PSN — Analysis of Digital Sovereignty Profiles

Why Italy's national cloud programme does not deliver digital sovereignty

National Digital Sovereignty Observatory — an independent project

05.08.2026

Generated automatically from osservatorio.mxmap.it/en/psn/. Page and PDF share a single source and cannot diverge.

Technical analysis

Encryption and confidential computing are real, useful security measures. They are also, on their own, unable to deliver sovereignty over a cloud controlled from another jurisdiction — and the French cyber-security agency says so in writing.

The Italian public cloud programme delivers **real consolidation** and **real security engineering**. It does **not** deliver digital sovereignty, and it is presented as if it did.

In its own user manual, the formal label **"data sovereignty" is attached to a periodic off-site backup** — a copy replicated monthly. A word carrying a legal meaning is used to name a storage option.

Across **161 pages** of contractual and operational documents, neither the terms (*CLOUD Act*, *extraterritorial*, *nationality*, *corporate control*, *third country*, *immunity*) nor the **substantive safeguard clauses** appear: *Article 48 GDPR*, *foreign judicial authority*, *third-country order*, *international transfers*, *mutual legal assistance* — all **zero**. It is not a matter of Italian legal vocabulary: the safeguards are absent in substance too.

Italy applied **corporate control where its law can reach** — golden power and consent to every change of capital, on the Italian concessionaire. The instrument that reaches the **technology provider** is not golden power, which cannot: it is the **procurement requirement** — and that one was never written.

The technical measures relied upon — encryption with external keys and confidential computing — are declared insufficient for exactly this purpose by the **French agency that wrote the European sovereignty standard**.

None of the four providers used holds any sovereignty qualification. In the French official catalogue, **Microsoft, Google, Amazon and Oracle appear zero times**.

What follows from this is not a technical remedy. The measures are effective against the adversaries they were designed for, and no measure can be designed against a legal order served on the provider. The variable that changes the answer is **where the provider is established, who controls its capital, and from where the service is administered** — and that variable is set by writing a requirement, not by buying a feature. France wrote it. Italy co-authored it in Brussels in 2021, lost it in 2024, and has never written it at home.

Every statement above is documented below, with a link to the primary source and, where the source is a file, an archived copy. A reader who wants to check rather than believe should start from how to verify this analysis.

The programme's own strongest defence, and why it does not hold

Confronted with the sovereignty question, the Italian public cloud programme answers with **two technical measures**, and they are the ones it puts forward first. It is worth stating them at their strongest, because both are real.

1. Keys held by the Hub itself

Encryption keys *"created and managed by the Thales infrastructure present on-premises in PSN data centres, **thereby excluding the CSP from encryption key management**"*; and, on the managed tier, *"**control of the Root Key**"* of the region.

2. Confidential computing

*"Confidential computing, **where enabled**, makes it impossible for the cloud service provider's operators to access the data **even during processing**."*

Source: PSN, Secure Public Cloud Azure user manual, ed. 04/04/2025 (PDF, 64 pp.)
[https://www.polostrategiconazionale.it/app/uploads/2025/04/PSN-Manuale-Utente-SPC-Azure.pdf] · services with Cloud Service Providers page
[https://www.polostrategiconazionale.it/soluzioni/servizi-con-cloud-service-provider/]

Taken together, these two would be a serious answer: the keys are outside the provider's hands, and the data is unreadable even while it is being computed on. **If that held, the jurisdictional question would largely dissolve.**

The French national cyber-security agency published a technical position paper on confidential computing on **17 October 2025**. It is the same agency that drafted **section 19.6 of SecNumCloud** — the clause that requires immunity from non-European extraterritorial law. Four sentences from that paper dispose of both measures.

*"Confidential Computing is **not secure enough to protect data integrity and confidentiality against a hostile administrator performing targeted, active attacks**."*

*"Confidential Computing is **not sufficient on its own**… **to meet the requirements described in section 19.6 of the SecNumCloud 3.2 framework**."*

*"Note that **'Bring Your Own Key' (BYOK) approaches do not solve this issue, as the CSP still needs to be trusted to use the keys provided by the user**."*

*"**Not rely on Confidential Computing if the cloud provider is considered untrusted or potentially hostile**… switching to a trusted CSP… **is a prerequisite**."*

Source: ANSSI, *Technical Position Paper on Confidential Computing* v1.0, 17.10.2025 (PDF, 13 pp.) [https://cyber.gouv.fr/sites/default/files/document/anssi-technical-position-paper-coco-v1.0.pdf] · and the SecNumCloud 3.2 framework [https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-exigences-v3.2.pdf], whose section 19.6 is cited

The two measures the programme relies upon are, in the words of the authority that defined the standard, **the two measures that do not meet it**. And the order of operations is reversed: a trusted provider is not an alternative to the technology — it is **the precondition without which the technology should not be relied upon at all**.

And one detail from the programme's own documents. Confidential computing is advertised on the commercial page with the qualifier *"where enabled"*. In the **64-page user manual** of the service on which it is advertised, the term *confidential computing* appears **zero times**. We do not claim it is unavailable — we state that the service's own operating manual does not document it, while the sales page makes it conditional. **The condition is not in the customer's hands.**

The technical reasons behind these four sentences — why a datum must be in the clear to be processed, why external key custody cannot prevent compelled use, and why attestation verifies software rather than location — are set out in Part II. A reader who accepts the four quotations can go straight to the table of the five offerings.

What the National Strategic Hub is, and what it promises

The **Polo Strategico Nazionale** is the infrastructure on which Italian public administrations are moving their systems, financed with European recovery funds. It exists to bring into a few supervised facilities the servers scattered across thousands of public bodies.

The consolidation is a real gain, and it should be said first. Concentrating thousands of scattered, unevenly maintained server rooms into a few supervised data centres improves physical security, continuity and management — *whatever software runs on top*. Anyone attacking this programme while ignoring that loses the argument in the first thirty seconds, and deserves to.

But the programme is not presented only as consolidation. Its own pages promise that public administrations will access services *"in full security, **autonomy and sovereignty**"*. This page examines that second word — because it is the one that carries a legal meaning, and because in the programme's own documents it turns out to mean something else.

*"The first requirement relates to **data sovereignty**… the replication of data onto PSN storage has a **monthly frequency** and only one version is retained."*

Source: PSN, Secure Public Cloud Azure user manual, ed. 04/04/2025, backup service section [https://www.polostrategiconazionale.it/app/uploads/2025/04/PSN-Manuale-Utente-SPC-Azure.pdf]

Read precisely, this is not a definition of sovereignty — and that is the point. The passage sits in the section describing the backup service, and states that one of that service's two requirements is *"related to data sovereignty"*, satisfied by a monthly replica. Anyone objecting that this is simply a recovery-point objective would be **right about the**

mechanism.

The finding is not that a monthly backup is a poor form of sovereignty. It is that **“data sovereignty” is the formal name given, in the operational documentation, to a storage measure** — and that this is the **only place in the documents we read where the term is attached to anything concrete at all**. A word that in European law denotes a jurisdictional condition is here doing the work of a retention policy. That is not a technical shortcoming: it is a semantic one, and it is what makes the rest of this page necessary.

On the Italian public cloud, **numerous technical measures have genuinely been deployed**: data encrypted at rest, keys held in hardware modules outside the provider's perimeter, network segregation, Italian regions, operational separation, confidential computing where enabled.

Not one of them can defend against a state actor able to compel the cloud service provider by legal order. That is not a hypothesis: it is the situation created by the United States **CLOUD Act** and by **Section 702 FISA** with respect to Microsoft, Google, Amazon and Oracle. And the reason is not that the measures are badly built. It is that **they are all measures against an attacker — and a legal order is not an attack**.

Part I answers the question directly, with the documents. **Part II** explains the technical reasons underneath — it can be read on its own, and it is what the answer rests on.

How to verify this analysis

This page is written to be **checked, not believed**. Every quotation is from a document we downloaded and read in full, not from secondary reporting. A security or infrastructure practitioner should be able to reproduce every finding independently, and this section says how.

The three conventions we use, and what they mean

Wording	What it asserts — exactly
“zero occurrences”	A full-text search was run over the named documents and returned nothing. The document set and the search terms are always stated, so the search can be repeated.
“not documented”	We read the document and did not find it. This is **not** a claim that the thing does not exist — only that the source does not state it.
“not found”	We looked for a document or a statement and could not locate it. Weakest of the three, and always flagged as such.

Reproducing the two scans

The two quantitative findings on this page are full-text searches, and both can be re-run in a few minutes.

1. **The 161 pages.** Download the four documents linked in section 1 — the concession agreement, the guide to the convention, the technical specification of services and the user manual for the Azure tier — extract the text, and search for: CLOUD Act, extraterritorial, nazionalità, capogruppo, paese terzo, controllo societario, immunità, legge straniera. **A methodological trap we fell into, and you will too.** The text layer of the convention guide is extracted *without spaces*: a naive search for software di base returns zero, falsely. Normalise whitespace out of the extracted text before searching, or you will report absences that are not there.
2. **The French catalogue.** Download the official catalogue of qualified products and services linked in section 8 and search for Oracle, Microsoft, Amazon, AWS, Polo Strategico.

The evidentiary standard we hold ourselves to

These twelve rules govern what may and may not be concluded on this page. They are published so that a reader can check whether we have followed them.

1. A marketing page does not prove a technical property unless accompanied by specifications, an audit or a contractual clause.
2. A generic vendor document does not prove the concrete implementation inside this programme.
3. **The absence of a word does not prove the absence of a rule.**
4. The presence of a connection or a dependency does not prove access to content.
5. The ability to update software is relevant, but is distinct from the present ability to read data.
6. A qualification is not an absolute guarantee and must be described within its scope.
7. **“Not documented” is not “non-existent”.**
8. **“Mitigated” is not “eliminated”.**
9. “Technically possible” is neither “legally authorised” nor “actually occurred”.
10. “Legally orderable” is not “technically executable without further modification”.
11. Every temporal claim must carry its date.
12. Every comparison must state whether the objects compared are genuinely comparable.

Two consequences we accept. First, *“zero occurrences”* means exactly and only **“no lexical match in this corpus, with these queries and these limits”** — not the absence of the risk, the rule or the discussion. Second, we have **privileged** normative, contractual, technical and scientific primary sources; where a journalistic source appears it is used **for context or as a route to the original document**, and never as proof.

Source manifest — files, sizes and hashes

Every file below has been archived in the project repository. The SHA-256 hash lets anyone confirm they are examining **the same document we examined**, and not a later revision.

Document	Size	SHA-256
Convenzione di concessione Polo Strategico Nazionale · DTD	53 pp 172 KB	ae3e3b0f2a97a91e38cd9e9ca71b2ac07d42a5405fcf7ba7a93dd231d062e0bb
Guida alla Convenzione Polo Strategico Nazionale · 08/2025	11 pp 199 KB	8b7e7ef454cb4679a8737e77c441a72836b240332e5d49f090b25e75e54575f6
Caratteristiche tecniche dei Servizi Polo Strategico Nazionale · 08/2025	33 pp 1060 KB	b839c349eb8b4a3a0c2be4b0da758eeaade0834b62c7354e708d4cd57104c4c1
Manuale Utente Secure Public Cloud Azure Polo Strategico Nazionale · ed. 04/04/2025	64 pp 3155 KB	bba442bd4a5afa8fc1d247d3619c83451ccb2da8ceb8a85aceb4941b370c09ab
Presentazione servizi a listino Polo Strategico Nazionale · 04/2026	121 pp 9783 KB	70344b74f2eab896aeba2e26622ba0858f30fd17ef00f99b2c20291eca7461ef
Deck istituzionale v12 Polo Strategico Nazionale · 10/2025	109 pp 8754 KB	c386b4ad00f8461e30b636480e003494d01763be7d449fe261b2ad82ff9f1a9a
Technical Position Paper on Confidential Computing ANSSI · v1.0, 17/10/2025	13 pp 309 KB	12b17100973fc205937866405dc243b453fa6b6f1ad99323fa58eb1e4e7eb128
Catalogue produits et services qualifiés ANSSI · 2026	130 pp 3597 KB	5a4bb87cf9216ae3251f35227a447563aa8b783c2298a83134bbf3f8843a69d4
Shareholder list — AWS European Sovereign Cloud GmbH Commercial Register, Potsdam · HRB 40853 P · notarised 20.10.2025	3 pp 87 KB	69c7ef33bcad326426e40b5c9121ec4bd97bec63fbda7857e279e16ba179d55f

The **“161 pages”** cited throughout refers to the four contractual and operational documents: **53 + 11 + 33 + 64**. The remaining files in the manifest support specific findings and are cited where used.

Documents we have not read, and what they would change

The corpus examined is contractual and operational. It does **not** include the national cloud strategy documents, which are known to acknowledge the risk arising from non-EU legal systems. That acknowledgement is not in dispute here, and this page does not claim the question was never raised in Italy — on the contrary, Italy co-authored the European immunity criteria in 2021.

The distinction this page rests on. Recognising a risk in a strategy document is not the same as turning it into **binding requirements, exclusion criteria, contractual clauses, technical verification or consequences for non-compliance**. Our finding is limited to the corpus in the manifest above: **in those documents, no such requirement was found**. Reading the strategy documents would refine the picture of intent; it would not by itself change what the contracts contain.

Where the sources are kept

Commercial pages change and PDFs are withdrawn. Every source file cited here has been **archived in the project repository**, so that the evidence does not depend on the continued availability of the vendors' websites. Links point to the original; the archived copy is the fallback.

Who is writing, and in what capacity. This Observatory is an **independent project**. It is **not a public body, not an authority and not an agency**, and nothing here carries institutional standing: the analysis is worth exactly what its sources are worth, which is why they are all listed with their hashes. The name describes the scope of the subject examined, not a public mandate.

And a point of consistency we owe the reader. A site that criticises dependence on non-European infrastructure while loading its own fonts, stylesheets and icons from third-party servers would be arguing against itself. **This page requests nothing from any third party.** Typeface, stylesheet, script and icon sprite are served from this domain: no visitor IP address leaves for a server outside our control in order to read this analysis. It can be checked in thirty seconds with the browser's network panel — and we invite you to.

This analysis is adversarial by design: it is meant to be attacked. If a quotation is inaccurate, a document has been superseded, or a technical reading is wrong, **we want to know and we will correct it in public**. Several findings on this page exist because an earlier version of our own reasoning was wrong and was corrected. That is the standard we hold ourselves to, and we invite the same scrutiny from anyone who works with these systems professionally.

Part I

1. Why this concerns Italy: the National Strategic Hub

The Italian public cloud programme — the *Polo Strategico Nazionale*, PSN — offers exactly these two measures as its protection, on the tier delivered from the hyperscalers' own public regions.

What PSN documents state	What follows from this page
Key management with keys *"created and managed by the Thales infrastructure present on-premises in PSN data centres, thereby excluding the CSP from encryption key management"*	Real and useful for data at rest. Does not address data in use — see section 13.
Confidential computing *"where enabled"* makes it *"impossible for the cloud service provider's operators to access the data even during processing"* (commercial page)	ANSSI states this technique does not meet SecNumCloud 19.6 and does not protect against a hostile administrator. And the conditional — *where enabled* — is decided by the operator.
In the 64-page user manual for the Azure tier, published April 2025, the term *confidential computing* appears **zero times**.	We do not claim it is unavailable. We state that the service's own user manual does not document it, while the marketing page qualifies it with *where enabled*.
Across 161 pages of contractual and operational PSN documents, these terms appear **zero times**: CLOUD Act, extraterritorial, nationality, parent company, third country, corporate control, immunity, foreign law.	The jurisdictional question is not answered by weaker technical means. It is **not asked at all**.

2. "PSN Managed" is two different architectures under one name

The Italian public cloud's most protected tier is presented as a single service. Its own page says otherwise, in one sentence:

> *"The service is based on **two technologies: Google Assured Workload and Oracle Alloy**." — "These infrastructures are hosted in **Italian regions or within Polo Strategico Nazionale Data Centres**."*

*"The service is based on **two technologies: Google Assured Workload and Oracle Alloy**." — "These infrastructures are hosted in **Italian regions or within Polo Strategico Nazionale Data Centres**."*

Source: PSN, *PSN Managed Public Cloud* [https://www.polostrategiconazionale.it/en/solutions/cloud-services-with-csp/psn-managed-public-cloud/] · service price list, 04/2026 [https://www.polostrategiconazionale.it/app/uploads/2026/04/Presentazione-servizi-a-listino-Polo-Strategico-Nazionale.pdf] · guide to the convention, 08/2025 [https://www.polostrategiconazionale.it/app/uploads/2025/08/PSN_Guida-alla-Convenzione_.pdf]

That **"or"** carries the whole weight. These are not two suppliers within one architecture: they are **two opposite architectures**, and only one of them is inside PSN's own data centres.

	Google side	Oracle side
Technology	Assured Workloads	Oracle Alloy
Where it runs	Google's own Italian regions — Milan europe-west8, Turin europe-west12	Inside PSN data centres
What it is	A **layer of policies** over public cloud	A **separate realm**, own hardware

PSN's own price list confirms both halves: on the Google side it lists a line item called *"Sovereign Controls"*, described as the ability to *"set policies within GCP"*. **Sovereignty as a price-list item, and as a policy setting.**

3. The five offerings, side by side

The first column is the benchmark: the only one of the five that holds a sovereignty qualification. Everything to its right does not.

	■■ PREMI3NS (benchmark)	■■ France Data Boundary	■■ PSN Managed — Google	■■ PSN Managed — Oracle Alloy	■■ Secure Public Cloud Oracle
Where the data runs	S3NS data centres	Google regions	Google regions — Milan, Turin	PSN data centres	**Oracle public region**
Nature	Separate infrastructure	Policy on public cloud	Policy on public cloud	Dedicated realm	Public cloud
Who operates the services	**S3NS staff only**	Google	Google	**Oracle** — "secure service operations"	Oracle
Software updates	**Quarantined, analysed and validated by S3NS** before deployment	Google	Google	Oracle produces them; PSN applies standard patching; **Oracle performs nonstandard upgrades**	Oracle
Control over updates	**Approval**	—	—	**Visibility only** — a dashboard listing emergency, mitigating, normal and routine changes	—
Provider access	"Google personnel have no access"	Split boundaries accessible to Google staff	Identical	*Operator Access Control* — **but it does not cover root automation**	Standard OCI
Sovereignty qualification	**Yes — SecNumCloud 3.2**	No	No	No	No

Source: Google, *Italy Data Boundary by PSN* [https://docs.cloud.google.com/sovereign-controls-by-partners/docs/data-boundaries/italy-data-boundary-psn] · France Data Boundary by S3NS [https://docs.cloud.google.com/sovereign-controls-by-partners/docs/data-boundaries/france-data-boundary-s3ns] · PSN price list 04/2026 [https://www.polostrategiconazionale.it/app/uploads/2026/04/Presentazione-servizi-a-listino-Polo-Strategico-Nazionale.pdf]

PSN's own price list introduces a further service, *Secure Public Cloud Oracle*, in these words:

*"Availability of services **that cannot be delivered through Alloy technology or cannot be implemented in PSN Data Centres**, thanks to the **direct use of the Oracle public region**." — "**Overcoming the limits** of Public Cloud PSN managed (Alloy): **new-generation Exadata (X9M, X11M)**, new compute classes, advanced Object Storage."*

To obtain the modern Exadata, one **leaves the PSN data centres and goes to Oracle's public region**. The "sovereign" perimeter is not where the best services are: it is where the ones Alloy can deliver are. And the mitigation is conditional again — *"use of the BYOK model **where applicable**"*.

4. The comparison, requirement by requirement

The Italian public cloud is delivered in **three tiers**, with three very different levels of control — all promoted under the same word. This table places them against the requirements that the French framework actually measures. Every cell about PSN comes from documents we downloaded and read in full: the concession agreement, the guide to the convention, the technical specification of services and the user manual for the Azure tier — 161 pages.

Requirement	SecNumCloud 3.2 §19.6	PSN Managed Google — Assured Workloads	PSN Managed Oracle Alloy	Hybrid on PSN site	Secure Public Cloud
Provider established in the EU	**Required**	**Not required anywhere.** The term does not appear as a requirement on providers in any of the 161 pages.			

Requirement	SecNumCloud 3.2 §19.6	PSN Managed Google — Assured Workloads	PSN Managed Oracle Alloy	Hybrid on PSN site	Secure Public Cloud
Capital control — non-EU stake capped	**Required**, ceiling at 24%	**Not required.** Zero occurrences of *nationality*, *parent company*, *corporate control*, *third country*. **Not because the tool was missing.** Golden power and consent to every change of capital are applied — *on the Italian concessionaire*, which is where Italian law can reach. The instrument that reaches the **provider** is the procurement requirement, as in the French framework. It was not written.			
Service administered from the EU	**Required**	**No.** Runs on Google's own Italian regions (europe-west8, europe-west12); Google operates.	**Partly — and it is real.** Hosting in PSN data centres, *"managed by PSN personnel"*. But Oracle supplies *"secure service operations"* and the product lifecycle.	**No.** *"A single control plane with Microsoft Azure Arc"*.	**No.** Delivered from the hyperscalers' *public regions*.
Immunity from non-EU extraterritorial law, stated	**This is the entire purpose of §19.6**	**Zero occurrences across 161 pages** of: CLOUD Act, extraterritorial, immunity, foreign law, foreign authority, non-EU. The two occurrences of *jurisdiction* concern litigation over the concessionaire, not data. **The question is not answered weakly. It is not asked.**			
Encryption key ownership	Necessary but, per the French agency, **not sufficient**	CMEK mandatory on 23 services; Cloud EKM available.	*"Control of the Root Key"*; central key management via PSN KMS/HSM. Real.	Not documented for this tier.	BYOK on Thales HSM on-premises, *"excluding the CSP from key management"*. Real — and the French agency states BYOK *"does not solve this issue"*.
Protection of data in use	Confidential computing **does not meet §19.6**	Not documented. Google states the boundary *"does not provide data residency controls for data in use"*.	Not documented.	Not documented.	Advertised *"where enabled"* on the commercial page. **Zero occurrences in the 64-page user manual.**
What "sovereignty" is defined as	A **legal condition**: establishment, capital, administration.	**The term is used but never defined** for these tiers in the documents we read.	**A monthly backup copy.** User manual, verbatim: *"the first requirement relates to **data sovereignty**… the replica onto PSN storage has a **monthly frequency** and only one version is retained"*.		
Is the requirement written in a binding act?	**Yes.** A qualification framework with legal effect for sensitive state data.	**No such requirement exists in Italian law or in the PSN contract.** There is therefore nothing to comply with, nothing to measure, and no ground on which a provider could be found wanting.			

Source: PSN concession agreement [https://www.polostrategiconazionale.it/app/uploads/2023/03/PSN-Concessione-Convenzione.pdf] · guide to the convention [https://www.polostrategiconazionale.it/app/uploads/2025/08/PSN_Guida-alla-Convenzione_.pdf] · SPC Azure user manual [https://www.polostrategiconazionale.it/app/uploads/2025/04/PSN-Manuale-Utente-SPC-Azure.pdf] · hashes in the source manifest

Why "PSN Managed" occupies two columns. As established in section 2, that service is two different architectures: on the Google side a policy layer over Google's own regions, on the Oracle side a dedicated realm inside PSN data centres. Collapsing them into one column would hide the only tier where the administration requirement is partly met — and would also credit the Google side with a property it does not have. **They are kept apart everywhere on this page.**

On method. Where a cell says *"not documented"* we mean exactly that: we read the documents and did not find it — which is different from asserting it does not exist. Where a cell says *"zero occurrences"*, we ran a full-text search across all four documents and state the result. The distinction is deliberate.

5. Why France is ahead — and it is not the reason usually given

First, the claim we do *not* make. It would be easy, and wrong, to say "French clouds are sovereign and Italian ones are not". France has **Bleu**, built on Microsoft technology, and **S3NS**, built on Google technology. Anyone can point at those two names and the argument collapses. So we do not make it.

The real difference is not in the purity of the providers. It is that **France wrote a requirement that can be measured, and Italy did not write one at all**. Three checks, each of which is either satisfied or not: where is the company established, who controls its capital, from where is the service administered.

Bleu and S3NS **exist because the rule exists**. No American company restructured out of goodwill: they did it because otherwise they could not sell to the French state. American technology, licensed; a European operator; non-EU capital capped at 24%. S3NS obtained ANSSI qualification on **17 December 2025**. **A fact that is inconvenient for our thesis turns out to be the proof that the rule works.**

In France, an American provider **had to change its corporate structure** in order to sell to the state.
In Italy, it was **never asked to change anything**.

That is the whole gap, and it is not a gap in technology, budget or engineering skill. Italy has excellent data centres, competent operators and a real consolidation programme. What it does not have is **a sentence in a binding document** saying what a provider must be in order to hold the state's most sensitive data. France wrote that sentence. It cost nothing to write. It changed the market.

And there is a detail that makes the comparison sharper still. Italy did not fail to think of this. **In 2021 Italy co-authored, with France, Germany and Spain, the European proposal that would have introduced immunity from foreign law into the Union's cloud certification.** Those requirements were removed in March 2024. Italy asked for the rule in Brussels — and in the same five years never wrote it at home, in the one instrument that depended on nobody else's vote.

6. Oracle Alloy, in Oracle's own words

First, what must be credited. Alloy is a genuinely separate realm, with *"its own control plane"*, *"physically and logically separated"* from Oracle's public cloud. PSN states two regions, an exclusive network with no public internet, all data in its own data centres, encryption to national-authority specifications. **On the infrastructure plane this is more than the Google Data Boundary offers.**

*"Oracle Alloy combines an **Oracle-managed cloud foundation** with an operator-managed business and customer experience layer. **Oracle supplies the cloud platform, secure service operations, and ongoing product lifecycle management.** The operator provides the **hosting environment** and runs the customer-facing cloud business on that foundation."*

The operator supplies the building and the commercial relationship. **Service operations are Oracle's.**

And Oracle's own vocabulary for the partner is unambiguous: the operator *"**resells** Oracle cloud services"* and manages *"the lifecycle of their **cloud reselling business**"*. A telling detail: the Oracle post titled *"Expanding Control & Flexibility"* for Alloy operators is about **multiple currencies and contract renewals**. The control being expanded is commercial.

Source: Oracle, *Alloy Overview* [https://docs.oracle.com/en-us/iaas/Content/dedicated/alloy/oracle-alloy-overview.htm] · oracle.com/cloud/alloy [https://www.oracle.com/cloud/alloy/] · Alloy Business Reporting [https://docs.oracle.com/en-us/iaas/Content/dedicated/alloy/alloy-business-reporting.htm]

Updates: who does what — stated precisely

Oracle's product page says the operator *"can independently manage **all standard operational tasks, such as basic patching and service updates**"*, and can rely on *"Oracle teams for troubleshooting, **nonstandard upgrades**, outage resolution, and escalations"*. Oracle's own VP for Dedicated Cloud sums it up: it is *"effectively a whole OCI region that the partner operating team can independently manage, maintain and enhance, **assisted by Oracle's upgrades and support**"*.

And what the operator gets over the changes themselves is a dashboard that *"provides **visibility** into scheduled and completed OCI service changes, including **emergency**, mitigating, normal, and routine changes"*. The verbs are observational throughout. **No approval, no refusal, no deferral is documented.**

Operator Access Control — real, and with three declared holes

Oracle offers a mechanism that is genuinely stronger than anything in the Google package: the customer **can approve or deny access by Oracle employees**, with time limits, full command logging and optional keystroke recording. It should be credited.

The three exclusions, in Oracle's words:

*"does not control **automation actions**, including the actions that are run as **root**, or other high privileged automation users, including **proxy-based automation access**"*

*"doesn't offer controls on external entities of Oracle Cloud Infrastructure, such as switches, **or other control plane software**"*

*"is a solution designed for auditing and compliance of Oracle access, **not a general purpose compliance solution**"*

Source: Oracle, *Operator Access Control* — overview [https://docs.oracle.com/en-us/iaas/operator-access-control/doc/overview-of-operator-access-control.html]

The gate controls people. It does not control the automation that runs as root.

Two honest caveats. Operator Access Control is documented for Exadata Cloud@Customer and Compute Cloud@Customer, not for Alloy as a whole — PSN does use Exadata on the Alloy platform, so it is pertinent, but we do not claim it covers everything. And Oracle's strongest claim — *"an Oracle Alloy Operator retains full control of the data and applications"* — is a **company statement we could not independently verify**, of the same kind as Microsoft's "it has never happened".

7. Amazon: Nitro Enclaves, and where the boundary actually is

Amazon is the **fourth cloud service provider** integrated into the Italian public cloud: PSN's own price list records the *"integration of the 4th cloud service provider, AWS"* in 2024, and describes *Secure Public Cloud* as based on the public services of *"the hyperscalers Microsoft Azure, Google Cloud, AWS and Oracle, with regions on Italian territory"*. So the question applies here too.

What Nitro Enclaves protects against — in AWS's own documentation

Nitro Enclaves is a genuinely well-built isolation technology. Its documented threat model is stated precisely, and it is worth reading twice:

> *"the data and applications inside the enclave cannot be accessed by the processes, applications, or users (**root or admin**) **of the parent instance**" — "The Nitro Hypervisor ensures that **the parent instance** has no access to the isolated vCPUs and memory of the enclave."*

*"the data and applications inside the enclave cannot be accessed by the processes, applications, or users (**root or admin**) **of the parent instance**" — "The Nitro Hypervisor ensures that **the parent instance** has no access to the isolated vCPUs and memory of the enclave."*

The party excluded from the enclave is **the customer's own instance** — its own root, its own admin, its own compromised code. **AWS is not named.** This is a defence against yourself, and a good one. It is not the defence the sovereignty debate is about.

Two further details from the same page. The enclave's life is bound to the instance: *"Enclaves are active only while their parent instance is in the running state. If the parent instance is **stopped or terminated**, its enclaves are terminated."* Whoever controls the hypervisor controls the switch. And attestation is integrated with **AWS KMS** — the key service operated by AWS.

Source: AWS, *What is Nitro Enclaves?* [https://docs.aws.amazon.com/enclaves/latest/user/nitro-enclave.html] · European digital sovereignty [https://aws.amazon.com/compliance/europe-digital-sovereignty/]

Two different things, and they must not be conflated. *Nitro Enclaves* is an EC2 feature that isolates an enclave from its **parent instance** — that is the threat model quoted above, and it concerns the customer's own environment. The *Nitro System* is the underlying platform architecture, and it is the subject of the far broader claim examined next. Answering a claim about the System with documentation about Enclaves would be a category error, so the two are treated separately here.

The Nitro System: the strongest claim of the four providers, and what supports it

AWS states that the Nitro System *"provides a strong physical and logical security boundary to enforce access restrictions so that **nobody, including AWS employees, can access customer workloads or data**"*. It is the boldest claim any of the three makes, and it deserves to be met with evidence rather than contradiction.

The claim rests on an external audit of the Nitro System. That audit declares **four limits of its own**:

- the auditor was **paid by AWS**;
- it is a **design review without testing** — the auditor states it cannot attest that the implementation matches the design;
- it places **outside its scope** the EC2 control plane, the hypervisor, the firmware and the Nitro Cards;
- and it gives **no assurance regarding future technical changes "chosen or *compelled*"**.

The word is the auditor's: ***compelled***.
The claim describes a design. **The audit of that design expressly excludes the scenario under discussion.**

An independent assessment not funded by AWS — Trail of Bits — puts the residual plainly: *"you must completely trust AWS"*.

The European structure, and what the commercial register says

On the corporate plane Amazon has done **more than Google or Oracle in Italy**, and it should be credited. AWS announced *"a new parent company and three subsidiaries incorporated in Germany"*, a management team of *"EU citizens residing in the EU"*, and an advisory board of four EU citizens *"including at least one independent board member who is not affiliated with Amazon"*, *"legally obligated to act in the best interest of the AWS European Sovereign Cloud"*. First region: Brandenburg.

We then looked the company up in the German commercial register, on two independent register services. The entry is **Amtsgericht Potsdam, HRB 40853**:

Date	Register entry
12–13.08.2021	Incorporated as **SCUR-Alpha 1391 GmbH**. Share capital **€25,000**.
21.10.2021	Renamed **Amazon Germany Holdco 1 GmbH**.
23.07.2025	Renamed **AWS European Sovereign Cloud GmbH**, seat moved to Potsdam.
17.06.2025 → 03.12.2025	**Kathrin Renz** — the managing director named in the announcement — appointed and then **no longer managing director**.
Today	Managing directors: **Stephane Israel** (14.11.2025) and **Stefan A. Höchbauer** (21.01.2026).

Date	Register entry
Sole shareholder	**A100 ROW, Inc.**, Wilmington, **Delaware, USA** — State File no. 4517940. **25,000 shares of €1.00 — total shareholding: 100%.** Notarised list, certified in Munich on 20.10.2025.
Purpose	*«Die Beteiligung an Gesellschaften, die durch den Betrieb europäischer Rechenzentren die Bereitstellung von Datenhosting-Diensten unterstützen»* — holding shares in companies that support data-hosting services.

Source: German commercial register — Amtsgericht Potsdam, HRB 40853 [https://openregister.de/company/DE-HRB-G1312-40853] · AWS governance announcement [https://www.aboutamazon.eu/news/aws/built-operated-controlled-and-secured-in-europe-aws-unveils-new-sovereign-controls-and-governance-structure-for-the-aws-european-sovereign-cloud]

We previously declined to state an ownership percentage, because the shareholder list is a paid document we had not read. **We have now read it.** The *Liste der Gesellschafter* for HRB 40853 P records a **single shareholder**:

A100 ROW, Inc. — Wilmington, Delaware, USA
25,000 shares of €1.00 · **total shareholding: 100%** · certified by a notary in Munich, 20.10.2025

The company presented as the **European** parent of the sovereign cloud is **wholly owned by a Delaware corporation**. Not partly, not jointly with a European partner: **one shareholder, one hundred per cent** — and it is not in Europe.

Where the chain stops, and why that matters. The German register proves the **first link** with a notarised document. The second — who owns A100 ROW, Inc. — cannot be proved the same way: **Delaware does not publish shareholder information**, which is among the reasons companies incorporate there. Converging secondary sources indicate Amazon.com, Inc.; we report that as such, and not as proof. **The point does not depend on it:** the sovereign cloud's parent company is already, on primary evidence, wholly owned outside the Union — and the chain then enters a jurisdiction where ownership is not disclosed at all.

The "new European parent company" is a pre-existing corporate vehicle, incorporated in 2021 and named *Amazon Germany Holdco 1 GmbH* until July 2025, with the statutory minimum capital of €25,000 and a corporate purpose of holding shares in other companies. And the managing director presented as the face of European governance **ceased to hold the office within roughly six months**.

Said fairly. Using a pre-registered corporate vehicle and the statutory minimum capital is **entirely ordinary corporate practice** in Germany, and proves no bad faith. To support a stronger judgement one would need the articles of association, shareholder agreements, veto rights, board composition and the licensing and operating dependencies — **none of which we have read**. The point is not the practice: it is the **distance between that practice and the language of the announcement**. The judgement is not about the vehicle: it is about the **distance between that ordinary practice and the language of the announcement**, and about the ownership recorded above.

And the sentence about it never having happened — better drafted than Microsoft's

Amazon's formulation is that since 2020 *"there have been no data requests to AWS that **resulted in the disclosure** of content **stored outside the USA** from **corporate or government customers** to the US government"*.

Three restrictions in a single line. It does not say there were no *requests*: it says none *resulted in disclosure*. It covers only content *outside the United States*. And only *corporate or government* customers. It is the same class of statement as the one examined in section 12 — and it is unverifiable for the same reason: the prohibition on saying so is itself the law.

Two further findings, stated for completeness. AWS's own announcement of the European Sovereign Cloud governance **does not discuss the CLOUD Act at all**: as with the Italian documents, the jurisdictional question is not answered weakly — it is not raised. And in the French agency's official catalogue of qualified products, **Amazon and AWS appear zero times**: neither qualified nor under assessment. Microsoft set up Bleu and entered assessment; Google set up S3NS and reached qualification. **Amazon set up a German GmbH and did not take it to French qualification.**

8. Who holds a sovereignty qualification, and who does not

The French agency publishes an official catalogue of qualified products and services. We read it in full — 130 pages — and searched it.

Oracle 0 · Microsoft 0 · Amazon 0 · AWS 0 · Polo Strategico Nazionale 0

Source: ANSSI, catalogue of qualified products and services (PDF, 130 pp.) [https://messervices.cyber.gouv.fr/visas/catalogue-produits-services-profils-de-protection-sites-certifies-qualifies-agrees-anssi.pdf] · list of providers under assessment [https://cyber.gouv.fr/offre-de-service/solutions-certifiees-et-qualifiees/services-de-securite-evalue/solutions-en-cours-de-qualification/prestataires-secnumcloud/]

What this count does and does not mean — and it matters. The French qualification attaches to a **specific offering**, not to a company or to a technology. An offering *built on* a vendor's technology but **operated by a European entity** can be qualified: that is precisely the case of **S3NS**, which runs on Google technology and **is qualified**, and of **Bleu**, which runs on Microsoft technology and is **under assessment**. The correct reading of the count is therefore narrow: **no offering used by the Italian programme holds such a qualification, and none is under assessment** — not that these vendors' technologies are incapable of supporting one. The French cases prove the opposite.

The **sixteen** offerings currently under assessment are equally telling: Adista, **Bleu SAS**, BLUE, Cegedim, Cloud Temple, Ecritel, Free Pro, GIP Mipih, ITS Integra, NumSpot, NRB, Orange Business, OVH, Prolival, Scaleway, Scalingo. **Bleu — the Microsoft, Orange and Capgemini venture — is on that list. Oracle is not.**

On **9 February 2021**, before the French National Assembly, the managing director of Oracle France announced that the company was *"in discussion with the agency"*.
Five and a half years later, Oracle appears neither among the qualified nor among those under assessment.

Microsoft, on the same road, set up **Bleu** — French controlling capital — and entered the assessment. Google set up **S3NS** with Thales and reached qualification, registered to **Thales Cloud Sécurisé**: the holder is the European controlling shareholder. **Oracle announced a discussion.**

What this finding does not prove. The absence of a qualification is not proof that Alloy is inadequate. It means something more precise, and more defensible: **Alloy has never been measured against that standard** — and the Italian public cloud programme, which builds its most protected tier on Alloy, **has not asked anyone to measure it**. We also found **no French agency analysis dedicated to Oracle Alloy**: not found is not the same as non-existent.

9. The four vendors, and the point where they coincide

Each of the four providers used by the Italian public cloud has built something real, and each has drawn a security boundary. Read one at a time, the four look different. Read side by side, **they exclude four different parties — and none of them excludes the same one**.

Vendor	Its strongest measure	Who it genuinely excludes	Who it does not exclude
Microsoft	Italian region, PSN-held keys, hybrid on PSN premises	Other tenants, disk theft, casual staff inspection	Whoever holds the control plane — declared as **Azure Arc** in PSN's own contractual guide
Google	Assured Workloads — residency and access policies	Resource creation outside the chosen regions, non-CMEK services	Whoever can change the policy — a change is **recorded, not prevented**, and can be given an exception
Amazon	Nitro Enclaves — encrypted, isolated execution	**The customer's own parent instance** — its root, its admin, its compromised code	Whoever runs the hypervisor and can stop the instance — and signs the attestation
Oracle	Alloy — a separate realm in PSN data centres, plus *Operator Access Control*	**Oracle employees** — genuinely: approval, time limits, command and keystroke logging	**The automation that runs as root** — excluded by Oracle's own documentation — and the update channel

Read the last column downwards. Every one of those parties is **the vendor itself**, in a different technical guise: the control plane, the policy engine, the hypervisor, the automation. **Four different measures, and each stops at the same wall.**

9.1 How the mitigations themselves create the exposure

This is the part that is easy to miss, and it is the sharpest point on this page. The American statute reaches data in a provider's **possession, custody or control**. Each of these mitigations, in order to work, must **create a new object** — and that object ends up in exactly that condition.

The mitigation	The object it must create	Where that object sits
Encryption at rest	A key that the platform must be able to *use*	In the key service, or reachable from it
Confidential computing	An attestation, signed by a root of trust	In the manufacturer's and the vendor's chain
Isolated enclave	A hypervisor that enforces the isolation and an instance that hosts it	Entirely with the vendor
Sovereign region / data boundary	A control plane that applies and verifies the rules	With the vendor — and, on the hybrid tier, **named in the contract**
Partner-operated realm	An update channel through which the platform stays alive	With the vendor, who produces the updates
European subsidiary	A chain of corporate ownership	Ending with a parent company outside the Union

A mitigation does not remove the legal hook. **It moves it, and gives it a new name.** The data becomes unreadable and the *key* becomes reachable; the memory becomes opaque and the *attestation* becomes signable; the region becomes national and the *control plane* stays abroad. This is why adding more measures does not converge on sovereignty: each new measure adds one more object to the list of things the vendor holds.

9.2 What the four have in common when they speak

The pattern repeats in the language, too. Each vendor makes a strong statement, and each statement is **true as written** — and narrower than it sounds.

- **Microsoft**, under oath: *"No, I cannot guarantee it, but, once again, this has never yet occurred."* The first half is the admission; the second half is unverifiable by design.
- **Amazon**: *"no data requests that **resulted in the disclosure** of content **stored outside the USA** from **corporate or government customers**"*. Three restrictions in one line.
- **Oracle**: *"an Oracle Alloy Operator retains full control of the data and applications"* — a company statement, alongside a documentation page that excludes root automation from the access controls.
- **Google**, in a document written for schools: *"we **carefully review** each request"*. Carefully review. **Not: refuse.**

And a silence they also share: in the official announcement of the AWS European Sovereign Cloud governance, in the Google data-boundary pages, and across 161 pages of Italian contractual documents, **the American statute is not discussed at all**. The jurisdictional question does not receive a weak answer. It is not put.

What none of this proves. It does not prove that any vendor has acted improperly, nor that any Italian public data has been disclosed. We have no evidence of either, and we say so. What the four analyses establish is narrower and firmer: **the measures deployed are effective against the adversaries they were designed for, and none of them was designed for a legal order served on the vendor**. That is not a defect of engineering. It is the boundary of what engineering can do.

A technical answer to a legal question

The providers subject to the CLOUD Act — Microsoft, Google, Amazon — are not standing still. They have invested heavily, and visibly, in what is marketed as *sovereignty*: European legal entities, national regions, local operations staff, external key management, encrypted enclaves, dedicated boundaries for EU data. Some of these are serious pieces of engineering, built by competent people, and this page will credit them individually.

It is worth being clear about why this is happening. It is not a change of heart: it is a **commercial response to a legal exposure**. European public administrations began asking an awkward question, France wrote it into a certification framework, and the market produced answers. That is healthy — and it is also where the problem starts.

Every one of these measures is **built, configured and operated by the very party it is supposed to protect you from**. That is not a flaw in any individual product: it is a structural property of buying a service from someone. And it means that each measure has a precise point at which it hands control back — a point where, to keep working at all, it must trust the provider again.

The table below is the map of this page. On the left, each measure and what it genuinely solves — because each one solves something real. On the right, **the point at which it closes back on itself**, with a link to the section that examines it. Read the right-hand column downwards and you will notice that the reason is always the same, expressed six different ways.

The measure	What it genuinely solves	Where it closes back on itself
Encryption at rest with external keys	Disk theft, other tenants, casual inspection of an archive. **Real protection.**	To process a record it must be decrypted, and the plaintext appears in the provider's memory. → §13
National region — data residency	Latency, continuity, and a set of genuine data-protection obligations on transfers.	Jurisdiction follows the company, not the disk: the statute reaches data in the provider's *possession, custody or control*, wherever located. → §15
Local staff and operational separation	Day-to-day access by foreign staff, and support performed from outside the country. **A serious property.**	An order is not served on the local operations team: it is served on the parent company. → §1
Confidential computing	Neighbouring tenants and passive reading of memory by the host. **Genuine defence in depth**, in ANSSI's own words.	It does not hold against an *active* administrator — and it is the operator who decides whether it is switched on at all. → §12
Remote attestation	Cryptographic verification that the workload running is the one you expect.	It verifies *what* runs, not *where* — and the mechanism itself was broken in 2026. → §12.4
European legal entity of the provider	Contracting, invoicing, civil jurisdiction, and a local point of accountability.	A European subsidiary of a non-European group is not a European group — a principle stated under oath by one of the providers themselves. → §12
"Sovereign" backup inside the national perimeter	Continuity and recoverability if the service becomes unavailable.	A copy is not an access restriction. Having a duplicate does not prevent anyone from reading the original. → §4

Each line in the right-hand column is a different way of writing: **the measure depends on the provider**. Which is why adding more of them does not help, and why the answer is not a better measure. Section 14 explains why this is not an engineering problem at all; section 15 takes the objections one by one; section 1 applies the whole thing to the Italian public cloud.

> *"Confidential Computing is **not secure enough to protect data integrity and confidentiality against a hostile administrator performing targeted, active attacks**."*
>
> — **ANSSI**, French National Cybersecurity Agency, *Technical Position Paper on Confidential Computing*, 17 October 2025

Read that threat model again: **a hostile administrator**. Not an outside hacker, not another tenant — the operator of the platform itself. That is exactly the situation a legal order under a foreign jurisdiction creates: a provider that is not malicious, but is *compelled*, and forbidden to say so.

10. A datum exists in three states. Encryption covers two.

This is the whole technical argument, and it fits in one table. It is not controversial: it is how computers work.

State	Protection	Does it work?
At rest on disk	Encryption with external keys	**Yes.** Genuinely effective. It protects stored blocks against disk theft, against other tenants, and against casual inspection by staff.
In transit on the wire	TLS	**Yes.** Mature, standard, effective.
In use in RAM, in the CPU	Confidential computing	**Partly, and not against the operator.** This is the subject of the rest of this page.

In **ordinary general-purpose cloud workloads** — a database, a mail server, an application — a datum must be **in the clear** inside an execution context in order to be processed. Every query, every search, every report, every login involves a moment in which the data is plaintext in the RAM of a machine owned and operated by someone.

A precision that matters, because the opposite is often written. It is *not* true in general that a processor cannot compute on encrypted data: **homomorphic encryption**, **secure multi-party computation** and privacy-preserving techniques do exactly that. They differ widely in scope, performance and maturity, and — on the evidence available — **they are not the basis of the architectures described on this page**. The claim made here is therefore narrower and checkable: in the ordinary workloads these programmes actually run, the datum is decrypted inside an execution context.

Whoever controls the hypervisor and the physical machine controls that moment. They can pause a virtual machine and dump its memory; they can snapshot it; they can read the CPU registers. None of this is exotic — it is ordinary platform administration, the same capability used every day for live migration, debugging and backup.

11. What confidential computing is — and what it genuinely achieves

Confidential computing is the industry's answer to the third row of that table. The processor creates an encrypted, isolated enclave — a *Trusted Execution Environment* — whose memory is encrypted with a key held in the silicon and, in principle, not available to the hypervisor. The main implementations are **Intel TDX**, **AMD SEV-SNP** and **ARM CCA**. A mechanism called **remote attestation** is supposed to let the customer verify, cryptographically, that their workload really is running inside such an enclave.

ANSSI — the same agency quoted at the top of this page — is explicit that the technology *"complements effectively at-rest and in-transit encryption by encrypting data in-use"* and *"still provides significant defence-in-depth"*. Used correctly, it *"may raise the complexity of attacks from the host or other tenants on the same physical machine, and reduce the size of the Trusted Computing Base"*. **This is not a bad technology.** Anyone claiming otherwise is overstating the case, and will lose the argument to any competent engineer.

12. Four reasons it does not produce sovereignty

12.1 The threat model excludes precisely our threat

Confidential computing is designed against a *curious* operator and against neighbouring tenants. It is not designed against an operator who is *determined*, who controls the firmware and the provisioning chain, and who has time. ANSSI's conclusion on that scenario is the sentence at the top of this page. And ANSSI adds what to do instead: users *"must avoid running on shared infrastructure operated by providers they cannot trust"*.

A legal order does not make a provider malicious. It makes it compelled — which, in the threat model, is the same thing.

*"**Not rely on Confidential Computing if the cloud provider is considered untrusted or potentially hostile**: against an active attacker, there are **too many known vulnerabilities to effectively guard against**. In such situations, **switching to a trusted CSP or using dedicated bare-metal hardware in a controlled physical environment is a prerequisite**."*

This is not a caveat buried in an annex. It is a numbered recommendation to users, in the agency's own position paper.

Note the word **prerequisite**. ANSSI does not present a trusted provider as an alternative to the technology: it presents it as the *precondition* without which the technology should not be relied upon at all. The order of operations is the opposite of the one implied by every "sovereign cloud" offering built on a provider under foreign control.

12.2 It does not meet the sovereignty standard — according to the agency that wrote the standard

*"The current analysis shows that Confidential Computing is **not sufficient on its own to secure an entire system, or to meet the requirements described in section 19.6 of the SecNumCloud 3.2 framework**."*

Section **19.6** of SecNumCloud is *the* immunity clause: the requirement that a qualified provider be shielded from non-European extraterritorial law — through establishment, capital control and where the service is administered from. **ANSSI wrote that clause. And ANSSI says confidential computing does not satisfy it.**

This is the single most important fact on this page. Every argument that offers confidential computing *as a substitute for* jurisdictional requirements is answered, in advance, by the authority that invented those requirements.

Exactly what ANSSI does and does not say — because the distinction matters. The words *sovereignty*, *state actor*, *extraterritorial*, *jurisdiction* and *law* appear **zero times** in the thirteen pages of the paper. We checked. ANSSI does not frame its analysis in political terms at all.

What it does is more useful. It describes the adversary **functionally** — a *"malicious admin"* who *"can control the creation and execution of workloads, including modifying them before they are started, and **reading or writing their memory at runtime**"*; and, among the actors against whom the model does not hold, *"attackers with a **very high power to coerce suppliers**"*. Then it declares the technique insufficient for the clause that exists to counter foreign state access. **The political conclusion is ours; the technical premises are entirely ANSSI's.**

12.3 Whoever operates the platform decides whether it is switched on

Confidential computing is not a property of the data. It is a *configuration of the platform*: a machine type to be selected, a feature to be enabled, firmware to be kept current. The entity that decides whether the enclave is active, for which workloads, and after which update, is the same entity the enclave is supposed to protect against.

This is why the wording used by providers matters so much. When a service is described as offering confidential computing **"where enabled"**, the protection has been made conditional — and the condition is not in the customer's hands.

12.4 A weakness found in how attestation is bound to the channel

The whole construction rests on remote attestation: without it, the customer has no way to know whether the enclave is real. The finding below **does not invalidate attestation in general** — it concerns a widely deployed way of binding attestation evidence to a TLS channel. In 2026 researchers led by **Muhammad Usama Sardar** (TU Dresden), with Mariam Moustafa and Tuomas Aura, showed that attestation performed inside the TLS handshake can be defeated by a relay attack. In The Register's summary of the work:

> *"A connection intended for one server can be **silently redirected to a different, compromised machine running identical software, anywhere in the world**, without the client ever knowing."*

*"A connection intended for one server can be **silently redirected to a different, compromised machine running identical software, anywhere in the world**, without the client ever knowing."*

The protocol *checks the software's integrity, not its location*. The vulnerability is tracked as **CVE-2026-33697** (CVSS 7.5) and affected systems already in production. The research is published as *Identity Crisis in Confidential Computing* (AsiaCCS 2026) and *Intra-handshake.fail* (ESORICS 2026). And on whether it can be fixed, the paper concludes that full protection *"may not be possible"* within intra-handshake attestation as currently architected, without breaking properties of TLS 1.3.

Stated precisely. This is a flaw in a widely deployed *way of doing* attestation, not proof that every confidential computing deployment is broken; mitigations exist and are being adopted. What it does establish is that attestation is an active research area with unsolved problems — which is a poor foundation for a claim of sovereignty.

12.5 And the marketing claim ANSSI corrects directly

ANSSI notes that the technology *"is often presented by commercial providers as a solution to run remote workloads with the same level of confidentiality and integrity as a local setup, i.e. resistant to a physical attack"* — and then states plainly: ***"physical attacks are explicitly out-of-scope of the security model"***.

Whoever owns the building has physical access to the machines. The security model of confidential computing does not cover that, and says so.

13. And the keys? The same problem, one level down

The second technical answer usually offered is key management: the customer holds the encryption keys outside the provider's perimeter, typically in a hardware security module. The models have names — **BYOK** (bring your own key), **HYOK** and external key management — and they differ in how far the key stays away from the platform.

This too is real, and it too must be credited before it is criticised. Keys held in a customer-controlled HSM genuinely remove a class of exposure: stored blocks cannot be read by copying a disk, an operator cannot casually browse an archive, and a key can be revoked.

> For a workload to run, the data must be decrypted. The decryption happens **inside the provider's execution environment**, because that is where the CPU is. However far away the key is kept, at the moment of use either the key or the plaintext — and usually both — is present in the memory of a machine the provider operates.

An analogy that survives scrutiny: you may keep the key to the safe in your own pocket, in another country. But if the safe is in someone else's building, and you ask their staff to open it and read the document out to you, **the location of the key is not what determines who can read the document**. External key management changes *who has to be compelled*, and how visibly. It does not change *whether* the plaintext exists inside the provider's perimeter.

> *"Note that **'Bring Your Own Key' (BYOK) approaches do not solve this issue, as the CSP still needs to be trusted to use the keys provided by the user**."*
>
> — ANSSI, same paper, in the section on availability and key handling

That single sentence disposes of the argument that external key custody produces sovereignty. The key is yours; **the hands that use it are not**. Trust in the provider is not removed by the architecture — it is relocated from "trust them with the data" to "trust them to use the key only as instructed". For a provider under a legal duty to comply with a foreign order, that is the same trust.

13.1 Where exactly BYOK stops working, step by step

It is worth following the key through an ordinary operation, because the point is not subtle once you see the sequence. Suppose an administration stores an encrypted database in the provider's cloud, with the key in its own hardware module.

#	What happens	Who can see what
1	The data sits on disk, encrypted.	**Nobody**, without the key. BYOK works. This is real protection.
2	A civil servant runs a search.	The platform must now decrypt. It requests the key, or requests that the external module perform the operation.
3	The external module authorises. This is the moment the whole architecture rests on.	The module cannot tell *why* the request was made, only that it is well-formed and comes from the expected platform. **It cannot distinguish a legitimate query from one executed under an order.**
4	The record is decrypted and processed.	The plaintext is **in the RAM of a machine the provider administers**. This is unavoidable: it is where the CPU is.
5	The result is returned.	Anyone who can snapshot that machine's memory has the data **in the clear** — regardless of where the key lives.

The external key module is therefore not a barrier to reading the data. It is **a switch that decides whether the system works at all**. Its real power is to stop everything — which is a genuine and valuable property, and also a very blunt one: an administration cannot revoke its own key every time it suspects something, because revoking it means shutting down the service.

And ANSSI notes the same trap from the availability side: making the platform depend on an external key introduces a failure mode that *"may result in an outage of the whole system"*. Key externalisation buys a kill-switch and pays for it in fragility — but it does not buy confidentiality against the operator.

There is one genuine benefit worth naming, because it is the strongest argument on the other side: revoking an external key is *observable*. A customer who withdraws the key learns that access has stopped. That is a real property — but it is a property about **future** access, and it is useless against an acquisition that already happened and that a non-disclosure order forbids anyone from mentioning.

14. Why a technical measure cannot solve a legal problem

This is the part that is worth understanding even if you skip everything else on this page, and it takes about a minute.

Every security measure ever built assumes an **adversary who has to get around something**. Encryption assumes someone who does not have the key. Access control assumes someone without credentials. Network segregation assumes someone on the wrong side of a boundary. Confidential computing assumes someone who must break out of an enclave. All of these work by *raising the cost of circumventing the rules of the system*.

> A legal order does not circumvent anything. **It is executed by the administrator, using the administrator's own legitimate powers, inside the rules of the system.** No boundary is crossed, no credential is stolen, no enclave is broken. The provider does what it is entitled to do on its own platform — and does it because a court has told it to.

Source: Google, *Monitor an Assured Workloads folder for violations* [https://docs.cloud.google.com/assured-workloads/docs/monitor-folder]

This is why the question *"which technical measure protects against the CLOUD Act?"* has no answer. It is like asking which lock protects against the landlord's own key. The lock is not defective. **The question is aimed at the wrong layer.**

And it explains why stacking measures does not help. Defence in depth multiplies the work of an attacker who must defeat each layer in turn. It does nothing when **every layer is administered by the same entity**, because that entity does not have to defeat them: it configures them.

15. The objections, one by one

These are the answers a provider or a public cloud programme can legitimately give. Each is reported in the strongest form we can give it, then answered. Where the objection is partly right, we say so.

"Confidential computing encrypts memory. Not even we can read it."

Yes — and: True for passive reading, and worth having. But the memory encryption protects the *contents* of a machine, not the *chain of command that decides how that machine is started*. Whoever operates the platform can decline to enable the feature, disable it, alter the image before boot, update the firmware, or restart the workload in a configuration without an enclave. ANSSI is explicit that the technology does not hold against an administrator performing **active** attacks.

"There is remote attestation. The customer verifies cryptographically."

Yes — and: Attestation verifies *what* is running, not *where*. In 2026 researchers showed a relay attack — CVE-2026-33697 — in which a connection is silently redirected to a different machine running identical software, anywhere in the world. And the trust root is the manufacturer chain: ANSSI lists among the relevant adversaries *"attackers with a very high power to coerce suppliers"*, able to obtain a copy of the private keys held in hardware.

"The encryption keys are yours, in a hardware module outside our perimeter."

Yes — and: ANSSI, verbatim: *"BYOK approaches do not solve this issue, as the CSP still needs to be trusted to use the keys provided by the user."* Custody is not use. To process a record the platform must obtain a usable key or the plaintext, and the external module cannot tell a legitimate request from one executed under an order.

"The data never leaves Italy. The region is Italian."

Yes — and: Jurisdiction follows the nationality of the company, not the position of the disk. The CLOUD Act reaches data in a provider's *possession, custody or control*, wherever located — including an Italian data centre. This is not our reading: it is why the statute was written after Microsoft won on the location argument in the Irish case.

"The staff who operate the service are Italian."

Yes — and: This is a real and valuable property at the operational layer, and it should be credited. But an order is not served on the Italian operations staff: it is served on the parent company. And where a hybrid control plane exists, it belongs to the provider — PSN's own contractual guide describes *"a single control plane with Microsoft Azure Arc"*.

"We combine several measures. Defence in depth."

Yes — and: Defence in depth multiplies the effort of an attacker who must defeat each layer. It adds nothing when all the layers share the same point of trust, because that party does not defeat them — it configures them. Two locks on the same door do not help if the same person holds both keys.

"You can revoke your key at any moment."

Yes — and: True, and it is the strongest argument on this list: revocation is *observable*, and the customer learns that access has stopped. But it governs **future** access only. It is useless against an acquisition that has already happened — and which a non-disclosure order forbids anyone from mentioning.

"It has never happened."

Yes — and: It cannot be fully verified, by us or by the person saying it. A non-disclosure order — where one is issued, and not every order carries one — makes the fact unspeakable by law, and the Italian rule requiring providers to report non-EU access requests asks for precisely the communication that the foreign statute forbids. The sentence is not a reassurance; it describes a silence guaranteed by law.

"The service is certified and qualified by the national authority."

Yes — and: The Italian qualification framework does not contain requirements on nationality, corporate control, parent company or third-country law. Across 161 pages of PSN contractual and operational documents, those terms appear zero times. The jurisdictional question is not answered weakly — it is not asked.

"Confidential computing is an industry standard."

Yes — and: ANSSI notes that it *"lacks security certifications"*, that the ecosystem *"currently lacks mature software stacks integrating attestation with secret delivery"*, and that deploying it correctly *"involves deep expertise to ensure the integrity of the entire TCB"*. It is a fast-moving field with unsolved problems, not a settled guarantee.

> Each objection is about a **capability**: encryption, attestation, key custody, location, staffing, certification. Not one of them is about **who can be ordered to act, by whom, and under which law**. That is the only variable that changes the answer — and it is not a technical variable.

16. Seven scenarios, graded

A binary verdict — sovereign or not sovereign — is easier to write and easier to refute. What follows is the same evidence organised by **threat scenario**, because the programme performs very differently across them. **In three of the seven it performs well**; that is not a concession, it is the result.

Scenario	Measure declared	Public evidence	Residual risk
A — Ordinary access by a service administrator	Italian operating staff on the managed tier; Oracle's *Operator Access Control* with approval, time limits and command logging.	Documented in vendor and programme sources.	**Low.** Root automation is excluded from those controls, by Oracle's own statement.
B — Provider compromise or vulnerability	Segmentation, encryption at rest with keys in a customer-controlled HSM, Nitro isolation, Zero Trust, network without public internet.	Documented, and technically sound.	**Genuinely reduced.** This is what these measures are built for, and they work.
C — Legal order served on the Italian party	Italian and European law, national oversight, golden power on the concessionaire.	Documented in the concession agreement.	**Not the subject of this analysis.** An order under Italian or EU law follows Italian or EU safeguards. Nothing here disputes that.

Scenario	Measure declared	Public evidence	Residual risk
D — Legal order served on a connected US company	Encryption with own keys; confidential computing *"where enabled"*.	The French agency states both are **insufficient** for this purpose, and no contractual clause on the point was found.	**Not addressed.** Whether the addressee holds possession, custody or control must be established case by case — but nothing excludes it, and nothing is written about it.
E — Imposed or malicious update	On the Oracle tier, standard patching by the operator. On the Google tiers, updates by the vendor.	The operator has **visibility** of changes, including emergency ones. **No approval or refusal is documented.**	**Open.** The Nitro audit expressly gives no assurance against changes *"chosen or compelled"*. This is a **software-control** risk, and should not be conflated with proof of data access.
F — Geopolitical or commercial interruption	Sovereign backup inside the national perimeter; two Alloy regions; exclusive network.	A copy exists. Whether the platform can operate **disconnected from the vendor**, and for how long, **is not documented anywhere we looked**.	**Unquantified.** Licences, support, updates and hardware replacement all run through non-EU parties. A backup is not continuity.
G — Request for metadata	Encryption protects content. Configurations, logs, identities, billing, telemetry and resource graphs are a separate matter.	**Not addressed in the documents examined.** We found no mapping of which components transmit telemetry outside the perimeter.	**Undetermined, and probably underestimated.** Metadata is often as revealing as content, and it is rarely encrypted end to end.

The pattern is not that the programme is weak everywhere. In **A, B and C** it does what it was built to do, and does it well. The exposure is concentrated in **D, E, F and G** — foreign legal order, software control, continuity without the vendor, and metadata — and those four share one feature: **none of them is a security problem. They are all questions about who holds what, and under which law.**

17. The best arguments in favour of the programme

An analysis that only presents the case against itself is not an analysis. What follows are the strongest arguments a competent defender of the Italian public cloud would make, stated **as well as we can state them** — and then answered with what the evidence supports, and only that.

The argument, at its strongest	What the evidence supports in reply
Consolidation is a genuine security gain. Thousands of unevenly maintained server rooms replaced by supervised data centres improves physical security, continuity and patching — probably more than any sovereignty clause would.	**We agree, without reservation.** Nothing on this page disputes it, and this analysis would be dishonest if it did.
The contracting and operating party can be Italian even where the technology is American. Governance, staffing and accountability genuinely sit in Italy.	True, and documented for one tier. It addresses *operational* sovereignty. It does not address who the legal order is served on, which is a different question.
Localisation, segmentation, encryption, logging and access control reduce real risks. Most actual incidents are not state orders.	**Correct, and important.** Our claim is not that these measures are useless — it is that they answer a different question from the one the word "sovereignty" raises.
A vendor's nationality does not prove possession, custody or control over every datum. It must be established case by case.	**Correct, and we say so ourselves.** We make no claim that any datum has been disclosed, nor that subjection follows automatically from ownership. What we document is that *no contractual clause excludes it*.
Confidential computing and external key management can limit even the provider's access. That is their stated purpose.	They can, and they do reduce several scenarios. But the agency that wrote the European sovereignty standard states that they **do not meet that standard** and do not hold against an *active* hostile administrator. That is not our judgement.
SecNumCloud is not the only legitimate model of sovereignty. A country may reasonably choose a different balance.	**Entirely true.** Our objection is not that Italy failed to adopt the French model — it is that **no equivalent requirement of any kind** was found in the corpus examined. A different model would also have to be written down.
Full technological autonomy has its own costs, delays and operational risks. A pragmatic solution may accept residual risk.	**Agreed — provided the residual risk is measured and declared.** That is the crux: a risk accepted openly is a policy choice; a risk described as absent is something else.

Of the seven arguments above, **we accept three outright and qualify three more**. The disagreement narrows to a single proposition, and it is falsifiable: **that the documents examined contain a requirement, of any model, binding a provider on establishment, ownership or administration.** Produce that clause and this analysis is wrong.

18. What could be done — six measures, in order of feasibility

Criticism that offers no alternative is commentary. What follows is ordered by how soon each measure could be adopted, and every one of them rests on an instrument that **already exists**. None requires abandoning the current providers.

#	Measure	Instrument that already exists
1	**Publish which tier each administration uses.**	Costs nothing and requires no negotiation. It is the single datum whose absence prevents anyone — including Parliament — from measuring the exposure. **Its absence is the third instance of the same pattern documented on this site.**
2	**Use the 12 January 2027 deadline.**	From that date, European law already in force prohibits charging a customer the cost of leaving a cloud. It is the only certain date in the whole picture, and it turns *"changing costs too much"* from an argument into a question.
3	**Map and publish the telemetry.**	Which components transmit outside the perimeter, which endpoints, which metadata. Scenario G is undetermined precisely because this map does not exist publicly — and producing it is an engineering task, not a political one.
4	**Require approval, not visibility, over platform changes.**	Today the operator sees changes, including emergency ones, on a dashboard. A contractual requirement of prior approval — and of quarantine and validation before release, as one French provider already does — converts scenario E from open to bounded.
5	**Write an establishment, ownership and administration requirement for the highest data classification.**	Three binary checks, applied only to the data that warrants them. It need not be the French model — but it has to be **written**, because a requirement that exists in no document cannot be complied with, measured, or breached.
6	**Join the European purchasing arrangement, without waiting.**	The proposed European regulation lets a local authority join **even if its own State does not**, and thereby comply with EU procurement law. **It is not yet in force** — approval is missing, the agreement between the Commission and at least two Member States is unsigned, and the platform does not exist. The point is not that the door is open: it is **where the door is**.

What we are not recommending. Not abandoning these providers, which would be neither feasible nor obviously wise; not full technological autonomy, which carries costs, delays and operational risks of its own; and not the French framework as the only legitimate model. **Accepting a residual risk is a legitimate policy choice.** Describing that risk as absent is a different thing, and it is the only thing this page argues against.

19. The conclusion, stated carefully

Encryption and confidential computing are **good engineering**. They defeat a wide range of real attackers: other tenants, intruders, thieves, individual rogue employees. They should be used, and a provider that offers them is doing something worthwhile.

But they are all measures that protect you *from someone else* while you are inside a house that belongs to a third party. **None of them answers the question of what happens when the owner of the house is served with an order — and is forbidden to tell you.** That is not an engineering question. It is a question of which law applies, and the only known ways to change the answer are the ones written into SecNumCloud and into the letters asking for EUCS High+: where the company is established, who controls its capital, and from where the service is administered.

Numerous technical measures have genuinely been deployed. Not one of them can defend against a state actor able to compel the cloud service provider by legal order — which is the position of the United States, through the CLOUD Act and Section 702 FISA, with respect to Microsoft, Google, Amazon and Oracle. The measures are good. They are aimed at attackers. **The order is not an attack: it is the administrator, doing what the administrator is allowed to do.**

Presenting these measures as sovereignty is not a technical error. It is a **category error**: answering a legal question with an engineering artefact. The measures are a mitigation. They are not an immunity — and the agency that defined immunity has said so in writing.

Sources

- ANSSI — *Technical Position Paper on Confidential Computing* v1.0, 17.10.2025 [https://messervices.cyber.gouv.fr/guides/en-technical-position-paper-confidential-computing] The primary source for every ANSSI quotation on this page. **The full 13-page PDF was downloaded and read in its entirety**, not the summary page. Direct link to the PDF [https://cyber.gouv.fr/sites/default/files/document/anssi-technical-position-paper-coco-v1.0.pdf] · SecNumCloud 3.2, the framework whose section 19.6 is cited [https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-exigences-v3.2.pdf]
- The Register — on the attestation relay attack, 04.07.2026 [https://www.theregister.com/security/2026/07/04/confidential-computings-trust-mechanism-is-broken-the-fix-may-not-exist/5266056] Reporting on the work of Sardar, Moustafa and Aura. Primary papers: AsiaCCS 2026 and ESORICS 2026; CVE-2026-33697.
- PSN — services with Cloud Service Providers [https://www.polostrategiconazionale.it/soluzioni/servizi-con-cloud-service-provider/] The commercial page. The contractual and operational documents quoted here (161 pages) were downloaded from the PSN site and read in full.

Every quotation on this page has been read at its primary source, not taken from secondary reporting. Where we could not verify a claim, we say so on the page itself.