CONF42

Cloud Native 2026

Keep Calm and Run on AWS: Engineering Compliance Without Abandoning Your Stack

Dmytro Hlotenko (he/him)

Senior Cloud Operations Engineer

Sage DPW GmbH

Disclaimer

The views expressed in this presentation are solely those of the presenter in a personal capacity and do not represent the position, strategy, or opinion of any current or former employer, client, or affiliated organization. This presentation is provided for informational and educational purposes only. Nothing contained herein constitutes legal, regulatory, financial, or professional advice of any kind. References to laws, regulations, and compliance frameworks (including but not limited to GDPR, CLOUD Act, FISA 702, DORA, and NIS2) are provided for general analytical context only. The presenter is not a licensed legal professional. All regulatory and legal matters should be assessed by qualified legal counsel in the relevant jurisdiction. Benchmark results, cost estimates, and architectural assessments reflect a specific operational context at a specific point in time. Results may vary significantly based on workload, configuration, and environment. No warranty is made as to accuracy or completeness. Cloud service capabilities, legal frameworks, and regulatory guidance change frequently. Verify all information against current official documentation before making any architectural or business decisions. The presenter assumes no liability for decisions made based on the content of this session.

SERVUS FROM VIENNA

“Technology alone is not enough.
It’s technology married with the liberal arts,
married with the humanities, that yields the
results that make our hearts sing,”

Steve Jobs once said.

aws sts get-caller-identity

Dmytro Hlotenko

WHO I AM

- Crazy IT Geek
- Senior Cloud Operations Engineer at Sage
- AWS Community Builder
- AWS User Group Vienna & Linz Leader

WHAT I DO

- M.Sc. in Telecom (Ukraine, 2022)
- Started with AWS in 2020
- 6x AWS Certified
- Motorsport fan and photography hobbyist

Raise your hand if someone told you AWS is not compliant enough.

This session is about making a defensible engineering decision – not resolving geopolitics.

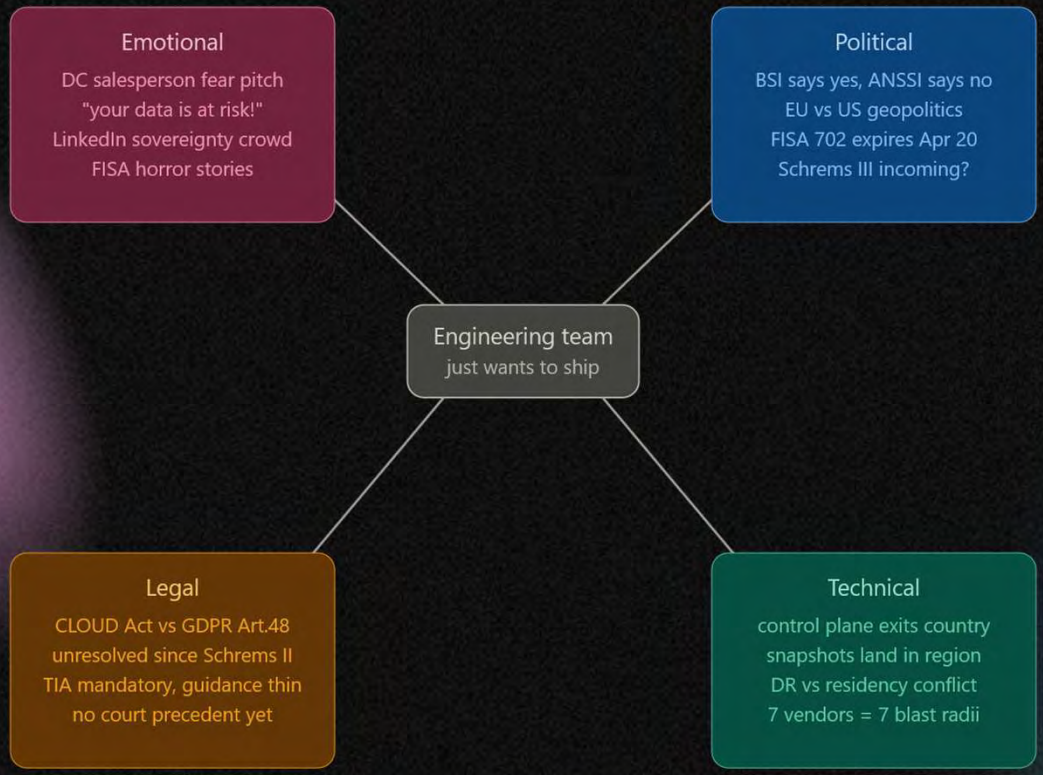
Raise your hand if someone told you AWS is not compliant enough.

Keep it raised if their alternative was simpler to operate.

This session is about making a defensible engineering decision — not resolving geopolitics.

THE NOISE

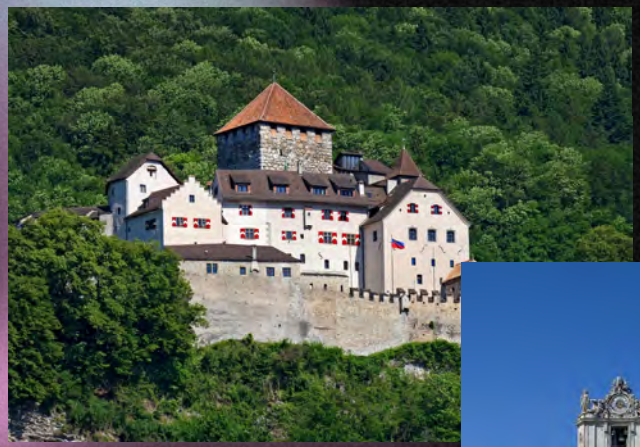
02.



all four hit your team simultaneously — none of them are your job to resolve alone

02.

Data resilience is local. Data sovereignty is legal.



geography does not equal jurisdiction

Data Residency = where the data sits. A pin on a map.
Data Sovereignty = who has legal control over access.

Authority, not geography.

The Compliance Trap: most organizations blur these two concepts entirely.
Complexity comes from the fantasies.

CLOUD Act regulates service providers, not software.

Control of the management plane dictates jurisdiction.
Self-hosted = outside scope
Managed service = US jurisdiction

CLOUD Act & FISA 702

Jurisdiction attaches to the entity, not the data→US company must produce data within its "possession, custody, or control" – regardless of location

FISA 702: warrantless, targets non-US persons, reauthorized 2024

Unlike CLOUD Act (requires warrant), Section 702 allows warrantless collection on non-US citizens

The Safety Valve: vendors point to court challenge option — functionally irrelevant in practice

AWS Track Record: zero enterprise content disclosures (per AWS transparency reports)

DORA & NIS2 – what they actually require

DORA (Financial Sector): supply chain risk, concentration risk, exit strategy→ Mandates resilience and third-party risk management.

Not EU-only cloud.

NIS2 (Critical Infrastructure): jurisdiction analysis of third-party suppliers→ Expands who qualifies as critical.

Forces supply chain security review.
Not EU-only cloud. Neither mandates EU-only cloud. They mandate risk assessment and documented controls.

"If you read the actual text of DORA and NIS2, the words 'European-only cloud' do not appear."

Core Question:
"Who operates the control plane?"

Path A: EU Legal Entity / Self-Managed

Result: Outside US ECSP Scope (No CLOUD Act exposure).

Why: Because your internal team (or a purely European managed service provider) holds exclusive administrative access, no US entity has "possession, custody, or control" of the environment.

Path B: US Legal Entity / Managed Service

Result: CLOUD Act Applies.

Why: Because a US-based company operates the management plane, pushes updates, or holds admin credentials, they have legal "control" over the service—triggering US jurisdiction.

Iceberg Effect

Visible Costs (The Spreadsheet)
The easily quantifiable metrics that make it into the initial budget approval.

Migration Services
New Licensing & Dual-Running
Data Egress Fees

Invisible Costs (The Reality)
The strategic and human costs that destroy engineering ROI, but never appear on the CFO's spreadsheet.

Velocity Loss
MTTR Increase
Recruiting Constraint
Opportunity Cost

5% of our systems are IaC,
the rest are Infra in Powerpoint
- Azuros Clouddapi

The spreadsheet versus reality

When leadership plans a migration to a sovereign cloud, they look at compute costs, storage rates, and compliance checklists. What they completely miss is the operational friction, the destruction of team muscle memory, and the chaos of vendor sprawl.

12–18 Months to Rebuild 3am Incident Confidence

Knowledge Bias Never Appears on Migration Proposals

7 Vendors × 7 SLAs × 7 Escalation Paths × 7 Blast Radius

What ESC actually added – January 2026

ws-eusc — separate partition, region eusc-de-east-1 (Brandenburg, DE)Not a new datacenter.

A completely separate cloud.EU-only operational staff (EU residents/citizens) — solves the "who" question

All metadata, CloudTrail, IAM stays in EU — plugs the telemetry leak

Dedicated EU Trust Service Provider for certificates — root of trust is European
Independent control plane — if global AWS goes down, ESC stays up

DORA SRF framework coverage + BSI C5 certified

Regulation × requirement × AWS tool matrix

"Stop treating the cloud as a monolith. Map the exact legal requirement to the exact technical control."

Regulation	Data Residency (Where)	Operational Sovereignty (Who)	Audit Trail (Proof)	Key Management (Lock)
GDPR *(Schrems II / Art. 48)*	Standard EU Region *(Covered)*	AWS ESC *(Standard requires TIA)*	CloudTrail *(Covered)*	KMS + XKS *(Requires Supplementary Measure)*
DORA *(Financial Resilience)*	Multi-AZ / Region *(Covered)*	Outposts *(Requires Exit Strategy)*	Audit Manager *(Covered)*	KMS *(Covered)*
NIS2 *(Critical Infra)*	Standard EU Region *(Covered)*	AWS ESC *(Covered)*	CloudTrail + Security Hub *(Covered)*	KMS *(Covered)*

Where The Gap Remains

Amazon.com Inc. = Delaware corporationA
WS European Sovereign Cloud GmbH = 100% wholly-owned subsidiary

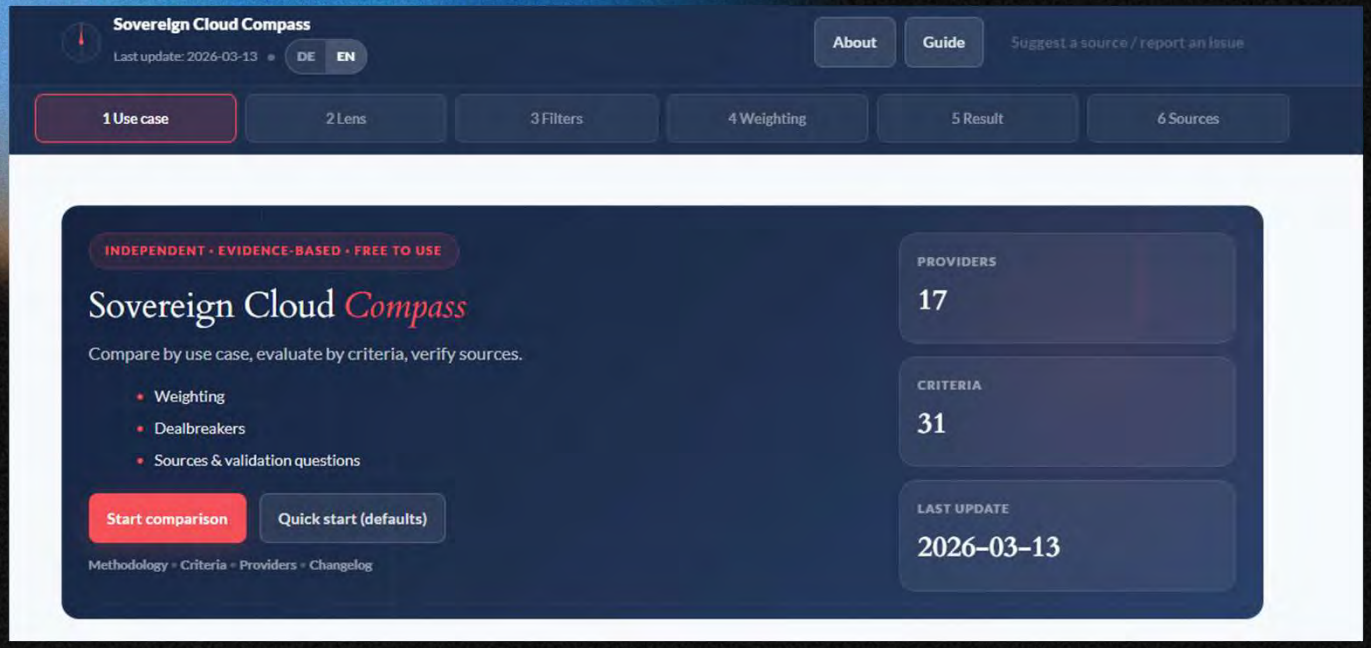
CLOUD Act applies at parent level
Subsidiary structure doesn't sever US jurisdiction
FISA 702: Amazon = US ECSP → warrantless access structurally possible
No SecNumCloudBSI: approved (technical isolation sufficient)
ANSSI: rejected (US ownership = disqualifier)

"Operational sovereignty: yes. Jurisdictional sovereignty: no."

Dimension	Outposts (std. AWS)	ESC (region only)	ESC + Outposts
Data residency (AT/EU)	✅	✅	✅
Metadata in EU	⚠ AWS Region control plane	✅	✅
EU-only ops access	❌	✅ (transition)	✅ (transition)
GDPR data residency	✅	✅	✅
GDPR oper. sovereignty	❌	✅ caveats	✅ caveats
CLOUD Act / FISA 702	❌ full exposure	⚠ reduced	⚠ reduced
NIS2 (critical infra)	⚠ interp.-dep.	✅ covers most	✅ covers most
DORA (financial sector)	⚠	✅ ESC SRF	✅ ESC SRF
In-country residency (AT)	✅ AT DC	❌ DE only	✅ AT DC
SecNumCloud (ANSSI)	❌	❌	❌
BSI C5	⚠	✅ path exists	✅ path exists
Control plane isolation	❌ shared global	✅ eusc-de-east-1	✅
Cert. authority (EU TSP)	❌	✅ EU-TSP	✅

Tipp for friends!

https://www.sovereigncloudcompass.de/



Let’s talk about AWS Outpost

Why We Looked At Outposts

SaaS platform. Enterprise customers. Austrian regulatory environment.

Existing AWS stack → years of operational muscle memory, IaC, runbooks, tooling.

Hypothesis: Outposts = data residency + keep the stack

Regulatory pressure said: data must stay local.
Business said: we cannot rebuild everything from scratch.

Engineering said: let's look at what AWS has. Outposts was originally built for low-latency edge compute. **The compliance story came later.**

What Outposts Was Actually Built For

Original use case:

- low-latency edge compute
- Manufacturing: automated operations next to machinery
- Retail: local EPOS, sub-10ms response
- Healthcare: real-time imaging, local patient data
- Telecoms: virtual network functions at edge

The compliance story was retrofitted later.

"Outposts is an engineering solution for physics, not a legal shield for jurisdiction."

What Outposts actually solves

Outposts is an engineering solution for physics, not a legal shield for jurisdiction.

Physical Data Residency

Context: Storing data in your own data center.

Talking Point: Outposts puts AWS-designed hardware directly into your physical facility.

Low-Latency Local Compute

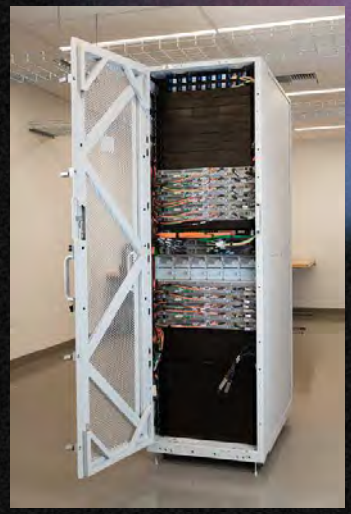
Context: Solving the speed of light.

Talking Point: Sometimes the cloud is just too far away.

Familiar AWS APIs and Tooling

Context: Avoiding the "What you technically lose" tax.

Talking Point: The magic of Outposts is that you don't have to rewrite your infrastructure code.

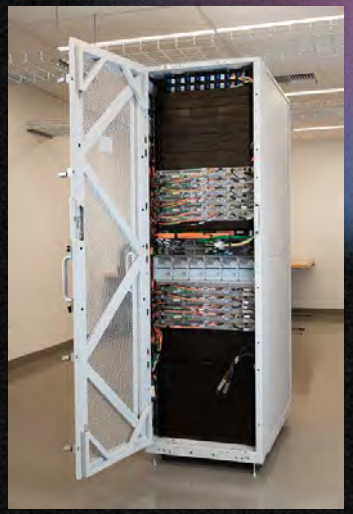


it is for organizations that do not have strict operational sovereignty requirements.

What Outposts quietly doesn't solve

You're paying colocation fees on top of Outposts costs for a compliance story that doesn't hold up under scrutiny.

Control Plane Metadata → Parent Region
Context: The technical architecture of managed services.
Talking Point: Outposts is not a standalone island; it is an extension of an AWS Region.
Solved by AWS ESC!



Operational Staff: Global AWS
Context: The "Who" of operational sovereignty.
Talking Point: Remember the rule: Who operates the control plane? When a hard drive fails on an Outpost, or a firmware update is pushed, it is managed by AWS Site Reliability Engineers (SREs).

CLOUD Act Exposure: Identical to eu-central-1
Context: The legal reality of the invisible tether.
Talking Point: Because AWS operates the control plane and maintains administrative access to the hardware, the legal entity (Amazon Web Services) has "possession, custody, and control" of the environment.

Services You Lose on Outposts

Not available locally on Outposts (run in parent region or not at all):

Lambda — no serverless compute locally, somehow via IoT Core
Athena, Glue — no serverless analytics
SageMaker Studio — no local ML workflows
Redshift — no local data warehouse
S3 Batch Operations — no bulk object processing
Transit Gateway — network architecture changes required
ALB: no mTLS, no sticky sessions, NLB also different
EKS is striped down
S3 on Outposts limits: has to be added separately

Benchmark: Methodology

Goal: measure what users feel, not what the network can do.

There is no way to directly “translate” VMWare Mhz to the Outpost capacity.

Azure Austria (not AWS → AWS — that's not a real test)

Why: our production traffic was predominantly local AT/DE. Azure AT represents a realistic external origin vs both AWS Frankfurt and on-premise Vienna DC.

Load tool: Locust + Playwright

- Playwright: real browser sessions, not API hammering
- Scenarios defined with support + dev teams: core HR/Payroll user flows
- Deployed on Azure Container Instances (Bicep IaC)

Metrics we tracked:

- Response time (click → fully rendered screen)
- Failure rate (at what concurrency does the server drop connections)
- RPS per user session

Environment: mirrored architecture DC vs AWS — no refactoring, like-for-like.

Benchmark: Why Azure Austria as Traffic Source

Goal: measure what users feel, not what the network can do.

The problem with obvious test setups:

Option 1: Test from AWS → AWS→ Both endpoints on same backbone. Not representative of real user traffic.

Option 2: Test from office/DC in Vienna→ Same network as production. Masks real-world latency.

Our approach: Azure Austria (Vienna region)

Different cloud provider = different network path

Represents external origin similar to enterprise customer traffic

Our Cloudflare analytics showed traffic predominantly AT/DE

Azure Austria sits "across the table" from both our DC and AWS Frankfurt

You can't benchmark cloud vs DC if both the load generator and the target are on the same network.

Benchmark: The vCPU Discovery

vCPU ≠ core. This will cost you.

DC config: NUMA — 2 sockets, 2 physical cores each = 4 real cores (+ SMT threads)

AWS instances tested: 2 vCPU, 4 vCPU, 8 vCPU at R, M and C specs between 5-8 Intel based gens.

Concurrency	4 vCPU (SMT threads)	4 vCPU (physical cores)	DC (4 real cores)
25 users	parity	parity	baseline
100 users	degraded, errors	parity	baseline

Finding: at high load, SMT threads are not equivalent to physical cores for this workload.To match DC performance at 100 concurrent users → need 8 vCPU on AWS (SMT) or 4 physical-core instance.

M-class instances outperformed C and R on this workload — multitenant host, single instance measurement, neighbor noise visible on C/R under light background load. Be careful with per vCPU licensing!

Storage Trap: gp3 Only, No io1/io2

Outposts gen 2: EBS volume types available

What this means for database workloads:

Any CPU gains from compute get erased under high IOPS load

io2 Block Express: sub-millisecond latency — not available

gp3 ceiling: 16,000 IOPS per volume — hard limit

Need more? RAID 0 striping across volumes — more complexity, more failure points

If your workload is IOPS-sensitive, benchmark storage separately before you benchmark CPU.

Storage Trap: gp3 Only, No io1/io2

We didn't wait for hardware. We simulated Outposts in the cloud.

Methodology:

Took AWS instances matching Outposts gen 2 specs: older CPU generation + gp3 storage limits (max 16,000 IOPS, 1,000 MiB/s)

Ran identical benchmark scenarios against DC configuration

Result: DC was clearly ahead

Why DC won:

Real physical cores vs SMT threads at high concurrencyio1/io2 IOPS headroom vs gp3 hard ceiling

No neighbor noise on dedicated iron

NUMA topology matched to the actual workload

What this told us: Any CPU gains on Outposts hardware get erased under real mixed load — web + batch + DB hitting storage simultaneously.We didn't need to wait for a rack delivery to know the answer.

Benchmark: Results

Same hardware generation (Xeon ≈ M5 class): -5% to +10% vs DC
Within measurement noise. Effectively parity.

Current generation instances: +10-25% better response time and failure rate vs DC config
Not dramatic — but consistent across test runs. Outposts hardware penalty:

Outposts ships ~2 generations behind current region

Tested baseline → Outposts-equivalent instances: -15 to -20% performance
You pay Outposts premium to run hardware that's slower than what's in eu-central-1 today.

Hybrid Approach & Sizing Reality

Hybrid: not everything needs the same compliance tier

→ Staging, test, non-PII workloads: standard AWS region→ Production compute + customer data: Outposts (if residency required)

This cuts Outposts footprint significantly.

Sizing reality:1:1 mapping from DC to Outposts is impossible
Different CPU/memory pairs, different NUMA topology
vCPU generation gap compounds the problem
You will overprovision. Plan for it explicitly.
Ideal sizing doesn't exist — you'll discover it in production

CapEx: What the Business Case Shows

What appears in the approval document:

Hardware lease (3-year term commitment)
Software licenses
Migration services

Total: looks manageable."The business case for an Outpost or private cloud usually only includes the hardware lease and the software licenses."

CapEx: What the Business Case Shows

What doesn't appear in the approval document:

Power: single rack draws 15–30 kVACooling: hot/cold aisle, sufficient BTU overhead

Multi-rack HA across two sites → €30,000–40,000/month power & cooling alone

DC prep work: months of pre-installation before AWS ships anything

Dedicated uplink: minimum 500 Mbps, 1 Gbps recommended, redundant

You don't get generator + UPS that a real DC gives you — unless you pay for it separately
Cloud economics don't apply here.

You are losing your DC certifications.

You're not renting compute. You're running a datacenter that happens to use AWS APIs.

DC Readiness Burden

If you run cloud, AWS owns the infrastructure problem. With Outposts – you do.

Before AWS installs anything, you need:

Physical space: rack dimensions, weight, floor load
Power: dedicated circuit, UPS, generator capacity
Cooling: hot/cold aisle, sufficient BTU
Network: dedicated uplink to parent region, redundant paths
Firewall decision: managed or dedicated appliance (and someone who knows it)

What datacenter gives you that Outposts doesn't:

Multiple locations, massive generator + battery backup, redundant power feeds
Outposts HA = second rack at second location = double the cost, double the complexity
The amount of preparatory work — by you and your DC — is not in the sales deck.

The Backup Trap

Your compliance story says Vienna. Your snapshots say Frankfurt.

Default behavior:

EBS snapshots → parent region (S3, Frankfurt) automatically
AWS Backup → same problem
The "fix" — S3 on Outposts: Local, but expensive. Very expensive.

Veeam, Commvault on Outposts: file-level backup onlyNo VSS, no full Windows backup, no configuration state.
N2W is the most serious from all Marketplace Outpost certified platform.
No deduplication. Needs EBS buffer volumes as temp + target.
Configuration drift will kill your recovery. Everything must be repeatable before you trust any restore.

Custom archistration, dependency on the external non-AWS targets like local alternatives for target storage (AT):APA-IT, Exoscale, Azure Blob Storage Austria (must be encrypted before upload!), whatever

DR Paradox

True data residency = data doesn't leave the country.
Working DR = you need a recovery target somewhere else.

These two requirements are in structural conflict by design. Primary in Vienna + DR in Frankfurt = violates Austrian residency

Primary in X + DR in X = 3-2-1 rule compromised

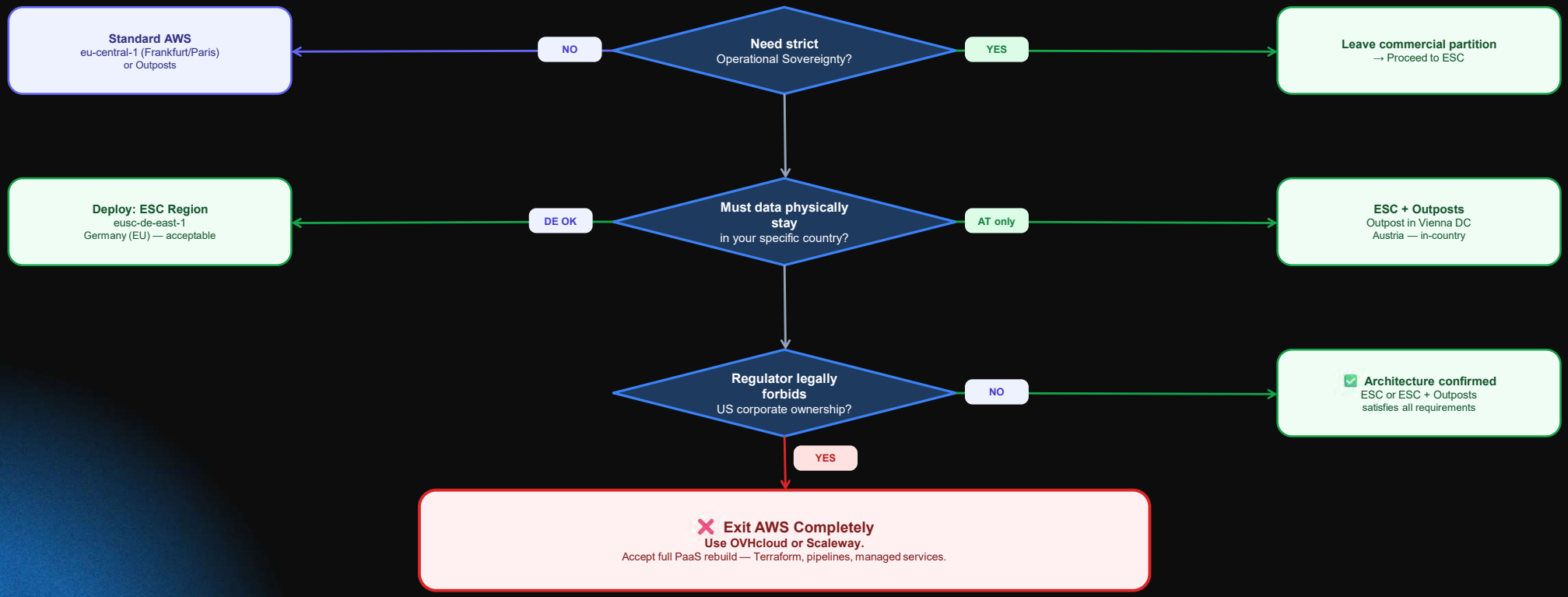
Three exits from this trap — none perfect:
Dual-DC in-country — second Austrian DC, far enough for disaster isolation. Doubles CapEx/OpEx.
Partial residency — encrypted backups allowed cross-border, active compute stays local. Shifts risk to legal team.
Accept the gap — country-wide disaster risk < cost of second domestic DC. Document the decision.Nobody puts this in the sales deck.

As recent GCC events show – current Region-Availability zones concept doesn’t guarantee you safety.

So what do we do?

Operational Sovereignty — Architecture Decision Tree

Start at the top. Follow YES or NO at each decision to reach your deployment architecture.



Decision framework – 3 questions

Q1: What does your regulator actually require?
Context: Forcing the compliance team to commit.
Talking Point: You cannot build an architecture based on a LinkedIn post.
You must ask your legal or compliance team

Q2: Who needs operational access to your environment?
Context: The "Who" of the control plane.
Talking Point: This question exposes the operational reality of the workload.

Q3: Where must backups and DR target physically land?
Context: Exposing the Trap #1 and Trap #2 realities.
Talking Point: If your regulator mandates that primary data must stay in Austria, where does the Disaster Recovery site go?

KEY TAKEAWAYS

Geography ≠ jurisdiction.
Control plane determines exposure, not zip code.
DORA and NIS2 require risk assessment and controls — not EU-only cloud.
ESC is operationally sovereign. Jurisdictionally — Delaware is still Delaware
Outposts solves physics (latency, residency). It does not solve law.
ESC + Outposts is the most compliant hyperscaler architecture possible. You will pay for it.
Benchmark your actual workload. vCPU generation and SMT vs physical cores matter more than instance names.

Ask three questions before any architecture decision: What does your regulator require? Who operates the control plane? Where must backups land?Your job is not to resolve geopolitics.

Your job is to make a defensible engineering decision with the information available today.

Thank you!

Dmytro Hlotenko (he/him)

dmytro.hlotenko@sage.com

Experience brought by:

Dmytro Hlotenko (he/him)

Senior CloudOps + AWS Community Builder