Move2Cloud

• WHITE PAPER — 2027 EDITION

EUROPEAN REGULATORY FRAMEWORK

Sovereign Cloud in Europe

The practical guide to understanding the new European regulatory framework (CADA, Cloud Sovereignty Framework, NIS2, DORA) and building a compliant, resilient and controlled cloud strategy.

11 pages · SEAL grid, roadmap and self-assessment included

48	€180M	SEAL 0→4
sovereignty criteria assessed	first European framework contract	assurance levels to know

PREPARED BY
Move2Cloud — Cloud & Infrastructure Consulting, Paris

PUBLICATION
September 2026

CONTENTS

What you will find in this document

A six-step journey, from understanding the regulatory framework to implementing an operational roadmap.

01 **Executive summary — the essentials on one page** p.3

02 **Why cloud sovereignty becomes a board-level issue** p.4

03 **The new European framework: CADA and Cloud Sovereignty Framework** p.5

04 **SEAL levels explained simply** p.6

05 **What the first €180M contract already tells us** p.7

06 **NIS2 and DORA: concrete impacts on your cloud architecture** p.8

07 **Self-assessment grid** p.9

08 **A 5-step roadmap** p.10

09 **Conclusion & about Move2Cloud** p.11

> **Who is this document for?** CIOs, CISOs, procurement departments and executives of French and European public or private organisations assessing their dependence on non-European cloud providers, or responding to tenders subject to sovereignty requirements.

EXECUTIVE SUMMARY

The essentials on one page

In 2026, cloud sovereignty moved from the realm of principles to that of public procurement award criteria and regulatory obligations.

Since April 2026, the European Commission has had an operational **Cloud Sovereignty Framework**: **48 criteria**, spread across **8 sovereignty objectives**, scored on a maturity scale called **SEAL** (Sovereignty Effectiveness Assurance Level, from SEAL-0 to SEAL-4). This framework has already been used to award a **180 million euro** contract over six years to four providers — three of them fully European and one, S3NS, still partly backed by American technology (Google Cloud), which has sparked debate about the framework's real reach.

In parallel, the proposed **Cloud and AI Development Act (CADA)**, presented in June 2026 as part of the AI Continent Action Plan, aims to **triple the Union's data centre capacity in five to seven years** and introduces its own four-level assurance system to classify providers according to the location and the effective control of data.

These initiatives do not replace obligations already in force: **NIS2** requires risk management, 24/7 detection and strict incident notification deadlines (**24h / 72h / 1 month**) for essential and important entities; **DORA** requires financial entities to rigorously manage the risk associated with third-party ICT providers, cloud included.

48
criteria across 8 sovereignty objectives (Cloud Sovereignty Framework)

€180M
first European framework contract awarded under this framework (April 2026)

×3
European data centre capacity targeted by CADA within 5 to 7 years

For a French organisation — local authority, public body, SME or mid-cap — the question is no longer "should we care about cloud sovereignty?" but "what SEAL level does my current architecture sit at, and what is the gap with the requirements of my contracts, my clients or my sector?". This document offers a pragmatic reading grid to answer it.

Copyright Move2Cloud — move2cloud.fr

SECTION 02

Why cloud sovereignty becomes a board-level issue

For a long time, digital sovereignty was treated as a legal or political concern, peripheral to architecture choices. Three shifts are reshuffling the cards in 2026 and turning it into a governance and business continuity issue.

1. European public procurement is taking it up in concrete terms

The Cloud Sovereignty Framework is no longer a statement of intent: it has been used as the evaluation grid to award a real contract. Public bodies bidding for European tenders, or buying from providers assessed against this framework, must now be able to position their suppliers on that scale.

2. Regulatory obligations are stacking up and overlapping

NIS2, DORA and the EU AI Act do not specifically target sovereignty, but they converge on the same operational requirements: mapping third-party dependencies, controlling concentration risk with a single provider, and demonstrating tested resilience. An organisation that handles these topics in silos multiplies the effort; one that handles them together, through a single architecture roadmap, significantly reduces the cost of compliance.

3. Dependency risk has stopped being theoretical

The regional infrastructure incidents that hit several hyperscalers in 2026 were a reminder that an architecture relying on a single zone or a single provider, however robust its contractual terms, remains exposed to a continuity risk. Sovereignty then meets the more classic question of resilience: supplier diversification, contractual reversibility, technical portability.

> *“ Data location is no longer enough to demonstrate sovereignty: what is now assessed is decision-making power. ”*

For any organisation exposed to these requirements — local authority, public body, SME or mid-cap — this translates into a simple question to ask today: in the event of an audit, a tender response or a regulatory inspection, would you be able to document the real level of sovereignty of your cloud architecture?

Copyright Move2Cloud — move2cloud.fr

SECTION 03

The new European framework: CADA and Cloud Sovereignty Framework

CADA, presented in June 2026 as part of the AI Continent Action Plan, aims to triple the Union's data centre capacity within five to seven years, while the Cloud Sovereignty Framework, operationally deployed in April 2026, assesses cloud providers against 48 precise criteria grouped into eight sovereignty objectives, each weighted differently in the final score.

SOVEREIGNTY OBJECTIVE	WEIGHT AND WHAT IS ASSESSED
Supply chain	20% — Provenance of the design, manufacturing and distribution of hardware and software.
Strategic	15% — Location and stability of authority, ownership and funding.
Operational	15% — Ability of European players to run and support the service autonomously.

> **Key takeaway:** The supply chain carries more weight than the legal location of data alone — a clear signal to providers that host in Europe without controlling the underlying hardware and software.

CADA's four assurance levels

CADA also introduces its own four-level assurance system, based on the location and the degree of control of data: Level 1 — hosting within the EU; Level 2 — independence from third countries and a transparent software supply chain; Level 3 — European ownership and control with enhanced security; Level 4 — full transparency and prevention of any third-country interference. The text addresses companies, cloud providers, investors, research organisations and public administrations, with reinforced support for sectors deemed strategic.

Copyright Move2Cloud — move2cloud.fr

SECTION 04

SEAL levels explained simply

A key point, often misunderstood: a provider does not receive a single SEAL score, but eight distinct scores, one per sovereignty objective.

LEVEL	DESIGNATION	CONTROL OVER THE INFRASTRUCTURE	SCOPE OF EUROPEAN LAW
SEAL-0	No sovereignty	Exclusive control by a non-EU player	Governance entirely outside European jurisdiction
SEAL-2	Data sovereignty	Significant non-EU dependencies remain	European law is enforceable
SEAL-4	Full digital sovereignty	Full control, with no non-EU dependency	Exclusively under European law

Common pitfall: A provider that announces "we are SEAL-3" without specifying which objective is involved says nothing verifiable — there is no SEAL certification or accreditation body. Only an assessment carried out by a public buyer within a procurement procedure produces an enforceable result; a self-assessment is worth no more than internal preparation. Likewise, hosting in Europe is not enough: what matters is the real decision-making authority over the infrastructure.

How the score is actually used in tenders

The mechanism relies on two successive steps. First, eliminatory floor thresholds: the public buyer sets a minimum SEAL level per objective, and a provider falling below any one of these thresholds is automatically ruled out, whatever its performance on the other criteria. Second, a weighted score to rank the remaining candidates: only providers that have cleared every threshold are then ranked according to the weighted score presented on the previous page.

SECTION 05

What the first €180M contract already tells us

In April 2026, the European Commission awarded a six-year, €180 million framework contract to four winners assessed under the Cloud Sovereignty Framework.

Four winners rather than one

The Commission's choice to split the contract between four winners — rather than designating a single provider — explicitly serves an objective of diversification and resilience, in order to avoid the lock-in that would result from dependence on a single supplier.

The S3NS case: a signal not to ignore

S3NS, a joint venture between France's Thales and Google Cloud (United States), was selected despite reaching only SEAL-2 — against SEAL-3 for the three other winners. The choice drew criticism over the framework's real ability to guarantee independence from US legal obligations, notably the Cloud Act.

Judging the reality, not the pitch

A local partnership or a commercial presence in France is not enough to qualify an offer as "sovereign" if the underlying technology and supply chain remain controlled by a non-European player. Scrutiny must bear on technical and legal reality, not only on the sales pitch.

WINNER	COMPOSITION AND SEAL LEVEL ACHIEVED
Franco-Luxembourg consortium	Post Telecom, OVHcloud, CleverCloud — SEAL-3
Belgian-French-Luxembourg consortium	Proximus, S3NS, Clarence, Mistral — SEAL-2

Copyright Move2Cloud — move2cloud.fr

SECTION 06

NIS2 and DORA: concrete impacts on your cloud architecture

These two texts are not sovereignty frameworks as such, but their operational requirements largely overlap with those of the Cloud Sovereignty Framework — hence the value of handling them in a single initiative.

NIS2: what your architecture must demonstrate

NIS2 calls for a documented risk register per workload, threat modelling and active 24/7 security detection on critical workloads (beyond simple performance monitoring); an early warning within 24h, formal notification within 72h and a final report within one month, with pre-established CSIRT communication channels; tested backups, separate recovery sites, annual exercises and documented RTO/RPO targets per critical workload; a complete inventory of ICT providers with critical dependencies mapped down to the second level of subcontracting; generalised MFA on privileged accounts and automated joiner/mover/leaver management; and TLS 1.2+ in transit, encryption at rest for sensitive data and customer-controlled key options where relevant.

DORA: the special case of financial entities

For financial institutions and their providers, DORA imposes structured management of ICT third-party risk — mapping of critical providers, contractual exit and reversibility clauses, regular operational resilience testing. A cloud provider poorly positioned on the "supply chain" or "operational" objectives of the Cloud Sovereignty Framework is, by construction, harder to secure in the DORA sense.

> **Key takeaway:** When you assess a provider that presents itself as "sovereign", ask which specific objective(s) of the framework it positions its offer against, and at which SEAL level. A vague answer is itself a piece of information.

In practice, untested business continuity plans, the lack of training of governing bodies and the fatigue caused by poorly calibrated security alerts come back as the three most frequently observed failings — and they are fixed by a single architecture roadmap, not by three separate audits.

Copyright Move2Cloud — move2cloud.fr

SECTION 07

Self-assessment grid

Before investing in a migration or a contract renegotiation, start by positioning your current architecture against these six questions.

- [ ] **Do you know, for each critical cloud provider, under which jurisdiction it is actually governed?** Not where the data is hosted, but who can legally demand access to it, and under which law.
- [ ] **Is your hardware and software supply chain documented?** Components, hypervisor, third-party software building blocks: do you know where they come from and who controls them?
- [ ] **Could you change your main cloud provider in less than six months?** Contractual and technical reversibility (open formats, no proprietary lock-in) is a criterion in its own right, not a convenience option.
- [ ] **Are your incident notification deadlines genuinely achievable?** 24h for the early warning, 72h for the formal notification: these deadlines assume detection is already in place, not to be built at the time of the incident.
- [ ] **Have you tested, over the past twelve months, a scenario involving a regional outage or a provider failure?** An untested recovery plan is not, in regulatory or operational terms, a recovery plan.
- [ ] **If a client or a funder asked you for your SEAL level across the eight objectives, would you be able to answer?** Even an approximate answer today is better than no answer at all on the day of a tender.

> **How to read your answers:** Three "no" answers or more out of these six questions generally indicate a significant gap between your current architecture and the level of requirement now expected in public and regulated markets. It is the natural starting point for a cloud sovereignty audit.

Copyright Move2Cloud — move2cloud.fr

SECTION 08

A 5-step roadmap

A progressive approach, designed to be carried out without interrupting the business or launching a brutal overhaul.

1

Map

Take inventory of cloud providers, their actual jurisdiction, critical workloads and dependencies down to the second tier of subcontracting.

2

Position

Assess each critical provider against the eight sovereignty objectives and estimate an indicative SEAL level per objective.

3

Prioritise

Identify the gaps that genuinely block a contract, a client or a regulatory obligation — rather than aiming for maximum sovereignty everywhere, which is often beyond budget reach.

4

Secure and test

Put in place 24/7 detection and NIS2 notification deadlines, and concretely test a failover or provider-loss scenario.

5

Document and maintain

Formalise the level of sovereignty achieved in a reusable file for tenders, audits and management reviews — and update it with every change in the regulatory framework.

Copyright Move2Cloud — move2cloud.fr

CONCLUSION

A regulatory constraint, or a competitive advantage?

Organisations that treat cloud sovereignty as a structuring architecture project — rather than an administrative box to tick — will gain a real advantage: greater operational resilience, easier access to public markets governed by the Cloud Sovereignty Framework, and NIS2/DORA compliance achieved in a single effort rather than three.

The European framework will continue to evolve over the coming months — CADA is still at proposal stage. But the fundamentals (mapping dependencies, reversibility, tested resilience) will remain relevant whatever the final version of the text: that is where it is reasonable to start right now.

Move2Cloud	is a consulting firm specialised in infrastructure, cloud and IT transformation. We support organisations in the audit, the design and the securing of their cloud environment.
Contact	Move2Cloud — Paris · move2cloud.fr
Next step	An initial cloud sovereignty audit makes it possible to answer the six questions on page 9 within a few weeks, with a prioritised and costed roadmap.

Sources

Commission européenne, « Proposal for the Cloud and AI Development Act (CADA) », digital-strategy.ec.europa.eu — Commission européenne, « Sovereign Cloud Framework explained », commission.europa.eu, 1 June 2026 — nlighten, « The EU Cloud Sovereignty Framework Explained: SEAL Levels, Sovereignty Objectives and the Sovereignty Score » — The Register, « Europe picks 4 sovereign cloud providers, but one has Google », 20 April 2026 — aenix.io, « NIS2 requirements for cloud infrastructure — a checklist for in-scope entities in 2026 », May 2026 — SoftwareSeni, « DORA, NIS2, and the EU AI Act Are Making Sovereign Cloud Mandatory for Some Workloads »

Document written by Move2Cloud as an example and illustration, for educational purposes. The European regulatory framework described here (CADA in particular) was, at the time of writing, still at proposal stage and subject to change; this document does not constitute legal advice.