AT COMPUTING

ATYPICAL OPEN SOURCE GURUS

CHECKLIST IT-SOEVEREINITEIT

Inventariseer de (on)afhankelijkheid van jouw IT-landschap

v1.01 || 3-12-2025

Checklist Soevereiniteit

Soevereiniteit van IT is al jaren een belangrijk gespreksonderwerp van diverse vooraanstaande IT-specialisten. Het onderwerp werd echter niet met hoge urgentie behandeld, omdat het gevoel overheerste dat Nederlandse data opslaan in applicaties en cloud-omgevingen van (bijvoorbeeld) Amerikaanse partijen veilig en betrouwbaar genoeg was.

Sinds Donald Trump begin 2025 is gestart aan zijn tweede termijn als president van de Verenigde Staten én het overduidelijk is dat er diverse landen zijn die zeer actieve en offensieve cyberprogramma's voor onder andere spionage voeren, is soevereiniteit wél een hot topic.

Deze checklist helpt je om de soevereiniteit van jouw IT-landschap in kaart te brengen. Aan de hand van 50 vragen, verdeeld over 5 categorieën, krijg je een genuanceerd beeld bij de huidige status: waar ben je al soeverein en waar nog niet? Met dit beeld kun je vervolgens strategische keuzes maken en adequaat aan risicobeheersing doen. In sommige gevallen is het immers helemaal niet zo erg om niet soeverein te zijn, als je er maar bewust voor kiest.

Laten we echter, voordat we meteen de checklist induiken, eerst eens op een rij zetten wat we precies met (IT) soevereiniteit bedoelen.

Wat is soevereiniteit precies?

Soevereiniteit betekent volgens Van Dale "oppermachtige heerschappij". Dat klinkt vrij dominant en is dus, afhankelijk van de context, zeker niet altijd positief.

Wanneer we in de context van IT over soevereiniteit spreken, dan bedoelen we in welke mate je controle (oppermachtige heerschappij) hebt over jouw applicaties, je data en je bijbehorende infrastructuur (netwerk, storage, compute).

IT-soevereiniteit gaat dus een stuk verder dan simpelweg al je applicaties en bijbehorende data ergens in Nederland stallen. Want wat als jouw leverancier plots wordt overgenomen door een *"kwaadaardige"* (buitenlandse) partij? Kun je dan eenvoudig je data oppakken en wegwezen? Wie heeft er toegang tot jouw data? En als jouw data is voorzien van encryptie: wie hebben de sleutels?

IT-soevereiniteit betekent dus...

Hoe vrij ben je om met jouw IT-landschap, applicaties en bijbehorende data precies te doen wat jij wilt?

- Hoeveel controle heb je erover?
- Waar zitten eventueel beperkingen?

Vijf kernaspecten van soevereiniteit

Om het antwoord op de vraag *"Hoe soeverein ben ik?"* onderbouwd te kunnen geven, hanteren we voor deze checklist 5 aspecten die hierbij volgens ons van essentieel belang zijn:

Data-soevereiniteit: waar staat jouw data precies opgeslagen en onder welke (juridische) voorwaarden?

Applicatie-soevereiniteit: in hoeverre heb je invloed op de ontwikkeling van de door jou gebruikte applicaties (bijv. zelf ontwikkeld of SaaS, open source of propriëtair?)

Infrastructuur-soevereiniteit: Wie beheert en controleert de infrastructuur (eigen beheer of ben je afhankelijk van een leverancier?)

Juridische soevereiniteit: op welke data en/of infrastructuur is welke wet- en regelgeving van toepassing? Is dat EU-wetgeving? NL-wetgeving? VS-wetgeving?

Operationele soevereiniteit: hoeveel vrijheid heb je om jouw data en applicaties te migreren/verhuizen of aan te passen?

Open source software (OSS)

Een soms onderbelicht onderwerp binnen de discussie over soevereiniteit is de beschikbaarheid van de broncode van applicatie(s), framework(s), module(s) of libraries die worden gebruikt.

De realiteit is echter simpel: **zonder toegang tot de broncode is volledige (applicatie-)soevereiniteit niet mogelijk**, want je kunt niet met zekerheid weten of vaststellen wat er precies in de code gebeurt als je die niet kunt inzien.

Ook zijn de mogelijkheden om aanpassingen te maken beperkt, want alleen degene met toegang tot de broncode kan dit doen.

Daarnaast zie je vaak dat de verdienmodellen rondom propriëtaire (gesloten) software ook voor een lock-in zorgen, waarbij eenvoudig migreren naar een andere applicatie niet (altijd) mogelijk is.

Dit kan bijvoorbeeld zijn vanwege:

- Beperkte export-functionaliteit
    - Quota (download-limieten)
    - Gesloten (propriëtaire) API's
    - Extra kosten voor dataverkeer ("egress fees", zoals vaak het geval is bij downloaden uit de cloud)
- Licentiestructuur (duurdere licentie nodig voor export-functionaliteit)
- Het gebruik van non-standaard / niet open formaten voor data-opslag

Open source ≠ soevereiniteit

We zijn bij AT Computing groot fan van OSS, maar nuance aanbrengen is ook op dit vlak belangrijk. Hoewel je niet soeverein kunt zijn zonder toegang tot de broncode, betekent dit niet dat je altijd soeverein bent wanneer je alleen maar OSS gebruikt. Ook bij OSS kun je afhankelijkheid van leveranciers (vendors) hebben en komt het geregeld voor dat er trammelant ontstaat binnen een open source project.

Denk aan licentiewijzigingen (door bijvoorbeeld Red Hat, HashiCorp en Elastic), forks (MySQL en MariaDB) of wijzigingen in de feature-parity tussen Community Edition (CE) en Enterprise Edition (EE) zoals bij Docker of GitLab.

Ook kan het voorkomen dat een project ineens met bepaalde distributiekanalen stopt. Zo besloot MinIO in 2025 niet langer een officieel container-image op Docker Hub te publiceren. Allemaal OSS, maar vanuit soevereiniteit wel degelijk met de nodige aandachtspunten en uitdagingen!

Een volgend punt van aandacht is het (cloud) platform waarop je jouw OSS draait. Als je over dit platform geen controle hebt, zoals een public cloud omgeving of propriëtaire virtualisatie-oplossing van een buitenlandse leverancier, dan ben je alsnog niet soeverein.

Een laatste aspect dat vaak wordt vergeten, is de governance van een open source project. Wie bestuurt het open source project? Is dat één (commerciële) partij of is er sprake van een stichting (foundation) waarin onafhankelijk eigenaarschap van het project is geborgd (ook wel steward-ownership)? En wat doe je als een project wegens een conflict wordt geforked?

De checklist

Op basis van de vijf genoemde aspecten, behandelen we vier niveaus van soevereiniteit. Per niveau kun je door het invullen van de checklist weergeven hoe soeverein je op dit niveau wel/niet bent.

Belangrijk: zie de niveaus en bijbehorende tabel niet als exacte wetenschap, maar als een leidraad. Het kan zomaar zijn dat jouw IT-omgeving van alles een beetje bevat en je dus niet zonder meer kunt stellen dat je met de hele spullenboel op hetzelfde niveau zit.

De niveaus en criteria helpen echter wel bij het classificeren van je landschap en bij discussies over bijvoorbeeld risicobeheersing en bij strategische afwegingen. Hierdoor ben je beter instaat de juiste beslissingen te nemen en adequate maatregelen te treffen.

Hoe vul je de tabellen in?

Iedere tabel bevat 10 aspecten, die ieder een gewicht hebben meegekregen. Belangrijke soevereiniteits-aspecten hebben hierdoor meer invloed op de eindscore dan minder belangrijke aspecten. Het maximale gewicht van een aspect is 3, het minimale gewicht is 1.

Het kan zijn dat je gedeeltelijk aan een aspect voldoet. Zo kan bijvoorbeeld een deel van je data fysiek zijn opgeslagen binnen de EU, maar niet alles. In dat geval ken je een deel van de punten toe. Ga hier als volgt mee om:

- **Voldoe je volledig?** -> ken de maximale score toe
- **Voldoe je voor een aanzienlijk deel** (bijv. >50%) -> ken max. gewicht - 1 toe (dus 2 ipv 3, 1 ipv 2 of 0 ipv 1)
- **Voldoe je minimaal of nauwelijks** -> ken een score van 1 toe bij max. gewicht 3 of 0 bij max. gewicht 1 of 2
- **Voldoe je in geheel niet?** -> ken een score van 0 toe

Is het antwoord onbekend, doe dan eerst een stuk onderzoek of vul 0 in. Onbekend is immers per definitie een risico!

Voorbeeld

max. 11 punten

Nr	Aspect	Gewicht	Score
1	Alle data staat fysiek opgeslagen binnen de EU	3	*2*
2	Data valt uitsluitend onder EU-wetgeving	3	*1*
3	Broncode/configuratie is inzichtelijk (geen black box)	2	*1*
4	Data is versleuteld tijdens transport (TLS 1.2+)	2	*2*
5	Logging/monitoring draait volledig binnen de EU	1	*0*
	Totale score:		**6**

Data-soevereiniteit

max. 20 punten

Nr	Aspect	Gewicht	Score
1	Alle data staat fysiek opgeslagen binnen de EU	3	
2	Data valt uitsluitend onder EU-wetgeving	3	
3	Data is versleuteld opgeslagen (encryption at rest)	2	
4	Data is versleuteld tijdens transport (TLS 1.2+)	2	
5	Encryptiesleutels volledig in eigen beheer	3	
6	Geen toegang door derde landen (Cloud Act-proof)	3	
7	Data-locatie is aantoonbaar en transparant	1	
8	Dataclassificatiebeleid bestaat en wordt toegepast	1	
9	Data kan 100% geëxporteerd worden zonder verlies	1	
10	Leverancieronafhankelijk back-upbeleid	1	
	Totale score:		

Applicatie-soevereiniteit

max. 20 punten

Nr	Aspect	Gewicht	Score
1	Applicaties zijn open source of eigen ontwikkeling	3	
2	Broncode/configuratie is inzichtelijk (geen black box)	2	
3	Software gebruikt open standaarden	2	
4	Applicaties zijn volledig portable tussen platformen	3	
5	Open API's zonder *vendor lock-in*	2	
6	Leverancier ondersteunt data-portabiliteit	1	
7	Voldoet aan EU/NL security- en compliance-eisen	2	
8	Updates/patches onafhankelijk uitvoerbaar	1	
9	Geen afhankelijkheid van niet-EU applicatielogica	2	
10	Geen afhankelijkheid van Amerikaanse cloudservices	2	
	Totale score:		

Infrastructuur-soevereiniteit

max. 20 punten

Nr	Aspect	Gewicht	Score
1	Infrastructuur staat volledig binnen de EU	3	
2	Eigendom én beheer zijn 100% Europees	3	
3	Geen afhankelijkheid van één IaaS-provider	2	
4	Workloads zijn eenvoudig verplaatsbaar naar andere providers	2	
5	Infrastructuur gebruikt open standaarden	2	
6	Geen Amerikaanse moederbedrijven in de keten	3	
7	Logging/monitoring draait volledig binnen de EU	1	
8	End-to-end encryptie in eigen beheer	2	
9	Containerplatform/VM's zijn portable (bijv. Kubernetes)	1	
10	Continuïteitsplan is onafhankelijk van leverancier	1	
	Totale score:		

Juridische soevereiniteit

max. 20 punten

Nr	Aspect	Gewicht	Score
1	Geen extraterritoriale wetgeving toepasbaar	3	
2	Contracten/SLA's volledig onder EU/NL-recht	3	
3	Leverancier heeft geen verplichtingen richting buitenlandse overheden	3	
4	Volledige transparantie over jurisdictie en eigendom	2	
5	Geen risico op Cloud Act / FISA / Patriot Act	3	
6	Duidelijke juridische exit-clausules aanwezig	2	
7	Dataportabiliteit juridisch geborgd	1	
8	Data-soevereiniteit contractueel vastgelegd	1	
9	Juridische audits mogelijk	1	
10	Juridische risicoanalyse aanwezig	1	
	Totale score:		

Operationele soevereiniteit

max. 20 punten

Nr	Aspect	Gewicht	Score
1	Exit-strategie beschikbaar én getest	3	
2	Data-portabiliteit technisch gegarandeerd	3	
3	Meerdere leveranciersopties beschikbaar	2	
4	Eigen beheer mogelijk zonder leverancier-specifieke tooling	2	
5	Interne controle over alle toegangsmechanismen	3	
6	Aanwezige skills voor zelfstandig beheer	2	
7	Volledige documentatie intern beschikbaar	1	
8	Multi-cloud/hybrid strategie voorkomt lock-in	1	
9	Geen afhankelijkheid van propriëtaire automation/tooling	1	
10	Monitoring/observability onafhankelijk te draaien	2	
	Totale score:		

Eindscore

max. 100 punten

Nr	Aspect	Score
1	Data-soevereiniteit	
2	Applicatie-soevereiniteit	
3	Infrastructuur-soevereiniteit	
4	Juridische soevereiniteit	
5	Operationele soevereiniteit	
	Eindscore:	

Conclusie op basis van eindscore

	Eindscore	Conclusie
🟢	>75 punten	Goed bezig! De IT-omgeving is grotendeels soeverein!
🟡	50-75 punten	Delen van de IT-omgeving zijn soeverein, maar er is nog volop ruimte voor verbetering.
🟠	25-50 punten	Er is sprake van enige soevereiniteit, maar er zijn diverse punten met sterke afhankelijkheden.
🔴	<25 punten	De IT-omgeving is nauwelijks soeverein. Er is grote afhankelijkheid van leveranciers en statelijke actoren.

Tot slot: trends en ontwikkelingen

Digitale soevereiniteit krijgt gelukkig steeds meer aandacht op zowel Europees als nationaal niveau.

Grote internationale spelers zoals Microsoft, Oracle en Amazon lanceren *"soevereine"* cloudoplossingen. Daarmee spelen zij in op Europese zorgen, maar tegelijk blijft de vraag hoeveel zeggenschap Europa werkelijk heeft zolang het eigendom in Amerikaanse handen blijft.

In sommige gevallen kan juridisch *ontkoppeld* worden van een Amerikaanse moedermaatschappij, waarmee bepaalde wetgeving niet meer van toepassing is. De vraag is echter in hoeverre de dienstverlening daarna betrouwbaar blijft wanneer er wegens sancties vanuit bijvoorbeeld de Amerikaanse of Chinese overheid geen patches of updates meer beschikbaar worden gesteld vanuit diezelfde moedermaatschappij.

Waakzaamheid voor pseudo- of schijn-soevereiniteit is hier op zijn plaats, want er wordt door diverse cloud- en hosting-leveranciers *sovereignty washing* toegepast, waarbij geschermd wordt dat een product of dienst soeverein is, terwijl dat feitelijk niet zo blijkt te zijn.

Ook stelt de Amerikaanse Cloud Act simpelweg dat de nationaliteit van de *onderneming* die de software of clouddienst levert leidend is voor data-inzage, niet het land waar het datacenter zelf gevestigd is of waar de data is opgeslagen.

In Nederland groeit de politieke druk om meer grip (autonomie) te krijgen op kritieke IT-systemen:

- Kamerlid **Barbara Kathmann (PvdA)** diende meerdere moties in om de afhankelijkheid van Amerikaanse cloud-partijen te verkleinen en Europese alternatieven te stimuleren
- Denk aan bijvoorbeeld projecten als **GaiaX**, **Mijn Bureau**, **Haven** of de inzet van Europese aanbieders als **OVH, Exoscale of Hetzner**
- De moties zijn stuk voor stuk met brede steun aangenomen
- Ook voormalig AIVD-toezichthouder en IT-expert **Bert Hubert** zet zich actief in om digitale autonomie en soevereiniteit hoger op de agenda te krijgen, onder meer door zijn bijdragen aan beleidsdiscussies en publieke debatten (met "Cloud Kootwijk" als beeldspraak)

Ook de sector zelf roert zich:

- De **Dutch Cloud Community** publiceerde een position paper waarin het pleit voor meer investeringen in Nederlandse en Europese cloud-capaciteit
- **IT Channel Pro** heeft soevereiniteit tot belangrijk thema verheven
- Ook open source brancheverenging **DOSBA** mengt zich in het debat

De trend is duidelijk: Soevereiniteit is geen theoretische exercitie meer, maar een urgente vraag waar politiek, bedrijfsleven, media en de samenleving gezamenlijk mee aan de slag moeten.

Contact & Services

AT Computing is vooral bekend vanwege haar trainingen, maar staat ook sinds 1985 klaar voor het leveren van diepgaande kennis over het gebruik van open source software binnen een IT-omgeving. Vanuit technisch perspectief kunnen we designs, configuratiescripts, infrastructuur of Python code reviewen, advies geven bij IT-uitdagingen of helpen bij het opzetten van een gestroomlijnde, geautomatiseerde workflow met bijvoorbeeld Ansible, Terraform, GitLab of Kubernetes. Ook voor advies over lokale LLM's voor GenAI toepassingen hebben wij expertise in huis. Vanuit governance- en risicomanagement perspectief kunnen we helpen bij het opstellen van open source software-beleid, advies geven over IT security, risicobeheersing en u helpen compliant te blijven zonder de voordelen van open source software op te geven.

Contact Information

AT Computing B.V.
Arnhemsestraatweg 33
6881ND Velp
The Netherlands

Email: info@atcomputing.nl
Phone: +31 (0)24 352 72 82
Web: https://atcomputing.nl