# Who Builds the Platform? Ownership vs. Stack

2026-07-09

Bleu, S3NS, Google, Microsoft, and AWS: how EU sovereign-cloud ownership claims pair with technology stacks — checked against primary sources. Part 2 of 6.

---

Part 1 raised the technology-supply-chain question with one case: Open Telekom Cloud, legally owned by Deutsche Telekom, running on a Huawei-licensed platform. Five more prominent, more recent cases turn out to follow the same pattern — checked here against primary sources, not just repeated from secondary coverage — alongside three providers where ownership and technology stack come closer to aligning, each with its own gaps left intact rather than smoothed over.

**⚠ Not a legal opinion**

The ownership, corporate-structure, and certification details below come from public sources — company press releases, official whitepapers, and reported journalism, including an on-the-record executive interview — gathered while researching a technical distinction (legal ownership vs. technology supply chain), not a legal one. I am not a lawyer, and this is not legal or regulatory advice. If sovereignty or compliance status is load-bearing for an actual decision, that needs review by someone qualified to assess it from a legal and regulatory perspective.

**i What**

Every claim below was checked against at least one primary source (a company's own press release, whitepaper, or official announcement) plus independent corroboration. Where a number or claim turned up repeated across secondary sources but could not be confirmed against a primary source — the exact Capgemini/Orange equity split in Bleu, the exact Thales/Google percentage in S3NS — this post says so explicitly rather than presenting it as settled. A few specific claims that did not survive that check (a named AWS executive's role, a Microsoft marketing claim about remote-access controls) are left out entirely rather than repeated with a caveat attached.

## The comparison

| Provider | Legal ownership | Underlying technology stack | Access / support model | Certification status |
|---|---|---|---|---|
| Open Telekom Cloud *(recap, see Part 1)* | Deutsche Telekom (Germany) | OpenStack-based, "powered by" Huawei (FusionSphere) | Not covered in this post | — |
| Bleu (France) | Capgemini + Orange; Microsoft holds no equity | Microsoft 365 / Azure | Microsoft support staff worked onsite as of the most recent reporting found (Oct. 2025); full separation still pending | SecNumCloud not yet fully certified as of Oct. 2025 reporting; commercial availability targeted H2 2026 |
| S3NS (France) | Thales (reported majority) + Google Cloud (reported minority — exact split not independently confirmed here) | Google Cloud (Compute Engine, Cloud Storage, Cloud SQL, GKE, BigQuery) | Not detailed in sources found | SecNumCloud 3.2 qualified Dec. 2025; GA Oct. 2025 |
| Google Cloud (no wholly-Google-run offering) | No independent EU-owned "European Sovereign Cloud" product exists; genuine infrastructure separation is delegated to partners (S3NS in France; a new Thales-owned entity in Germany) | Google's own stack, either via a control layer on shared infrastructure or via partner-operated dedicated infrastructure | Base tier routes support to "global support personnel"; EU-only support is a paid add-on; engineering/ops access undocumented | New German entity in preview as of this writing, targeting GA end of 2026 |
| Microsoft Sovereign Cloud (Sovereign Public/Private Cloud) | Microsoft-operated directly; no independent EU co-owner found in Microsoft's own materials, and no specific legal entity name confirmed | Microsoft's own Azure / Microsoft 365 stack | "Data Guardian": EU-resident personnel approve/monitor remote engineer access — Microsoft's own claim, no independent audit found | Sovereign Public Cloud generally available across European regions as of early 2026; Sovereign Private Cloud's GA status less clearly confirmed |
| AWS European Sovereign Cloud | 100% Amazon.com Inc. (four German GmbHs; no independent EU co-owner) | AWS's own software stack; global AWS engineering teams continue development per AWS's own whitepaper | EU-resident AWS employees operate day-to-day, but remain AWS employees | Launched ≈Jan. 2026; entity structure documented Sept. 2025 |

## Case: Bleu (France)

Bleu's own material states plainly that "100% des capitaux de Bleu sont français" — its equity is held solely by Capgemini and Orange, with Microsoft named in every primary source only as a

technology and strategic partner, not a shareholder. The exact split between Capgemini and Orange themselves is not stated in any source found for this post; treat that detail as unconfirmed rather than a guessed number.

What runs underneath that ownership is unambiguous. Bleu's own press materials describe the platform as "based on Microsoft 365 and Microsoft Azure services" and "specific technology developed by Microsoft." A March 2026 extension adds SAP applications on top of the same Bleu-operated Azure infrastructure.

How close is Bleu to operating that stack independently of Microsoft? Bleu's own CEO, Jean Coumaros, said the clearest thing on record: SecNumCloud certification requires Bleu to become "entièrement étanche" (entirely sealed off) from Microsoft, and Microsoft's support teams would need to have left Bleu's sites before that certification is granted — meaning, at the time of that August 2024 interview, they had not yet left. Reporting from October 2025 describes Bleu retaining only a request-based right to inspect specific portions of Microsoft's source code for security checks, not full or continuous audit access, with Bleu itself acknowledging this could miss issues in code it does not otherwise see. As of the most recent reporting found for this post, Bleu had cleared only procedural milestones toward SecNumCloud (April and September 2025), with full commercial availability targeted for the second half of 2026 — worth re-checking against Bleu's current status before treating any certification claim as final.

## Case: S3NS (France)

S3NS is commonly described as majority-owned and controlled by Thales, with Google Cloud holding a minority stake reported around 20%, under SecNumCloud rules that cap any single non-EU shareholder below 25% and non-EU shareholders collectively below 39%. That reported split is consistent across secondary sources, but no primary source — a Thales press release, the SecNumCloud referential itself, or a French regulatory filing — surfaced during this research confirming the exact percentage. Treat the specific number as reported, not independently verified here.

The technology stack is not in dispute. S3NS's own announcement of its PREMI3NS offering states it "integrates Google Cloud technologies including Compute Engine, Cloud Storage, Cloud SQL, Google Kubernetes Engine, BigQuery," with generative AI services planned as a future addition. PREMI3NS reached general availability in October 2025 and received the ANSSI SecNumCloud 3.2 security qualification, covering the full offering, in December 2025.

## Case: Google Cloud

Unlike Microsoft and AWS, Google Cloud has no wholly-Google-run offering that matches the phrase "European Sovereign Cloud." The only verbatim use of that exact phrase found on Google's own sovereign-cloud page refers to a physical facility — the Munich "Sovereign Cloud Hub," a customer-engagement and training center that opened in November 2025 — not a cloud product. Google's own marketing umbrella for this area is simply "Sovereign Cloud from Google."

Google's documentation describes a tiered structure, and only the lightest tier is something Google operates directly: "Google Cloud Data Boundary" applies data-residency and access-logging controls on top of Google's standard, shared public-cloud infrastructure — the same infrastructure any other Google Cloud customer uses — with independent partner oversight of encryption keys

offered as optional, not structural. Genuine infrastructural separation is delegated entirely to named local partners: in France that partner is S3NS, covered above. For Germany, Google and Thales announced a new, Thales-owned German entity on May 20, 2026, described as "legally and operationally independent… from Google Cloud" — still in preview at the time of writing, targeting general availability by the end of 2026, with its exact ownership structure not yet public at announcement. Treat any comparison of its equity split to S3NS's as unconfirmed rather than assumed identical.

Google's own support documentation also complicates a blanket "EU-only operations" claim: the base Data Boundary package states that support cases "are routed to global support personnel," not EU-restricted ones — EU-only support routing is available only as a pricier add-on requiring an Enhanced or Premium support subscription. Nothing found in Google's documentation for this post addresses whether global (non-EU) engineering or operations teams, as distinct from customer support, retain any access path — a documentation gap, not a stated denial either way.

The clearest independent challenge to this model followed the EU's April 2026 selection of S3NS as one of four providers for a sovereign-cloud framework contract. CISPE, a European cloud-industry trade association, objected publicly: "Recognising S3NS, which leverages Google's cloud technology, as sovereign is clearly an own goal and threatens to institutionalize sovereignty washing at the highest levels" — the same term this series' opening post is also built around.

## Case: Microsoft Sovereign Cloud

Bleu is Microsoft's technology running under someone else's ownership — a model Microsoft's own documentation calls a "National Partner Cloud" (the same category Delos Cloud, an SAP subsidiary in Germany, falls into). Separately, Microsoft also runs a directly-branded sovereign offering of its own: "Microsoft Cloud for Sovereignty" launched as a private preview in July 2022, then evolved into the umbrella "Microsoft Sovereign Cloud," under which Microsoft announced two Microsoft-run deployment models — "Sovereign Public Cloud" and "Sovereign Private Cloud" — in June 2025.

Ownership here is more direct than either Bleu or AWS European Sovereign Cloud: Microsoft's own documentation describes Sovereign Public/Private Cloud as hosted in Microsoft-operated datacenters on Microsoft's global Azure infrastructure, with no joint-venture partner or separate legal entity mentioned anywhere — in explicit contrast to how the same documentation names Bleu and Delos as independently owned and operated. What no source confirms, unlike AWS's whitepaper naming specific German GmbHs, is a specific Microsoft legal entity (for example, a named EU subsidiary) that owns and operates this infrastructure; treat that as an open gap, not a confirmed fact either way.

Microsoft's access-control claim is called "Data Guardian": remote access by Microsoft engineers to systems storing European customer data must be approved by EU-resident personnel in real time, logged in a tamper-evident ledger. That is Microsoft's own documentation language; no independent technical audit of the mechanism was found. A separate, longer-running commitment — the EU Data Boundary, covering data residency for Azure, Microsoft 365, Dynamics 365, and

Power Platform — reached its final rollout phase in February 2025, again as a Microsoft-stated commitment rather than a third-party-verified one.

The most direct independent evidence on whether any of this delivers operational independence from Microsoft's global (US) organization is not a critic's inference — it is Microsoft's own on-the-record testimony. On June 10, 2025, before a French Senate hearing, Anton Carniaux, Microsoft France's director of public and legal affairs, was asked whether he could guarantee that French citizens' data would never be transmitted to US authorities without French authorization. He answered: "No, I cannot guarantee it." Analyst Axel Oppermann, quoted by CIO, separately describes Microsoft's sovereignty claims as a governance layer rather than architectural independence.

## Case: AWS European Sovereign Cloud

AWS European Sovereign Cloud is structurally different from Bleu and S3NS: there is no independent EU company involved at all. AWS's own announcement describes "a new parent company and three subsidiaries incorporated in Germany" — four entities in total — and independent analysis of the structure states plainly that all four are 100% subsidiaries of Amazon.com Inc. AWS states that day-to-day operations (data-center access, technical support, customer service) are run by EU-resident AWS employees — but they remain AWS employees inside a wholly Amazon-owned entity group, not employees of a separately-owned company the way Bleu's staff work for Capgemini/Orange or S3NS's for Thales.

The most notable finding here is a statement in AWS's own September 2025 whitepaper, not a critic's claim: "While global AWS teams will continue to develop AWS services, the AWS European Sovereign Cloud will be controlled by Qualified AWS European Sovereign Cloud Staff. We plan for AWS European Sovereign Cloud teams to establish mechanisms for consultation with global technical specialists as needed…" AWS is stating directly that the software itself continues to be developed by its global engineering organization — the same underlying pattern documented for Bleu/Microsoft and S3NS/Google, in AWS's own words.

## The pattern across six cases

Put next to Open Telekom Cloud from Part 1, these five cases show that the ownership layer and the technology-stack layer move independently of each other, not together:

- **Ownership genuinely diverges from technology stack.** Open Telekom Cloud, Bleu, and S3NS all have real, non-hyperscaler equity holders with reported or confirmed majority control (Deutsche Telekom, Capgemini/Orange, Thales respectively), while running platforms licensed from, or developed by, a non-EU technology vendor (Huawei, Microsoft, Google).
- **Sometimes both layers point the same direction.** Microsoft Sovereign Cloud and AWS European Sovereign Cloud have no independent EU ownership to diverge from in the first place — the entity structure and the technology stack are both under the hyperscaler's control, relocated into EU-based operations or EU-incorporated subsidiaries. In both cases, the strongest evidence on this point comes from the vendor's own words: AWS's whitepaper states its global engineering teams continue developing the software, and Microsoft's own France legal director told the French Senate, under oath, that he could not guarantee EU data would never reach US authorities.

- **Sometimes the hyperscaler doesn't claim a direct sovereign layer at all.** Google Cloud has no wholly-Google-run offering matching the other five; genuine infrastructure separation is delegated entirely to local partners (S3NS, and the new Thales-owned German entity still in preview), while the one layer Google does operate directly runs on the same shared infrastructure as any other customer.

None of this is presented here as a verdict on whether any of these six offerings "is" or "isn't" sovereign — that word means different things to different regulators, customers, and vendors, and the SecNumCloud qualifications some of these have earned are a specific, defined technical and organizational bar, not a general sovereignty certificate. What the public record does show, consistently across all six cases, is that checking legal ownership alone does not answer what technology a platform runs on, or who continues to develop, support, or access it.

## Where ownership and technology stack align

The six cases above all show some version of the same gap: ownership checks out as EU, but the technology underneath — or who has access to it — does not, cleanly. Three providers often raised as EU alternatives show what closer alignment looks like in practice. None of them is spotless; each has at least one product line or capability gap worth naming, so this stays pro-and-con rather than turning into an EU-cloud advertisement.

| Provider | Ownership & jurisdiction | Core infrastructure | The gap |
|---|---|---|---|
| OVH (France) | OVH Groupe, governed by French law | Self-built servers and data-centers; OpenStack-based Public Cloud, "OpenStack Powered" certified; SecNumCloud-qualified | Hosted Private Cloud runs on VMware (Broadcom, US) or Nutanix (US); OVH also operates a US subsidiary, OVH US LLC, itself directly subject to US law |
| STACKIT (Germany) | Schwarz Digits / Schwarz Group, no external shareholders | All data centers in Germany/Austria; Kubernetes engine (SKE) built on Gardener, EU-origin CNCF open source | SKE still lacks native Kubernetes API-server audit-log streaming (management-API-level logging only, as of early-2026 docs); colocation product is rack/room rental, not API-provisioned bare metal |
| Aruba Cloud (Italy) | Aruba S.p.A., Cecconi-family controlled; no foreign parent found | Italian-headquartered since 1994 | Cloud platform markets OpenStack-based and VMware-based (Broadcom, US) instances as parallel product lines, not a niche exception |

### OVH (France)

OVH designs and assembles its own bare-metal servers in company-owned factories (Croix, France, and Beauharnois, Canada) and builds its own data centers and network, including owned dark-fiber links. Independent French tech-press coverage of OVH's 2021 Strasbourg data-center

fire is corroborating evidence for how self-contained that supply chain actually is: OVH replaced roughly 18,000 servers from its own factory within weeks, the kind of response a third-party-operated supply chain would not produce on that timeline. Its Public Cloud line is OpenStack-based and certified "OpenStack Powered" by the OpenInfra Foundation — a foundation-governed open-source project, not a single vendor's proprietary platform the way Huawei's FusionSphere is. OVH also holds France's SecNumCloud qualification, which requires certified data to never leave the EU and to be operated exclusively by EU-based personnel.

The gap sits in a different product line. OVH's Hosted Private Cloud runs on proprietary software licensed from US vendors — VMware (owned by Broadcom) or Nutanix — including a dedicated "NC2 on OVHcloud" product built on Nutanix-qualified hardware. OVH's own marketing for that product still uses the word "sovereignty." Whether "sovereignty" there refers to infrastructure location and legal jurisdiction, or extends to the underlying software's origin, isn't specified in that marketing — the same ambiguity this post already flags for Bleu and S3NS, here inside a single provider's own catalog rather than across a joint venture.

A second, separate nuance is worth naming plainly. OVH's own EU-facing materials describe "the OVHcloud Group" as a European group whose commercial entities "fall under the exclusive jurisdiction of European Union member states," with "no dependency links to any entity… subject to the jurisdiction of states that do not provide an adequate level of data protection." At the same time, OVH operates a US subsidiary — OVH US LLC, doing business as OVHcloud, based in Reston, Virginia — whose own legal documentation describes handling US law-enforcement requests under US law directly, as its own entity. Whether a shared corporate parent creates any practical CLOUD Act exposure for EU-held data is a legal question this post is not qualified to answer (see the disclaimer above) — but the existence of that US subsidiary, and OVH's own two separate legal pages describing two different jurisdictional postures, is worth knowing before taking a "CLOUD Act free" claim at face value.

### STACKIT (Germany)

STACKIT is wholly owned by Schwarz Digits, the digital/IT arm of the privately held Schwarz Group (parent of Lidl and Kaufland) — no external shareholders, no reported change of ownership. Every STACKIT data center is located in Germany or Austria. Its Kubernetes engine, STACKIT Kubernetes Engine (SKE), is built on Gardener, a cluster-management project originally created by SAP and now governed as a CNCF open-source project — EU-origin, foundation-adjacent technology, not a licensed foreign platform.

The gap here is capability, not ownership. As of STACKIT's own documentation, SKE still does not offer native Kubernetes API-server audit-log streaming — the only generally available audit trail covers SKE's own management-API actions (cluster creation, version changes, node-pool updates), not activity inside the cluster's Kubernetes API itself. STACKIT's docs reference an early-2026 target for closing this gap; worth re-checking at read time rather than assuming it has shipped by now. Separately, STACKIT's colocation product is physical rack and room rental where the customer supplies their own hardware — not an API-provisioned bare-metal server product — while STACKIT's actual provisioned compute offering (STACKIT Server) is VM-only.

### Aruba Cloud (Italy)

Aruba Cloud's parent, Aruba S.p.A., is an Italian company founded in 1994 and still controlled by the Cecconi family, with no foreign parent or private-equity stake found in this research.

Its technology stack shows the same split seen at OVH: Aruba markets both OpenStack-based cloud servers and VMware-based cloud servers as parallel product lines, not a niche exception — meaning at least one core Aruba Cloud product depends on the same Broadcom-owned, US-proprietary virtualization software as OVH's Hosted Private Cloud. A specific claim about Aruba's data-center footprint relying partly on partner facilities outside Italy did not hold up under verification for this post and is deliberately left out here; Aruba's exact data-center ownership geography would need its own dedicated check before saying anything more specific about it than "Italian headquartered."

## Additional information

None of these three is offered here as "the answer" to the six cases above — a SecNumCloud-qualified Public Cloud at OVH sits in the same catalog as a VMware/Nutanix product line; a wholly German-owned platform at STACKIT still has a real audit-logging gap. The point is narrower: EU ownership and an EU-built technology stack can and do align, in specific products — just not as a blanket property of a company's entire catalog. The same product-by-product scrutiny this post applies to Bleu, S3NS, Microsoft, and AWS applies here too.

Independent, regulator-level assessment now backs that alignment: in April 2026, the European Commission awarded its own Sovereign Cloud framework tender — the same body citing the same underlying supply-chain concern this post traces — and rated Post Telecom (bidding with partners CleverCloud and OVHcloud), STACKIT, and Scaleway at SEAL-3, the framework's highest published level, defined as a provider's service, technology, and operations being immune from supply-chain disruption by non-EU third parties. Proximus/S3NS — the joint venture covered above — was accepted into the same framework, but only at SEAL-2. That's not a blanket "OVH and STACKIT are sovereign" verdict: SEAL-3 is a specific bar assessed for one procurement framework, not a general certification, and OVH's rating came via the Post Telecom consortium bid rather than a standalone OVH assessment. But it's the same ownership-and-stack alignment argued from primary sources above, now assessed the same way by the regulator this series keeps citing.

> **i What SEAL means**
>
> SEAL stands for **Sovereignty Effectiveness Assurance Level** — the European Commission's own scoring mechanism for cloud sovereignty, part of its Cloud Sovereignty Framework. The Commission's own explainer names three of the levels directly: SEAL-2 corresponds to "data sovereignty," SEAL-3 to "technological autonomy," and SEAL-4 to "full sovereignty." SEAL-2 was also the minimum level a provider needed to reach just to be eligible for this specific procurement framework at all — so OVH, STACKIT, and Scaleway's SEAL-3 rating clears that bar, not just meets it. SEAL-0 and SEAL-1 are not defined on that same Commission page; secondary sources describe them as "no sovereignty" and "jurisdictional sovereignty," but that couldn't be confirmed against a Commission primary source for this post.

A common argument against OVH, STACKIT, and Aruba as EU alternatives is that political pressure funds a burst of sovereign-cloud activity, but market gravity eventually consolidates it back into the hyperscalers it was meant to reduce dependence on (InfoWorld, June 2026). That argument fits venture-backed sovereign-cloud startups more cleanly than it fits these three. OVH's Klaba family holds roughly 82% of voting rights as of an April 2026 Euronext filing — well above their actual capital stake, thanks to a dual-class structure granting double voting rights to shares held over two years, built specifically to resist a hostile takeover. STACKIT is wholly owned by the privately held Schwarz Group (parent of Lidl and Kaufland), operated as a long-term strategic asset rather than a venture with a built-in exit. Aruba Cloud remains Cecconi-family controlled. None of this makes any of the three permanently unbuyable — a public listing keeps a tender offer structurally possible, and a private family owner can still decide to sell — but the specific consolidation mechanism the argument describes, a capital-starved provider getting acquired, doesn't apply to companies that were never venture-funded in the first place.

## What this post doesn't cover

Part 1's Question 2 asked about two related but distinct things: the technology supply chain (covered here) and who — or what — has day-to-day technical access to a system (human operators, support staff, service accounts, and increasingly AI agents). Bleu's on-site Microsoft support staff and Microsoft's own "Data Guardian" access-approval claim both touch this second question, but a proper treatment of access models, auditability, and technical scoping needs research grounded in operational practice, not a web search. That remains a separate, still-open part of this series.

This post also doesn't tell a reader whether any specific provider above is "sovereign enough" for their own situation — that isn't something a public blog post can decide from the outside. Whether a given gap matters depends on the workload: which regulatory regime it falls under, how sensitive the data is, and what risk is actually being managed. A hyperscaler's own disclosure that its global engineering teams retain some form of access may be irrelevant for a workload with no confidentiality requirement at all, and disqualifying for one under a strict national-security classification. Every provider named here — hyperscaler-run, joint-venture, or EU-native — serves real use cases; the point of laying out ownership, technology stack, and access model side by side is to make that trade-off visible, not to make the decision for the reader.

**Next in this series:** Part 3 — Who Has Access? Humans, Accounts, AI Agents →

## Related

- Sovereign-Cloud-Washing: Five Questions — the framework this post's Question 2 comes from

## Sources


- Deutsche Telekom and Huawei launch Open Telekom Cloud, "powered by" Huawei (2016 press release), the Huawei whitepaper naming FusionSphere as the platform, and WirtschaftsWoche, 2025: "Die Cloud wird nicht von Huawei betrieben" (T-Systems CEO interview) — the Open Telekom Cloud/Huawei case now covered in Part 1
- Capgemini and Orange announce plan to create "Bleu" and launch of commercial activities
- Orange newsroom: Bleu commercial launch

- next.ink: Bleu on SecNumCloud, étanchéité, and its relationship with Microsoft
- journaldunet: interview with Bleu CEO Jean Coumaros
- solutions-numeriques: SAP and Bleu
- S3NS: PREMI3NS SecNumCloud qualification announcement
- DataCenterDynamics: Thales details French sovereign cloud joint venture with Google
- Google Cloud: Sovereign Cloud overview and Sovereign Cloud Hub launch in Munich (Nov. 2025)
- Google Cloud: EU Data Boundary control package documentation and support-routing documentation
- Thales: new Thales-owned German sovereign-cloud entity with Google Cloud (May 2026)
- The Register: EU picks four sovereign-cloud providers, incl. CISPE's "sovereignty washing" objection to S3NS (April 2026)
- Microsoft: Cloud for Sovereignty (2022 private preview announcement) and Announcing comprehensive sovereign solutions (2025)
- Microsoft Learn: Microsoft Sovereign Cloud overview and Data Guardian
- Microsoft: EU Data Boundary, phase completion (Feb. 2025)
- CIO: How sovereign is Microsoft's Sovereign Cloud really?
- The Register: Microsoft exec admits it "cannot guarantee" data sovereignty
- AWS: Built, operated, controlled, and secured in Europe and AWS European Sovereign Cloud whitepaper (PDF)
- Computerworld: AWS European cloud service launch raises questions over sovereignty
- ITIF: France's Cloud Service Restrictions (SecNumCloud ownership caps)
- next.ink: inside OVHcloud's Croix factory and Roubaix datacenter and Usine Nouvelle: OVH opens a server factory in Croix
- OpenInfra Foundation: OVH Public Cloud, OpenStack Powered and OVHcloud: global infrastructure
- OVHcloud: SecNumCloud compliance and NC2 on OVHcloud (Nutanix)
- OVHcloud Blog: the CLOUD Act and the OVHcloud Group's EU jurisdiction position and OVHcloud US: CLOUD Act FAQ (OVH US LLC)
- Schwarz Digits: STACKIT product portfolio and Schwarz Group: STACKIT digitalization story
- Gardener project: STACKIT Kubernetes Engine on Gardener
- STACKIT docs: Kubernetes Engine FAQ, audit log, colocation, and Server (compute)
- Aruba Cloud: why choose Aruba, OpenStack cloud server, and VMware cloud server
- InfoWorld: Europe's cloud sovereignty push may backfire (June 2026)
- European Commission: Commission advances cloud sovereignty through strategic procurement (April 2026, SEAL-3 tender award) and Sovereign Cloud Framework explained (June 2026, SEAL definition)
- Euronext: OVHcloud information on share capital and voting rights (April 2026)