



OBSERVATORY

SecNumCloud

SEPTEMBER 2026 EDITION

SecNumCloud: the summer when the doctrine turned into a market

The obligation comes into force, the offering expands. What remains to be seen is whether France has built a national exception or the vanguard of a doctrine amid an emerging trusted cloud offering.

The legal shift

The summer of 2026 marked a political and legal turning point for SecNumCloud. The decree of 12 August issued by the Prime Minister approves the framework applicable to cloud computing service providers: SecNumCloud 3.2, in a version dating back to March 2022. Nothing therefore changes fundamentally in the requirements. Everything changes in their scope. What ANSSI qualified now becomes, for certain sensitive data, the procurement rule for the State, its operators and six public-interest groupings, pursuant to the decree of 14 April 2026 and Article 31 of the SREN law. The sequence is now complete: structuring law, perimeter decree, standards decree. Sovereignty is no longer merely a doctrine or a preference. Within a defined scope, it becomes a procurement constraint.

It remains incomplete. Local authorities and hospitals are not directly covered by this general obligation, even though they handle some of the most sensitive data. They also account for a considerable share of public digital procurement. The decree also provides for a transition: where an acceptable offering exists, certain earlier projects may benefit from an exemption of up to eighteen months; where no acceptable offer exists, a one-year exemption can be granted and renewed until an offering becomes available. The obligation is therefore real, but its scope remains narrow and its application also depends on the existence of an offering that effectively meets the need.

From qualification to market

Côté offre, le mouvement s'accélère. Le 1^{er} sep On the supply side, momentum is accelerating. On September 1st, two qualifications are announced on the same day. OVHcloud obtains SecNumCloud qualification for the SNC Cloud Platform, its usage-based public cloud offering, the group's third qualified offering after Bare Metal Pod and VMware on OVHcloud. Numspot, a joint venture between Bouygues Telecom, Banque des Territoires, Dassault Systèmes and Docaposte, in turn obtains qualification for its cloud services

platform. Scaleway, for its part, is continuing its qualification process and has been selected to host the future sovereign platform of the Health Data Hub.

Taken separately, these developments are industrial. Taken together, they begin to form a market. This is probably where the real shift of 2026 lies. The problem with SecNumCloud has never been solely the cost of qualification. It was also the demand on the other side. For many months, applicants had to finance long, costly and demanding cycles in order to access a market whose depth no one could guarantee. By making the use of offerings meeting these requirements mandatory for certain sensitive data, the State changes the equation. It does not subsidise supply: it organises demand.

The battle is now European

The European debate has long opposed two conceptions. On one side, cloud certification centred on cybersecurity. On the other, the French position that trust cannot be reduced to technical security: it also requires knowing which company controls the service, which legal system it falls under and which extraterritorial orders it may be subject to. Europe is beginning to move beyond this opposition.

The draft Cloud and AI Development Act presented by the Commission on 3 June proposes a four-tier European framework for cloud sovereignty. The higher the level, the more requirements emerge concerning localisation, control over technology, personnel, dependencies and exposure to third-country jurisdictions. The shift is significant: sovereignty is no longer viewed solely as an attribute of cybersecurity certification. It becomes a standalone characteristic of the offering and a criterion in public procurement.

This is precisely the ground on which France has been experimenting for several years. Two trajectories are now possible. SecNumCloud may remain a French exception: demanding, protective, but limited by the size of its market and gradually circumvented by different European architectures. Or the French experience may help define the highest tier of a European trust architecture: technical security, operational control, jurisdictional control and technological autonomy. In the first case, France will have built a fortress. In the second, it will have built a standard.

The summer of 2026 has therefore not brought the SecNumCloud debate to a close. It has changed its nature. The question now is whether France will be able to transform a national requirement into a European market.

SÉBASTIEN GARNAUT
Founder of CyberTaskForce
& Paris Cyber Summit

SecNumCloud

What's Up?

RÉPUBLIQUE FRANÇAISE

JOURNAL OFFICIEL

LOIS ET DÉCRETS

The SecNumCloud framework becomes mandatory for private providers processing State data.

By a decree dated 14 August, Prime Minister Sébastien Lecornu makes SecNumCloud qualification mandatory for private providers processing data belonging to the State, its operators and public-interest groups.

The order makes the technical framework legally binding; until now, it had been a set of best practices that public administrations were encouraged to follow.

The framework itself has not been amended.



SecNumCloud

What's Up?



Wimi successfully completes J3 and obtains SecNumCloud qualification



NumSpot successfully completes J3 and obtains SecNumCloud qualification for its IaaS offering.*



OVH successfully completes J3 and obtains SecNumCloud qualification for its SNC Cloud Platform offering (PaaS and IaaS)*

*These qualifications have been publicly announced by the providers but are not yet reflected in ANSSI's official catalogue.



NRB submits a request to ANSSI for SecNumCloud qualification of its IaaS offering.



Interstis submits a request to ANSSI for SecNumCloud qualification of its SaaS offering.

SecNumCloud

What is it?

SecNumCloud is ANSSI's framework defining security and sovereignty requirements for cloud computing services used by public administrations and companies in France.

The qualification process

J0 Qualification request

J1 Assessment strategy accepted

J2 Assessment work validated

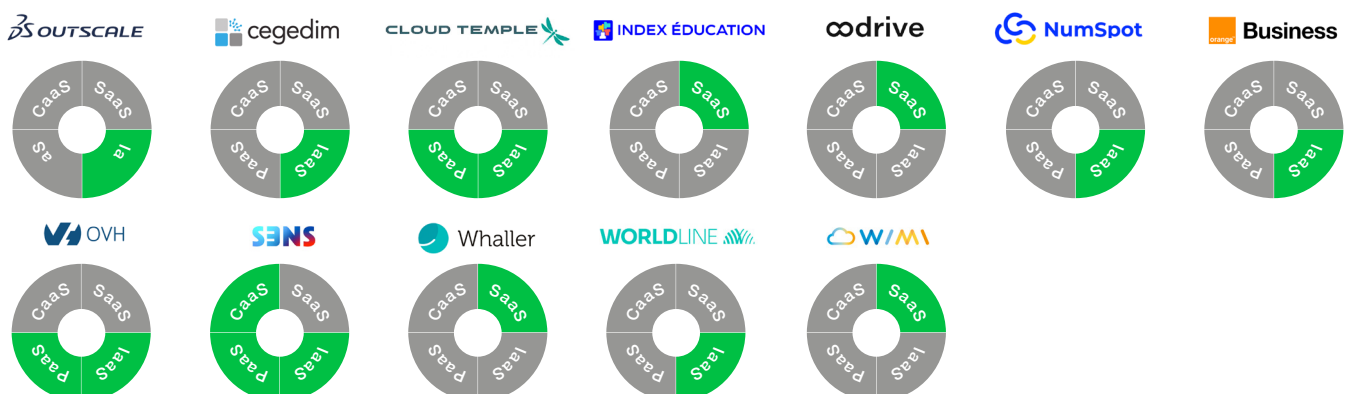
J3 Qualification decision by ANSSI



IN PROGRESS



QUALIFIED PROVIDERS



Glossary of Cloud Offerings



IaaS (Infrastructure as a Service)

- > Provision of physical computing resources.
- > **The provider owns** the physical infrastructure and rents it or makes it available to a user.
- > **The client builds** his activity on this platform
- > **The provider owns** all the physical material, including machines, network, and storage.
- > **The client** builds the services according to his needs, decides the scope/perimeter, and determines the possible uses on the leased infrastructure.

The Specifics of IaaS

- **Strict segregation** between users.
- To prevent data recovery during resource reallocation or physical support recovery, **encryption (of the disk, file system, or by volume) with a key per client is required**

CaaS (Container as a Service)

- > Provision of tools allowing **the deployment, management, and orchestration of application** containers.
- > **A container** is like a small, isolated box that contains everything necessary for an application to function (libraries, code, tools, etc.), without interfering with others.
- > **The provider** manages the underlying infrastructure (servers, storage, network, operating system).
- > **The client** controls the containers and the technical elements related to their applications

The Specifics of CaaS

- **Strict segregation** between clients.
- **Recommended cryptography:** encryption by volume (one key/client).
- **Secure obliteration** at the end of the contract means the secure erasure of the encryption keys for the client's storage spaces.
- Administration and supervision operations must be carried out **from within the European Union**

PaaS (Platform as a Service)

- > Provision of **a technical platform ready for use** to develop, host, and run applications.
- > **The provider** manages the entire infrastructure part (network, servers, storage, operating system, etc.).
- > **The client** focuses on the development and management of their own applications

The Specifics of PaaS

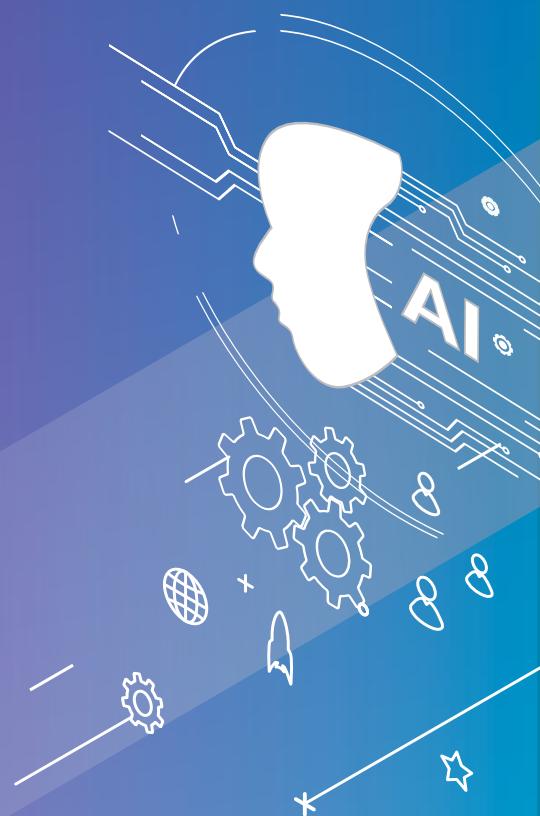
- The provider has a **duty to inform** the client in case of modification to the software elements that the provider controls.
- **Strict segregation** between clients interfaces: the resources allocated for the use of one client must not be accessible to other clients

SaaS (Software as a Service)

- > Provision of **ready-to-use applications**, hosted in the cloud and fully managed by the provider.
- > The user simply accesses the application via the Internet—without having to install, host, or maintain anything.
- > **The provider** manages all the technical aspects requiring IT skills.
- > **The client** does not control the cloud platform but can modify configuration settings within the application.

The Specifics of SaaS

- **Multi-factor authentication** for end-user access.
- **Segregation** between the administration interfaces made available to clients and the interfaces allowing end-user access



SEPTEMBER
2026
EDITION