2026: <https://www.mckinsey.com/about-us/new-at-mckinsey-blog/what-leaders-need-to-know-about-building-tech-resilience-amid-geopolitical-risk>

⁷² 'What leaders need to know about building tech resilience amid geopolitical risk,' McKinsey Blog 20 Februari 2026: <https://www.mckinsey.com/about-us/new-at-mckinsey-blog/what-leaders-need-to-know-about-building-tech-resilience-amid-geopolitical-risk>

Zijn alternatieven voor de standaardproducten van Google, Apple, Facebook, Amazon, Microsoft (GAFAM) en van de nieuwe grote techbedrijven (OpenAI, Anthropic, Tesla) wel even goed?

Hoe goed een product is, hangt af van de concrete noden.

- *Wil je vooral werken met bedrijven die iedereen kent?* De diensten van GAFAM (Google, Apple, Facebook, Amazon, Microsoft) zijn inderdaad wereldwijd in gebruik.⁶³ Europese alternatieven hebben meestal een kleiner bereik en zullen – vooral buiten Europa – minder gekend zijn.⁶⁴
- *Hoe aangepast moet jouw toepassing zijn aan lokale wetgeving?* De diensten van Europese aanbieders zijn meestal beter aangepast aan lokale wetgeving, vooral als het over CRM gaat.⁶⁵
- *Hoe AVG-compliant moeten jouw productiviteitssuites zijn?* Europese productiviteitssuites zijn meestal wel AVG-compliant zijn, diensten van GAFAM zijn dat in mindere mate.⁶⁶
- *Hoe aanpasbaar moeten jouw digitale toepassingen zijn?* Door opensourcesoftware te gebruiken, kunnen bedrijven beter inspelen op lokale noden door de software te herschrijven naargelang de vereisten. Een SaaS dienst van GAFAM kan in mindere mate aangepast worden aan concrete noden. Tegelijk zijn mensen vaak – niet altijd terecht – terughoudend over *opensourcesoftware* en leeft het gevoel dat dit minder performant is en minder ruimte laat voor hulplijnen.⁶⁷

Een eenduidig antwoord op de vraag of de standaardproducten gewoonweg beter zijn is er niet. Alles hangt hier af van het type digitale toepassingen, de verwachte inzetbaarheid, het wettelijke kader en de verwachte aanpasbaarheid.

Is het niet logischer om zoveel mogelijk diensten af te nemen van dezelfde leverancier?

Ook hier is geen eenduidig antwoord: concentreren of diversifiëren hangt van vele factoren af. Sommige studies wijzen op voordelen van concentratie zoals:

- Kostenverlaging en operationele winsten door snellere implementatie en lagere trainingsnoden.⁶⁸
- Duidelijkere aansprakelijkheid en incidentmanagement ('one throat to choke').⁶⁹

Tegelijk zijn er ook nadelen verbonden aan te hoge concentratie, zoals:

- Concentratie van leveranciers leidt op termijn tot verhoogde kosten om van leverancier te veranderen en tot verminderde onderhandelingscapaciteit.⁷⁰
- Kwetsbaarheden bij dominante leveranciers veroorzaken *single points of failure*.⁷¹
- Hoge afhankelijkheden zorgen voor minder architecturale vrijheid en hogere kosten voor toekomstige innovatie.⁷²

⁷³ 'Interview: Zeggenschap en controle over data terugpakken,' DSR Magazine februari 2026: <https://www.dsnews.eu/magazine-nl/editie-01-2026/zeggenschap-en-controle-over-data-terugpakken-0118/>

⁷⁴ OECD (2025), 'OECD Supply Chain Resilience Review : Navigating Risks.' Beschikbaar hier: https://www.oecd.org/en/publications/oecd-supply-chain-resilience-review_94e3a8ea-en.html

⁷⁵ M. Godefroid et al. (2022). 'How to measure the status quo bias? A review of current literature.' Management Review Quarterly 73: 1667-1711: <https://link.springer.com/article/10.1007/s11301-022-00283-8>; Shirish, A. (2021). Technology renewal, user resistance, user adoption: status quo bias theory revisited. Journal of Organizational Change Management. <https://doi.org/10.1108/JOCM-10-2020-0332>

⁷⁶ M. Saghaian et al. (2021). 'Stagewise Overview of Issues Influencing Organizational Technology Adoption and Use,' Frontiers in psychology 12: 630145

⁷⁷ Beer M, Nohria N. Cracking the code of change. Harv Bus Rev. 2000 May-Jun;78(3):133-41, 216. PMID: 11183975; J. Marschall (2025), 'The human factor: Why business tech projects fail and how to prevent,' Qodea 6 maart 2025: <https://www.bynd.com/eu/articles/why-business-tech-projects-fail-and-how-to-prevent-it>

⁷⁸ Zie: IBRS (2021), 'The Economic Impact of Software as a Service in Australia,' Hier beschikbaar:

Voor publieke overheden zijn andere elementen ook relevant.

- Aanbestedingen worden vaak ondeelbaar gemaakt in plaats van opgedeeld in verschillende percelen (zoals: aparte percelen voor softwareontwikkeling, hosting, onderhoud, support, etc).⁷³ Dit verhoogt de drempel voor aanbieders om zulke opdrachten te ambiëren, het bevoordeelt grotere spelers en kan vendor lock-in versterken. Volgens art. 46 van Europese richtlijn 2014/24/EU, omgezet in art. 58 de Belgische wet op de overheidsopdrachten, zou een overheid een aanbesteding in verschillende percelen moeten opdelen. Doet men dit niet, dan hoort men dit te motiveren. Een ondeelbare aanbesteding laat namelijk minder concurrentie toe (zie overweging 78 van de richtlijn).
- Concentratie van leveranciers leidt tot hogere aanbestedingskosten, minder democratische controle en grotere kwetsbaarheid voor geopolitieke schokken.⁷⁴

Waarom is er vaak weerstand om stappen te zetten richting meer digitale soevereiniteit?

Veranderingen in bedrijfsprocessen en leveranciers kunnen aanvoelen als een opgave. Dit is het geval voor zowel werknemers als bedrijfsleiders. Onderzoek toont aan dat ook bedrijven vaak avers zijn voor verandering (*status quo bias*) of verandering afwijzen omdat hiermee vroegere investeringen lijken te verdwijnen (*sunk cost fallacy*).⁷⁵ Zo hebben heel wat bedrijven hun data gemigreerd naar datacenters van Amazon, Google of Microsoft, en zijn werknemers vooral geschoold in het gebruik van de digitale oplossingen van deze bedrijven.⁷⁶

Om deze redenen gaat digitale soevereiniteit niet enkel over het al dan niet gebruiken van digitale technologieën, maar ook over de adoptie door medewerkers. Zo'n 70% van transformatieprocessen falen, met als voornaamste redenen een gebrek aan training, trage adoptie van de nieuwe technologie of een algehele weerstand tegenover verandering.⁷⁷ Daarom is het essentieel om bij de implementatie van nieuwe technologieën voldoende aandacht te hebben voor de eindgebruiker en hen maximaal deel te maken van deze digitale transformatie.

Betekent meer soevereiniteit ook meer werk voor mijn IT-personeel? Kunnen zij dat aan?

Het is mogelijk dat bepaalde keuzes voor meer controle over data en digitale technologieën gepaard gaan met meer nood aan IT-ondersteuning. Intern IT-personeel kan afgebouwd zijn doordat organisaties kiezen voor de dienstverlening van grote Amerikaanse bedrijven. Zo kunnen sommige organisaties niet over het menselijk kapitaal beschikken om, bijvoorbeeld, *opensourcesoftware* te gebruiken.⁷⁸ Dit element zal meespelen in een kosten/baten analyse van bepaalde overstappen, namelijk: heb ik bijkomend menselijk kapitaal nodig om deze overstap te maken? Tegelijk zijn er ook tussenoplossingen, zoals IT-bedrijven die opensourcesoftware 'as a service' aanbieden waardoor er geen extra interne capaciteit nodig is.

⁷⁹ 'DNIP Briefing #48: Dokumentierte Überwachung,' DNIP 4 November 2025: <https://dnip.ch/2025/11/04/dnip-briefing-48-dokumentierte-ueberwachung/>

⁸⁰ Interview: Zeggenschap en controle over data terugpakken,' DSR Magazine februari 2026: <https://www.dsnews.eu/magazine-nl/editie-01-2026/zeggenschap-en-controle-over-data-terugpakken-0118/>

Amerikaanse bedrijven bieden nu ook soevereine oplossingen aan. Kan ik niet gewoon hierop overstappen?

Veel onduidelijkheid bestaat over welke digitale toepassingen het label 'soverein' verdienen. Bijvoorbeeld, de *Sovereign Cloud* van Microsoft heeft twee versies:

- De *Sovereign Public Cloud* bewaart data uitsluitend binnen Europese grenzen en geeft de gebruiker controle over zijn data: wat wordt opgeslagen, wie toegang heeft en wie over de encryptiesleutels beschikt. Hier blijft Microsoft nog steeds de eigenaar van het platform, waardoor ze nog steeds onder de Amerikaanse *CLOUD Act* en *FISA* vallen.
- De *Sovereign Private Cloud* bewaart data in jouw lokaal datacenter en kan volledig worden afgesloten ('air-gapped'). Hier blijft de technologie onder de licenties van Microsoft vallen en blijft het systeem afhankelijk van de updates en beveiliging van Microsoft.

Deze clouddiensten bieden bepaalde opties voor organisaties die geen absolute maar wel verhoogde controle toelaten. Zaken om na te kijken bij datacontracten zijn, bijvoorbeeld:

- Wie controleert het platform of heeft hier eigenaarschap over?
- Hoe juridisch onafhankelijk van niet-EU wetgeving is deze aanbieder?
- Gebruikt de aanbieder open standaarden?
- Is de gebruikte software opensource?
- Kan ik mijn data laten interopereren met mijn andere bedrijfsprocessen?⁷⁹

Het Europese *Cloud Sovereignty Framework* bevat acht doelstellingen waaraan een clouddienst moet voldoen om effectief soverein te zijn. Een clouddienst soverein noemen zonder aan deze doelstellingen tegemoet te komen, is *sovereignty washing*. Amazon's *European Sovereign Cloud*, Google's *Sovereign Controls* of Microsoft's *Sovereign Cloud* zijn dan niet soverein in de volledige zin.⁸⁰ Toch blijft het afwachten op de resultaten van de Taskforce voor meer concrete soevereiniteitsstandaarden.

Visie en Aanbevelingen



Digitale soevereiniteit is eerder een richting dan een einddoel. Het staat niet op zich, maar het is een element dat meer en meer een rol gaat spelen in besluitvorming. Organisaties kunnen aarzelen om controle te ambiëren over digitale technologieën omdat het uiteindelijke doel – volledige digitale soevereiniteit – ver weg of zelfs onbereikbaar lijkt. Deze aarzeling komt voort uit het idee dat soevereiniteit een binaire toestand is, in plaats van een geleidelijk op te bouwen vermogen.

In de praktijk wordt digitale soevereiniteit niet bereikt via één beslissende sprong, maar door een reeks incrementele keuzes die afhankelijkheden verminderen, de handelingsvrijheid vergroten en de controle over kritieke assets versterken. Zelfs gedeeltelijke stappen – zoals het herwinnen van zeggenschap over data, het diversifiëren van leveranciers of het opbouwen van interne technische expertise – leveren hoe dan ook waarde op.

De vraag is dan ook niet of volledige soevereiniteit ooit haalbaar is, maar of de organisatie zich in de juiste richting beweegt. Doorheen die reis is het geen probleem om (tijdelijk) een risico op controleverlies te aanvaarden. Hierbij kan je rekening houden met, enerzijds, hoe groot het risico op controleverlies is bij een bepaald proces en, anderzijds, hoe moeilijk het is om stappen richting soevereiniteit te zetten.

Het soevereiniteitsvraagstuk zal de komende jaren een centraal thema blijven in het debat over digitale technologie. Omdat niemand precies kan voorspellen hoe deze discussie zich zal ontwikkelen, formuleert het Kenniscentrum Data & Maatschappij hieronder een aantal aanbevelingen voor de korte en middellange termijn.

Voor elke organisatie

- Soevereiniteit is een belangrijk doel, maar niet het enige dat telt. Weeg de nood aan controle steeds af tegen andere belangen, zoals gebruiksgemak, gegevensveiligheid, kostprijs en technische integratie.
- Behandel soevereiniteit eerder als een richting dan een einddoel. Herbekijk regelmatig de gebruikte technologieën en wie ze aanlevert met het oog op mogelijk controleverlies. Een leverancier die vandaag Belgisch of Europees is, kan morgen verward geraakt worden met partijen buiten Europa.

- Hoe zwaarder digitale technologie – en zeker AI – doorweegt in je organisatie, hoe belangrijker soevereiniteit wordt. Schat daarom systematisch in wat het risico is als je de controle over een bepaald systeem verliest samen met de waarschijnlijkheid dat dit controleverlies zich voordoet. Stem je aanpak op dat risico af. Je kan hiervoor een klassieke risicomatrix gebruiken, zoals ISO 31000.
- Omdat niemand goed kan voorspellen hoe de situatie op langere termijn evolueert, is flexibiliteit cruciaal. Ga na welke toepassingen zo kritiek zijn dat hun uitval de hele organisatie zou verlammen (dit noemt men een *single point of failure*: één onderdeel waarvan alles afhangt), en voorzie hiervoor minstens een back-upoplossing geworteld in Europese infrastructuur, of een andere concrete exitstrategie. Dit kan je opnemen in een Service Level Agreement.

Voor de Vlaamse overheid

- Koppel VLAIO-steunprogramma's voor Europese cloud- en AI-technologie aan concrete soevereiniteitscriteria, bij voorkeur gebaseerd op het Europese Cloud Sovereignty Framework. Zo hanteert iedereen dezelfde maatstaf.
- Handel zoveel mogelijk collectief. Investeer, bijvoorbeeld, in gedeelde Vlaamse of Belgische digitale infrastructuur, bijvoorbeeld gemeenschappelijke datacenters, zodat kleinere lokale besturen niet elk apart moeten onderhandelen met grote techbedrijven. Dit kan gebeuren door middel van het programma EuropAI.
- Bouw eigen expertise op om te toetsen of leveranciers hun claims zoals over soevereine oplossingen (zoals de *Sovereign Cloud*-varianten van Microsoft, Amazon of Google) ook werkelijk waarmaken. Zo steunen overheidscontracten op verifieerbare criteria in plaats van op marketingtaal. Steun ook hier op het Europese Cloud Sovereignty Framework.
- Maak vaker gebruik van de mogelijkheid om aanbestedingen op te splitsen in percelen (art. 58 van de Wet Overheidsopdrachten) – dat wil zeggen: afzonderlijke deelopdrachten, bijvoorbeeld hosting, onderhoud en support apart in de markt zetten in plaats van als één groot pakket. Zo krijgen ook kleinere aanbieders kansen, wat je leveranciers spreidt en het risico op *vendor lock-in* verkleint.
- Wees je bewust van de juridische kaders (waaronder de AI Act en AVG) en adviezen (waaronder van de Vlaamse Toezichtcommissie) die van toepassing blijven bij de verwerking van persoonsgegevens, ook wanneer beroep gedaan wordt op niet-Europese leveranciers

Voor beleidsmakers van de Vlaamse overheid

- Benader digitale soevereiniteit in de brede zin – dus niet enkel als een vraag over waar data wordt opgeslagen (datasoevereiniteit), maar ook op het gebruik van al je digitale technologieën en jouw menselijk kapitaal.
- De Europese taskforce voor digitale soevereiniteit heeft nog geen concrete indicatoren opgeleverd. Vlaanderen kan hierop vooruitlopen met een eigen monitoring- of maturiteitskader voor overheidsdiensten.
- Verduidelijk welke soevereiniteitsvereisten precies gelden voor diensten die onder de NIS2-richtlijn vallen. Neem minimumvereisten op, zoals een verplichte *fallback*-vereiste voor kritieke processen, met een lijst van erkende Europese alternatieven.

- Neem in het AI-beleidsplan stimulansen op voor publiek gefinancierde AI-projecten om waar mogelijk open(ere) modellen en open standaarden te gebruiken. Zo blijven de resultaten van publiek gefinancierd onderzoek niet volledig opgesloten in het ecosysteem van één leverancier. Dit kan uitgebreid worden naar de ontwikkeling van alle digitale toepassingen.
- Behandel rekenkracht (*compute*, de reken- en verwerkingscapaciteit die nodig is om AI-modellen te trainen en te gebruiken) als een apart aandachtspunt naast data: onderzoek of de Vlaamse en Europese *AI Factories* voldoende toegankelijke en betaalbare rekenkracht bieden als volwaardig alternatief voor Amerikaanse cloud-GPU's. Advies hiervoor kan ingewonnen worden bij de Belgische *AI Antenna*.
- Maak datasoevereiniteit een expliciete voorwaarde bij de keuze van AI-leveranciers voor overheidstoepassingen: waar worden de trainingsdata (waarmee het model werd ontwikkeld) en inferentiedata (de data die het model verwerkt bij gebruik) bewaard, en wie kan er op basis van buitenlandse wetgeving (zoals de Amerikaanse CLOUD Act) juridisch toegang tot krijgen?
- Investeer in AI-kennis en technisch personeel binnen de eigen administratie, zodat de AI-strategie niet uitsluitend wordt bepaald door de logica – en het kostenplaatje – van externe leveranciers.
- Overweeg bij publiek-private samenwerkingen contractuele voorwaarden of verplichte wettelijke screenings die overnames verbieden waaruit een risico op controleverlies zou kunnen voortkomen. Dit voorkomt complexe discussies zoals recent in Nederland.
- Lobby bij de federale overheid om als België aansluiting te zoeken bij de Digital Commons EDIC.

Voor koepelorganisaties

- Ontwikkel sectorspecifieke leidraden of modelcontracten waarin exitclausules, dataportabiliteit (het gemakkelijk kunnen overzetten van je data naar een andere leverancier) en een verbod op oneigenlijke overstapkosten standaard zijn opgenomen, zodat niet elk lid dit apart moet bevechten.
- Bundel de vraag van leden naar Europese of opensourcealternatieven, zodat ze samen meer onderhandelingsmacht hebben.
- Informeer leden actief over regelgeving die raakt aan digitale soevereiniteit – de *NIS2*-richtlijn (cybersecurity-eisen), de *Data Act* en de AVG – en over wat het label “soverein” bij een product precies wel en niet garandeert.

Voor bedrijven en organisaties: wat kan nu al?

- Maak een eenvoudige risicokaart van je eigen systemen: hoe essentieel is het systeem, hoeveel controle heb je er nodig over, hoe complex is de uitstap? Begin met de meest kritieke of gevoelige processen.
- Vermijd dat je bij nieuwe contracten volledig afhankelijk wordt van één leverancier. Neem overwegingen rond optionaliteit en portabiliteit sterk op in de IT-architectuur. Dat kan bevorderd worden door opensourcesoftware of open standaarden te gebruiken.

- Test opensourcealternatieven eerst uit op minder kritieke, minder sterk geïntegreerde toepassingen. Zo bouw je ervaring op zonder meteen het volledige risico te dragen.
- Betrek de eigen IT-afdeling vroeg bij de kosten-batenanalyse van een overstap: is er voldoende interne kennis en capaciteit, of moet die eerst worden opgebouwd?
- Zie soevereiniteit als een geleidelijk proces, niet als alles-of-niets. Ook kleine stappen – een contract heronderhandelen, één dienst diversifiëren, personeel bijscholen – leveren al waarde op, zelfs als volledige soevereiniteit niet haalbaar of nodig is.
- Pauzeer niet-dringende, lopende migraties naar Amerikaanse leveranciers tot er een bewuste afweging is gemaakt. Veel migraties lopen door zonder dat er écht haast bij is; een tijdelijke pauze kost meestal weinig, terwijl eenmaal gemigreerd in de praktijk vaak betekent: definitief gemigreerd.
- Lokale aannemers betrekken in processen is een vorm van *Corporate Social Responsibility* die klanten en werknemers verwelkomen. Maak hiervan gebruik en communiceer het duidelijk als een bedrijfsstrategie.

8.1

Verdiepend: Soevereiniteit in cyberspace?

⁸¹ S. D. Krasner (1999). Sovereignty: Organized Hypocrisy. Princeton University Press. <https://doi.org/10.2307/j.ctt7s9d5>

⁸² Zie art. 89 van het VN Zeerechtverdrag (1982) en art. 2 van het VN-Ruimteverdrag (1967).

⁸³ M. Mueller (2020), 'Against Sovereignty in Cyberspace,' International Studies Review (2020) 22: 779–801

⁸⁴ M. Mayer & Y.-C. Lu (2022), Digital Autonomy? Measuring the Global Digital Dependence Structure. Bonn. Center for Advanced Security, Strategic and Integration Studies; E. Akilli (2025). 'Forging the Digital Autonomy'. In: Cognitive Diplomacy and Digital Autonomy. Palgrave Macmillan, Cham.

⁸⁵ J.P. Barlow (1996) 'A Declaration of the Independence of Cyberspace,' Hier beschikbaar: <https://www.eff.org/cyberspace-independence>

⁸⁶ J. Pohle & T. Thiel (2020), Digital sovereignty, Internet Policy Review, 9(4).

⁸⁷ W. Chun (2005), Control and Freedom: Power and Paranoia in the Age of Fiber Optics. Harvard, Ma.: The MIT Press. N. Smicek (2016), Platform Capitalism. Polity Press; L. Denardis (2014). The Global War for Internet Governance. New Haven: Yale University Press.

⁸⁸ G. Falkner et al. (2024), 'Digital sovereignty - Rhetoric and reality,' Journal of European Public Policy 31: 2099–2120.

De term 'soevereiniteit' is niet nieuw. Klassiek gaat soevereiniteit over de mogelijkheid om het hoogste gezag uit te oefenen; of: om niet ondergeschikt aan hogere autoriteiten te zijn. Dit drukt zich uit op de drie vlakken van politieke macht: zelf regels maken (wetgevend), zelf deze regels uitvoeren (uitvoerend) en zelf de naleving controleren (rechtsprekend).

Soevereiniteit is steeds gekoppeld aan een gebied of territorium: de Belgische staat is de hoogste macht op Belgisch grondgebied. Dat idee stamt uit de principes van de Vrede van Westfalen (1648). Hier verklaarden de toenmalige Europese grootmachten dat elke natiestaat binnen het eigen territorium de hoogste macht uitoefent: *cuius regio, eius religio*.⁸¹ Tegelijk betekent dit dat buiten dat territorium of in gemeenschappelijke ruimtes (*commons*), zoals internationale wateren of in de ruimte,⁸² diezelfde natiestaat geen gezag kan laten gelden.

Daarom voelt het eigenaardig om te spreken over *digitale* soevereiniteit: cyberspace valt moeilijk in een (fysiek) territorium te vatten waarover iemand gezag kan laten gelden.⁸³ Vandaar dat sommigen liever over digitale autonomie spreken, als het vermogen om vrij te bewegen in cyberspace.⁸⁴

Aan de wieg van het wereldwijde web lag daarenboven ook een ideaal van een open, gemeenschappelijke en zelfregulerende ruimte. Denk bijvoorbeeld aan de *Declaration of the Independence of Cyberspace* van J.P. Barlow uit 1996:

*"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."*⁸⁵

Meer gematigde stemmen argumenteren daarentegen dat het internet wel gereguleerd moet worden, maar dan niet alleen door staten. De regels moeten uitgaan van de rechtstreeks belanghebbenden, inclusief de industrie en gebruikers.⁸⁶

Dat ideaal van het internet als een open en machtsvrije plek is vandaag moeilijk vol te houden.⁸⁷ Deze ommekeer versnelt in de jaren 2010 door het sterke marktoverwicht van bepaalde techbedrijven. Zo is de impact van techbedrijven, vaak ingebed in een zekere nationale politiek (of die nu Amerikaans, Chinees, Russisch of Europees is) onmiskenbaar. Het overwicht van bepaalde Amerikaanse techgiganten maakt het Europa alsmaar moeilijker om de eigen regels en waarden in de digitale sfeer te handhaven.⁸⁸ Daarom is het zinvol om na te denken over het vergroten van soevereiniteit in de digitale wereld, namelijk om vrij te doen in cyberspace wat we willen onder de (voor)waarden die we belangrijk vinden.

Verdiepend: Vrije en opensourcesoftware, en digitale soevereiniteit

⁸⁹ Z. Erlich (2007). "Open Source Software". Handbook of Research on Open Source Software. IGI Global. pp. 187–188.

⁹⁰ Zie hiervoor, bijvoorbeeld, de campagne van Free Software Foundation Europe: 'Public Money? Public Code!': <https://fsfe.org/activities/publiccode/index.en.html>

⁹¹ zie hiervoor het Open Source Initiative: <https://opensource.org/about>

⁹² De Duitse OSBA zet voor Europa hier vaak de toon: <https://osb-alliance.de/>

⁹³ In België is de voornaamste voortrekker hiervan BeLibre: <https://belibre.be/en/>

⁹⁴ Zie hiervoor: Kenniscentrum Data & Maatschappij, Verslag: Advancing Digital Sovereignty Initiatives in Belgium.' Hier beschikbaar: <https://data-en-maatschappij.ai/publicaties/verslag-advancing-digital-sovereignty-initiatives-in-belgium>

⁹⁵ M. Klare & U. Lechner (2025). 'Digital Sovereignty: Affordances in Open Source Projects.' In: Papatheocharous, E., Farshidi, S., Jansen, S., Hyrynsalmi, S. (eds) Software Business. ICSOB 2024. Lecture Notes in Business Information Processing, vol 539. Springer, Cham.

⁹⁶ Dit is de Open-Source Digital Ecosystems Strategy. Meer informatie: <https://digital-strategy.ec.europa.eu/en/news/commission-opens-call-evidence-open-source-digital-ecosystems>

In discussies rond digitale soevereiniteit wordt vaak gesproken over vrije en *opensource*software (FOSS). Opensourcesoftware is software waarvan de broncode van de softwaretoepassing vrij bekeken en aangepast kan worden; vrije software volgt de zogenaamde vier vrijheden, namelijk de vrijheid om:

- **Software te gebruiken**, voor eender welk doel
- **Software te bestuderen en aan te passen** aan je eigen behoeften
- **Software te delen** om anderen te helpen
- **Je aangepaste software te verspreiden** en te delen met de gemeenschap.⁸⁹

FOSS wordt vaak ontwikkeld en onderhouden door leden van de FOSS-gemeenschap en zijn daarom vaak minder commercieel ingesteld. Denk hierbij aan: Apache, PostgreSQL, MySQL, OpenSSL, Drupal, Git, NodeJS, Docker, Log4, Python, Kubernetes, PyTorch en JQuery. Afhankelijk van de licentie kan je meer of minder vrijheid genieten in het gebruik van FOSS.

FOSS taat tegenover *proprietaire software*, waarvan de broncode niet vrij beschikbaar is en bindende regels bestaan voor het gebruik en de verspreiding. Denk hierbij aan Microsoft Office, Adobe Photoshop en AutoCAD.

Verscheidene organisaties pleiten voor meer gebruik van FOSS. De *Free Software Foundation* – en haar Europese zusterorganisatie *Free Software Foundation Europe* – vertrekken hier vanuit de vrijheid van de gebruiker die controle moet hebben over de technologie. Daarenboven vinden deze organisaties dat technologie die (deels) ontwikkeld wordt door publiek geld, ook publiek beschikbaar moet zijn.⁹⁰ Andere organisaties pleiten eerder voor FOSS voor praktische voordelen, zoals snellere innovatie, betere interoperabiliteit en eenvoudigere samenwerking tussen ontwikkelaars.⁹¹ Daarnaast zijn er ook commerciële bedrijven die pleiten voor FOSS, vaak ondersteund door nationale Open Source Business Alliances (OSBA), die pleiten voor (hun eigen) FOSS omwille van lagere ontwikkelingskosten, snellere innovatie en eenvoudigere samenwerking.⁹²

Ten slotte pleiten sommige organisaties voor het gebruik van FOSS voor het bevorderen van digitale soevereiniteit⁹³ Voor hen is FOSS geen doel op zich of een middel om innovatie te stimuleren, maar een middel om vendor lock-in te voorkomen.⁹⁴ Uit onderzoek blijkt dat FOSS inderdaad een bijdrage kan leveren aan de digitale soevereiniteit van een organisatie, door te zorgen voor

- Meer transparantie omdat je kan zien hoe software werkt
- Minder afhankelijkheden van een leverancier die proprietaire software gebruikt
- Hogere aanpasbaarheid aan context of gebruikersbehoeften.⁹⁵

Ook de Europese Unie heeft recent een strategie uitgeschreven die sterk wil inzetten op FOSS voor de Europese digitale economie.⁹⁶

- Akilli, E. (2025). 'Forging the Digital Autonomy.' In: *Cognitive Diplomacy and Digital Autonomy*. Palgrave Macmillan, Cham.
- Bapna, R. et al. (2022). 'Single-Sourcing vs. Multisourcing: An Empirical Analysis of Large Information Technology Outsourcing Arrangements.' *Information Systems Research*, 34: 1109–1130.
- Battle, S. & van Waeyenberge, A. (2024). 'EU-US Data Privacy Framework: A First Legal Assessment.' *European Journal of Risk Regulation*, 15: 191–200.
- Beer, M. & Nohria, N. (2000). 'Cracking the code of change.' *Harvard Business Review*, mei-juni 2000, 78(3): 133–141, 216. PMID: 11183975.
- Bruford, E. et al. (2020). 'Guidelines for human gene nomenclature.' *Nature Genetics*, 52: 754–758.
- Chun, W. (2005). *Control and Freedom: Power and Paranoia in the Age of Fiber Optics*. Harvard, Ma.: The MIT Press.
- Couture, S. & Toupin, S. (2019). 'What does the notion of "sovereignty" mean when referring to the digital?' *New Media & Society*, 21: 2305–2322.
- Denardis, L. (2014). *The Global War for Internet Governance*. New Haven: Yale University Press.
- Erich, Z. (2007). 'Open Source Software.' *Handbook of Research on Open Source Software*. IGI Global, pp. 187–188.
- Falkner, G. et al. (2024). 'Digital sovereignty – Rhetoric and reality.' *Journal of European Public Policy*, 31: 2099–2120.
- Fratini, S. et al. (2024). 'Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models.' *Digital Society*, 3: 1–27.
- Godefroid, M. et al. (2022). 'How to measure the status quo bias? A review of current literature.' *Management Review Quarterly*, 73: 1667–1711.
- Klare, M. & Lechner, U. (2025). 'Digital Sovereignty: Affordances in Open Source Projects.' In: Papatheocharous, E., Farshidi, S., Jansen, S., Hyrynsalmi, S. (eds) *Software Business*. ICSOB 2024. Lecture Notes in Business Information Processing, vol 539. Springer, Cham.
- Krasner, S. D. (1999). *Sovereignty: Organized Hypocrisy*. Princeton University Press.

Marschall, J. (2025). 'The human factor: Why business tech projects fail and how to prevent.' *Qodea*, 6 maart 2025.

Mariotti, S. (2025). "'Open strategic autonomy" as an industrial policy compass for the EU competitiveness and growth: The good, the bad, or the ugly?' *Journal of Industrial and Business Economics*, 52: 1–26.

Mayer, M. & Lu, Y.-C. (2022). *Digital Autonomy? Measuring the Global Digital Dependence Structure*. Bonn: Center for Advanced Security, Strategic and Integration Studies.

Mbuba, F. et al. (2014). 'Software as a Service Adoption: Impact on IT Workers and Functions of IT Department.' *Journal of Internet Technology*, 15: 103–114.

Michaels, E. & Sus, M. (2024). '(Not) Coming of age? Unpacking the European Union's quest for strategic autonomy in security and defence.' *European Security*, 33(3): 383–405.

Mueller, M. (2020). 'Against Sovereignty in Cyberspace.' *International Studies Review*, 22: 779–801.

O'Hara, K. & Hall, W. (2018). *Four Internets: The Geopolitics of Digital Governance*.

Opara-Martins et al. – (zie ook algemene literatuur over vendor lock-in, niet expliciet in voetnoten maar relevant voor verdere lectuur)

Penttinen, R.-K. et al. (2023). 'The Vicious Circles of Skill Erosion: A Case Study of Cognitive Automation.' *Journal of the Association for Information Systems*, 24: 1378–1412.

Pohle, J. & Thiel, T. (2020). 'Digital sovereignty.' *Internet Policy Review*, 9(4).

Pohle, J. et al. (2024). 'Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices.' *Policy & Internet*, 16: 666–671.

Repetto, S. (2025). 'Concept "Stretching" or Concept Innovation? A Review of the Usages of Sovereignty in the Digital Sovereignty Literature.' *Policy & Internet*. <https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.70011>

Saghafian, M. et al. (2021). 'Stagewise Overview of Issues Influencing Organizational Technology Adoption and Use.' *Frontiers in Psychology*, 12: 630145.

Shirish, A. (2021). 'Technology renewal, user resistance, user adoption: status quo bias theory revisited.' *Journal of Organizational Change Management*. <https://doi.org/10.1108/JOCM-10-2020-0332>

Smicek, N. (2016). *Platform Capitalism*. Polity Press.

Wetgeving, beleidsdocumenten en officiële EU/overheidsbronnen

Europese Commissie (2013). *Towards a more competitive and efficient defence and security sector*. Communication from the Commission.

Europese Commissie (2020). *Europe's moment: Repair and Prepare for the Next Generation*. COM(2020) 456 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0456&from=en>

Europese Commissie (2021). *Trade Policy Review – An Open, Sustainable and Assertive Trade Policy*. COM(2021) 66 final.

Europese Commissie: Directorate-General for Research and Innovation (2025). *Open for startups & scaleups – EU startup and scaleup strategy making Europe a startup powerhouse*. Publications Office of the European Union.

Europese Commissie, Directorate-General for Digital Services (2025, 20 oktober). *Cloud sovereignty framework* (Version 1.2.1). Publications Office of the European Union. https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en

Europese Commissie (2026). *Proposal for a Regulation on ENISA, the European cybersecurity certification framework, and ICT supply chain security (repealing Regulation (EU) 2019/881), "Cybersecurity Act 2"*. COM(2026).

European Digital Infrastructure Consortium – EDIC. <https://digital-strategy.ec.europa.eu/en/policies/edic>

European External Action Service (2016). *Shared vision, common action: a stronger Europe. A global strategy for the European Union's foreign and security policy*. https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf

European Investment Bank (2024). *The scale-up gap: Financial market constraints holding back innovative firms in the European Union*.

European Union (2022). *Declaration for European Digital Sovereignty*. Brussels.

Elysée (2025, 18 november). *Summit on European Digital Sovereignty Delivers Landmark Commitments for a More Competitive and Sovereign Europe*. <https://www.elysee.fr/en/emmanuel-macron/2025/11/18/summit-on-european-digital-sovereignty-delivers-landmark-commitments-for-a-more-competitive-and-sovereign-europe>

European Data Protection Supervisor (EDPS) (2024). *Decision of the European Data Protection Supervisor following its investigation into the European Commission's use of Microsoft 365*.

European Data Protection Supervisor (EDPS) (2025). *Letter to Commission of July 11th, 2025*. https://www.edps.europa.eu/system/files/2025-07/25-07-11_letter-to-commission_2021-0518_en.pdf

Hof van Justitie van de EU. Case C-362/14, *Schrems v Data Protection Commissioner*, EU:C:2015:650.

Hof van Justitie van de EU. Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems*, EU:C:2020:559.

Homeland Security (2020). *Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China*.

Kenniscentrum Data & Maatschappij (2026). 'Data Act: Vijf vragen die elke onderneming zich moet stellen.' https://data-en-maatschappij.ai/uploads/Data-Act_5_vragen_KDM.pdf

Kenniscentrum Data & Maatschappij. *Verslag: Advancing Digital Sovereignty Initiatives in Belgium*. <https://data-en-maatschappij.ai/publicaties/verslag-advancing-digital-sovereignty-initiatives-in-belgium>

Rechtbank Amsterdam, afdeling privaatrecht. *Stichting Bits of Freedom tegen Facebook Netherlands, Meta Platforms Ireland LTD. en Meta Platforms Inc*, zaaknummer C/13/774725/KG ZA 25-687 MK/JD.

Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS2-richtlijn); omgezet in België via de wet van 26 april 2024 ("wet NIS2").

Verordening (EU) 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens (Algemene Verordening Gegevensbescherming, AVG), art. 28.

Verordening (EU) 2023/2854 van 13 december 2023 betreffende geharmoniseerde regels inzake een eerlijke toegang tot en gebruik van data (Data Act), art. 29, Pb.L. 2023, L 2854.

Vlaams Parlement, plenaire vergadering. 'Toespraak van Henna Virkkunen,' 3 februari 2026.

Vlaams Parlement, Commissie Algemeen Beleid, Financiën, Begroting, Justitie en Onroerend Erfgoed. Diependaele, M., Vraag om uitleg 2113 (2025_2026).

VN Zeerechtverdrag (1982), art. 89; VN-Ruimteverdrag (1967), art. 2.

Rapporten van consultancy- en marktonderzoeksbureaus

Cisco (2017). 'Single versus multiple vendors: Asking the right questions.'

Cisco (2026). 'A Shifting Paradigm: Governance in the Age of AI.'

Datanyze (2026). 'Office Suites Software Market Share.' <https://www.datanyze.com/market-share/office-suites--370>

Gartner (2025). 'Gartner reveals top technologies shaping government AI adoption,' 9 september 2025.

Gartner (2025). 'Magic Quadrant for Strategic Cloud Platform Services.'

IBRS (2021). 'The Economic Impact of Software as a Service in Australia.'

Insikt Group (2025). 'H1 2025 Malware and Vulnerability Trends.' <https://assets.recordedfuture.com/insikt-report-pdfs/2025/cta-2025-0828.pdf>

KPMG (2025). 'Cloud Monitor 2025: Digital sovereignty begins in the cloud – how companies create innovation, security and trust.' <https://assets.kpmg.com/content/dam/kpmg/tr/pdf/2025/10/kpmg-cloud-monitor-2025-consulting.pdf>

Market.us Scoop (2026). 'Video Conferencing Statistics By Connecting Technology (2026).' <https://scoop.market.us/video-conferencing-statistics/>

McKinsey & Company. 'Sovereign AI: Building ecosystems for strategic resilience and impact.'

McKinsey Blog (2026). 'What leaders need to know about building tech resilience amid geopolitical risk,' 20 februari 2026.

OECD (2022). *OECD Handbook on Competition Policy in the Digital Age*.

OECD (2025). *OECD Supply Chain Resilience Review: Navigating Risks*. https://www.oecd.org/en/publications/oecd-supply-chain-resilience-review_94e3a8ea-en.html

Resonate (2026). 'HubSpot Market Share 2026: CRM Share, Revenue & Customers.' <https://www.resonatehq.com/blog/hubspot-market-share>

Stolwijk, C. et al. (2023). *Digital Sovereignty: How Europe Takes Back Control. The Opinion of European Digital Leaders*. TNO. <https://publications.tno.nl/publication/34640695/aPvPww/TNO-2023-digital.pdf>

Synergy Research Group (2026). 'Cloud Market Share Q1 2026: AWS, Microsoft, Google Battling In AI Era.' <https://www.crn.com/news/cloud/2026/cloud-market-share-q1-2026-aws-microsoft-google-battling-in-ai-era>

Nieuws- en opiniestukken

'8 in 10 Europeans don't trust US, Chinese firms with data.' *Politico*, 10 april 2026.

'Berichten-app Telegram komt in Europa onder Belgisch toezicht.' *VRT NWS*, 6 mei 2024.

Bythepulse (2026). 'European vs US SaaS Tools 2026: Privacy-First Wins Complete Analysis.' <https://bythepulse.io/european-vs-us-saas-2026/>

Clifton, B. (2025). 'Schrems III – how likely is it and how to be prepared.' <https://briancclifton.com/blog/2025/05/19/schrems-iii-how-likely-and-how-to-prepare/>

'Commission fines Google €890 million for breaches of the Digital Markets Act.' *European Commission News*, 23 juli 2026.

'Commission fines X EUR 120 million under the Digital Services Act.'

'DNIP Briefing #48: Dokumentierte Überwachung.' *DNIP*, 4 november 2025. <https://dnip.ch/2025/11/04/dnip-briefing-48-dokumentierte-ueberwachung/>

'EU Moves Against TikTok's "Addictive Design."' *The European Times*, 10 april 2026.

'EU-US Data Privacy Framework in 2026: What Organizations Need to Know.' *GlobalDataShield*, 27 maart 2026.

Gur, B. (2024). 'Resilient Connectivity: SpaceX's Stellar Solution for Gaza's Internet Amid Conflict.' <https://directionsblog.eu/resilient-connectivity-spacexs-stellar-solution-for-gazas-internet-amid-conflict/>

'Interview: Zeggenschap en controle over data terugpakken.' *DSR Magazine*, februari 2026. <https://www.dsnews.eu/magazine-nl/editie-01-2026/zeggenschap-en-controle-over-data-terugpakken-0118/>

'Iran Targets Big Tech, Expands War Beyond Battlefields.' *Analytics Insight*, 1 april 2026.

'Life without US tech.' *The Big Read Technology Sector*, *Financial Times*, 11 mei 2026.

'Meta negeert uitspraak Nederlandse rechter over algoritme.' *VPN Nederland*, 24 oktober 2025.

Michelotti, A. (2025). 'Concentration of Power in the Broligarch Era.' *Tech Policy Press*. <https://www.techpolicy.press/concentration-of-power-in-the-broligarch-era/>

'Microsoft admits it "cannot guarantee" data sovereignty.' *The Register*, 25 juli 2025.

'Microsoft expands its Sovereign Cloud as Europe demands greater data control.' *Windows Central News*, 17 juni 2025.

'She Spoke Out About Gaza. Now She Can't Use a Credit Card.' *Politico*, 30 maart 2026.

'SpaceX curbed Ukraine's use of Starlink internet for drones – company president.' *Reuters*, 9 februari 2023.

'Statement on the US government directive to suspend access to Fable 5 and Mythos 5.' *Anthropic website*, 12 juni 2026. <https://www.anthropic.com/news/fable-mythos-access>

'"Chinese kill switches" found in Chinese-made power inverters in US solar farm equipment...' *Security Affairs*, 18 mei 2025.

'The Invisible Cage: How Cloud Vendor Lock-In Threatens European Digital Sovereignty.' *Sovereign Sky blog*, z.d.

'What the CLOUD Act Really Means for EU Data Sovereignty.' *Wire*, 15 juli 2025.
'X appeals \$140M penalty from the EU Commission.' *Social Media Today*, 22 februari 2026.

Overige online bronnen

BeLibre (België). <https://belibre.be/en/>

Free Software Foundation Europe. 'Public Money? Public Code!' <https://fsfe.org/activities/publiccode/index.en.html>

Open Source Business Alliance (OSBA, Duitsland). <https://osb-alliance.de/>

Open Source Initiative. <https://opensource.org/about>

Open-Source Digital Ecosystems Strategy, Europese Commissie. <https://digital-strategy.ec.europa.eu/en/news/commission-opens-call-evidence-open-source-digital-ecosystems>

Vignoli, I. (z.d.). 'FOSS and Open Standards for Digital Sovereignty.' <https://www.scribd.com/document/489531856/FOSS-and-Open-Standards-for-Digital-Sovereignty>

VLAIO. 'Financiële steun voor AI en digitalisering.' <https://www.vlaio.be/nl/begeleiding-advies/digitalisering/artificiele-intelligentie/advies-begeleiding-en-financiele-steun/financiele-steun-voor>

Barlow, J.P. (1996). *A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation. <https://www EFF.org/cyberspace-independence>

Colofon

De Visiepaper digitale soevereiniteit als richting voor een veerkrachtige onderneming is een publicatie van het Kenniscentrum Data & Maatschappij (KDM) voor publieke en private organisaties die willen werken aan digitale soevereiniteit.

Publicatiejaar

2026

Vanden Auweele, D. (2026), Digitale soevereiniteit als richting voor een veerkrachtige onderneming.

De auteur is bereikbaar via:

dennis.vanden.auweele@vub.be

Voor de ontwikkeling van deze visiepaper zijn we vertrokken van eigen inzichten aangevuld met:

- Inzichten uit workshops en co-creatiesessies, georganiseerd door het Kenniscentrum Data & Maatschappij.
- Inzichten uit de wetenschappelijke literatuur
- Gesprekken met strategische stakeholders.

Dit werk is voornamelijk door een mens gemaakt. AI werd gebruikt voor stilistische aanpassingen, zoals wijzigingen in structuur, woordkeuze en duidelijkheid. AI werd aangestuurd voor haar bijdragen, of AI-assistentie werd ingeschakeld. AI-gegenereerde inhoud werd nagekeken en goedgekeurd. De volgende model(len) of applicatie(s) werden gebruikt: Claude Sonnet 5.

Verantwoordelijke Uitgever

Pieter Duysburgh
Kenniscentrum Data & Maatschappij
Pleinlaan 2
1050 Brussel
info@data-en-maatschappij.ai

Dit rapport is beschikbaar onder een [Creative Commons CC BY-NC-ND 4.0 licentie](#).

data-en-maatschappij.ai
↑