Why CIOs need to respond to **Digital Sovereignty now ?**

Regulations

The "Schrems II" Ruling

Privacy Commission tightens oversight of American cloud services

"The Belgian Data Protection Authority and its European counterparts are moving from text audits to technical verification. European companies can no longer hide behind standard contractual clauses (SCCs) if the technical reality allows foreign intelligence services potential access to European citizen data."

July 2020

Dora and NIS2

Digital security: how NIS2 and DORA push cyber risk onto board agendas

With the strict implementation of NIS2 and DORA, digital risk has officially graduated to the boardroom. Directors can now be held personally liable for systemic security failures and blind spots in their third-party supply chains. **Sovereignty is no longer a luxury** for public administrations; it is a legal requirement for enterprise survival.

December 2022

Regulations

The "Schrems II" Ruling

Privacy Commission tightens oversight of American cloud services

"The Belgian Data Protection Authority and its European counterparts are moving from text audits to technical verification. European companies can no longer hide behind standard contractual clauses (SCCs) if the technical reality allows foreign intelligence services potential access to European citizen data."

July 2020

Dora and NIS2

Digital security: how NIS2 and DORA push cyber risk onto board agendas

With the strict implementation of NIS2 and DORA, digital risk has officially graduated to the boardroom. Directors can now be held personally liable for systemic security failures and blind spots in their third-party supply chains. **Sovereignty is no longer a luxury** for public administrations; it is a legal requirement for enterprise survival.

December 2022

Risk awareness

Security.NL

"We zijn als Nederlandse samenleving allemaal Microsoft-verslaafd op dit moment

Het is niet zo dat je van de ene op de andere dag alternatieven hebt. Maar we zullen in ieder geval moeten streven naar meer soevereiniteit." - Staatssecretaris Van der Burg (Koninkrijksrelaties en Slagvaardige Overheid)

May 2026

Parlement

Federale IT-infrastructuur pijnlijk afhankelijk van Amerikaanse techreuzen

De federale overheid raakt steeds vaster verstrikt in de netten van Amerikaanse cloudleveranciers. Vitale overheidsdiensten kunnen bij een geopolitiek conflict binnen 48 uur operationeel verlamd worden. We hebben de sleutels van onze digitale schatkist aan Washington gegeven.

February 2026

Regulations

The "Schrems II" Ruling

Privacy Commission tightens oversight of American cloud services

"The Belgian Data Protection Authority and its European counterparts are moving from text audits to technical verification. European companies can no longer hide behind standard contractual clauses (SCCs) if the technical reality allows foreign intelligence services potential access to European citizen data."

July 2020

Dora and NIS2

Digital security: how NIS2 and DORA push cyber risk onto board agendas

With the strict implementation of NIS2 and DORA, digital risk has officially graduated to the boardroom. Directors can now be held personally liable for systemic security failures and blind spots in their third-party supply chains. **Sovereignty is no longer a luxury** for public administrations; it is a legal requirement for enterprise survival.

December 2022

Oversight

Gegevens Bescherming Authoriteit

The Data Protection Authority toughens its stance on the American Cloud Act

A contract stating that data remains in Brussels is worthless if a US judge can use a secret warrant to compel the parent company to hand over the encryption keys. Belgian CIOs must transition to BYOK (Bring Your Own Key) or risk multimillion-euro fines under NIS2.

December 2025

Risk awareness

Security.NL

"We zijn als Nederlandse samenleving allemaal Microsoft-verslaafd op dit moment

Het is niet zo dat je van de ene op de andere dag alternatieven hebt. Maar we zullen in ieder geval moeten streven naar meer soevereiniteit." - Staatssecretaris Van der Burg (Koninkrijksrelaties en Slagvaardige Overheid)

May 2026

Parlement

Federale IT-infrastructuur pijnlijk afhankelijk van Amerikaanse techreuzen

De federale overheid raakt steeds vaster verstrikt in de netten van Amerikaanse cloudleveranciers. Vitale overheidsdiensten kunnen bij een geopolitiek conflict binnen 48 uur operationeel verlamd worden. We hebben de sleutels van onze digitale schatkist aan Washington gegeven.

February 2026

Regulation as a Catalyst

Sovereignty & Data Governance: A regulatory avalanche:

Regulation / Law	Enforcing Authority	Sovereignty Impact	Penalties / Fines	Who is in Scope
CLOUD Act (US)	U.S. Department of Justice	U.S. jurisdiction overrides foreign sovereignty for data held by U.S. providers.	No explicit fines; contempt or sanctions for non-compliance.	U.S.-headquartered cloud and tech providers, their subsidiaries worldwide.
FISA §702 (US)	FISA Court / U.S. Department of Justice / FBI	Enables U.S. surveillance of non-U.S. persons' data on U.S. infrastructure.	No monetary fines; enforced via court orders.	U.S. electronic communication service providers.
Stored Communications Act (US)	U.S. Department of Justice	Warrant-based access to data stored by U.S. providers globally.	Criminal fines; imprisonment up to 5 years.	U.S. service providers storing communications.
GDPR (EU)	EU DPAs (e.g., CNIL, ICO)	Restricts transfers; enforces EU data localisation principles.	Up to €20M or 4% global turnover.	Any entity processing EU personal data (controllers & processors).
Schrems II (EU)	CJEU	Invalidated Privacy Shield; SCCs require risk assessment.	GDPR penalties apply.	Controllers/exporters transferring EU data.
NIS2 Directive (EU)	National cybersecurity authorities & ENISA	Resilience for critical digital infrastructure.	Up to €10M or 2% turnover (essential entities).	Operators of essential services, digital service providers, MSPs.
DORA (EU)	EU financial regulators	ICT resilience for financial ecosystem sovereignty.	Up to €5M for providers; individuals up to €1M.	Financial institutions, ICT third-party providers (incl. cloud).
ePrivacy Directive (EU)	National DPAs	Sovereignty control over electronic communications.	Up to €20M or 4% turnover.	Telecoms, ISPs, digital service providers.
UK Data (Use & Access) Act 2025	Information Commissioner's Office (ICO)	Defines UK-controlled data flows post-Brexit.	Up to £17M or 4% turnover.	UK-based controllers/processors.
FCA PS21/3 & PRA SS1/21 (UK)	Financial Conduct Authority (FCA) & Prudential Control Authority (PRA)	Operational resilience for UK financial sovereignty.	Multi-million fines, e.g. £48M for TSB.	Banks, insurers, payment firms, FMIs.
Cyber Security & Resilience Bill (UK)	DSIT & sector regulators	Expands UK cyber sovereignty to MSPs, data centres.	Up to £17M or 4% turnover; daily fines up to £100K.	MSPs, cloud providers, critical suppliers.
NIS Regulations 2018 (UK)	Sector regulators & National Cybersecurity Centre (NCSC)	Foundational UK cybersecurity law for essential services.	Up to £17M or 4% turnover.	Operators of essential services, DSPs.
Telecoms Security Act 2021 (UK)	Ofcom	Secures UK telecom sovereignty.	Up to 10% annual turnover.	Telecom operators, network providers.
Privacy Act 1988 (Australia)	Office of the Australian Information Commissioner (OAIC)	Sovereignty over personal data and breach reporting.	A$2.1M for corporate breaches.	Australian entities processing personal data.
Critical Infrastructure Act 2018 (Australia)	Sector regulators	Protects critical infrastructure sovereignty.	A$10M; criminal penalties.	Operators of critical infrastructure sectors.
Cloud and AI Development Act (CADA)	European Commission & EU Member State Regulatory Authorities	Defines 4 strict cloud sovereignty tiers (Level 1-4). Targets sovereign washing; Level 4 bans foreign interference entirely.	Exclusions from public procurement; fines tied to risk classifications.	Cloud service providers, AI developers, public sector bodies across the EU.

How is Sovereignty Defined
8 or 4 shades of grey ?

8 Sovereignty Objectives

European Commission: Cloud Soverignty Framework - October 2025

Strategic
Provider anchor within the EU legal and industrial ecosystem.

Legal
Immunity from extraterritorial claims (e.g. US Cloud Act).

Data & AI
Customer-exclusive cryptographic control and visibility.

Operational
Manage and maintain tech without non-EU vendor involvement.

Supply Chain
Transparency and origin of critical hardware components.

Technology
Adherence to open standards to prevent vendor lock-in.

Security
Alignment with ENISA, NIS2, and DORA frameworks.

Ecological
Long-term autonomy regarding energy and raw materials.

They draw on European initiatives such as CIGREF's Trusted Cloud Referential v2, Gaia-X policy rules and architecture, and the European Cybersecurity Certification Framework (ENISA, NIS2, DORA). In addition, they echo lessons from national cloud sovereignty strategies (e.g., France's "Cloud de Confiance", Germany's "Souveräner Cloud"), as well as international practices in export controls, supply chain resilience, and security auditability.

Sovereignty Effective Assurance Levels

From zero sovereignty to full digital autonomy

SOVEREIGNTY

SEAL-0 — **No Sovereignty**
Service, technology or operations under exclusive control of non-EU third parties, governed entirely in non-EU jurisdictions.

SEAL-1 — **Jurisdictional Sovereignty**
EU law formally applies with limited practical enforceability; service, technology or operations under exclusive control of non-EU third parties.

SEAL-2 — **Data Sovereignty**
EU law applicable and enforceable, with material non-EU dependencies remaining; service, technology or operations under indirect control of non-EU third parties.

SEAL-3 — **Digital Resilience**
EU law applicable and enforceable. EU actors exercising meaningful but not full influence; service, technology or operations under marginal control of non-EU third parties.

SEAL-4 — **Full Digital Sovereignty**
Technology and operations under complete EU control, subject only to EU law, with no critical non-EU dependencies.

Cloud Sovereignty in Practice

Mapping cloud deployment models to SEAL levels

SEAL-1 / SEAL-2

Standard Global Public Cloud

Microsoft Azure | AWS | Google Cloud Platform (GCP)

Even with European data centers, these services generally top out at SEAL-2. While EU data residency and encryption are provided, the underlying software, global admin access capabilities, and corporate parentage mean that material, indirect dependencies on non-EU entities remain.

EU data residency
but US corporate control

SEAL-3

Sovereign Cloud Enclaves & Partner Models

Microsoft Cloud for Sovereignty | AWS European Sovereign Cloud | S3NS (France) | Delos Cloud (Germany)

These models introduce strict operational boundaries, ensuring that day-to-day operations and metadata are handled exclusively by EU-based personnel, thereby limiting non-EU third-party intervention to a marginal, strictly audited level.

EU operations
audited non-EU involvement

SEAL-4

Fully Decoupled / Local Partner Stacks

OVHcloud | STACKIT| Outscale | Disconnected deployments

Technology and operations must be entirely immune to foreign extraterritorial laws (like the US Cloud Act). This requires complete legal, operational, and structural autonomy within the EU.

Full EU autonomy
no foreign legal reach

European Technological Sovereignty Package

Europe is putting in place a strategy to achieve technological sovereignty

Interconnected initiatives spanning chips, infrastructure, software, cloud and AI

1

Chips Act 2.0

Strengthen the semiconductor ecosystem and supply chain resilience, boost domestic demand

2

Cloud and AI Development Act (CADA)

Unlock the potential of AI and cloud to transform industrial ecosystems and improve societal outcomes

3

EU Open Source Strategy

Reduce dependencies across the entire technology stack

4

Strategic Roadmap for Digitalisation and AI in Energy

Accelerate digitalisation and AI deployment in the energy sector

EU or Not EU

Does that matter to you or your business ?

or should you focus on the answer to key control questions

- Where does the data live?
- Who controls the platform?
- Where are operations performed?
- Who has administrator access?
- Can evidence be produced on demand?

Sovereignty is about: who controls the system, who governs it and who can prove it under pressure