Digital Sovereignty on Oracle OCI: A Comprehensive Analysis of the European Union and German Market

Executive Summary

The European digital landscape is currently undergoing a seismic shift, driven by a confluence of geopolitical tension, regulatory tightening (GDPR, Schrems II, NIS2), and a strategic imperative for technological autonomy. For enterprises and public sector organizations in Germany and the broader European Union (EU), the consumption of cloud services is no longer merely a question of agility and cost; it has become a fundamental question of jurisdiction, control, and survival in a fragmented global digital economy.

This research report provides an exhaustive, expert-level analysis of Oracle Cloud Infrastructure's (OCI) response to these sovereignty demands. Unlike hyperscale competitors who often overlay data residency policies onto a shared global control plane, the analysis indicates that Oracle has adopted a strategy of **architectural bifurcation**. Through the implementation of distinct "Realms"—specifically the OC19 realm for the EU Sovereign Cloud—Oracle effectively severs the control plane dependencies that historically linked European workloads to United States administrative domains.

Our analysis, grounded in the provided 8-level Sovereignty Framework, reveals several critical insights:

1. **Architecture as Policy:** Oracle's primary differentiator is the "Realm" construct, which provides physical and logical isolation at the network and identity layers. This prevents the "fate-sharing" and extraterritorial data leakage risks inherent in global commercial clouds.
2. **Operational localization:** The establishment of separate, EU-domiciled legal entities to own and operate the infrastructure addresses the "Operational Sovereignty" layer more aggressively than standard "follow-the-sun" support models.
3. **The German Anchor:** The strategy is heavily anchored in Germany, with the **EU Sovereign Central** region in Frankfurt (eu-frankfurt-2) operating alongside—but distinctly separate from—the commercial Frankfurt region (eu-frankfurt-1). This dual-presence offers German entities a unique choice between global integration and sovereign isolation within the same metropolitan area.
4. **Service Parity:** Contrary to the industry trend where sovereign clouds often lag in feature availability, Oracle maintains near-parity, including the availability of high-demand services like Generative AI within the sovereign boundary.

This report dissects these offerings—**Oracle EU Sovereign Cloud**, **OCI Dedicated Region**, and **Oracle Alloy**—providing the technical depth, implementation patterns, and due diligence criteria necessary for German CIOs, CISOs, and compliance officers to make defensible architectural decisions.

1. Sovereignty Framework & Oracle's Distributed Cloud Strategy

To rigorously evaluate Oracle's offerings, we apply the 8-Level Cloud Sovereignty Framework. This model moves beyond simple "data residency" to encompass the full spectrum of control, from physical access to legal immunity.

1.1 The Challenge of the "Global Control Plane"

In standard hyperscale architectures, while customer data (Data Plane) may sit in Frankfurt, the systems that manage that data—identity providers, billing aggregators, and patch management systems (Control Plane)—often reside in the US or rotate globally. This creates a vector for extraterritorial data access (e.g., via the US CLOUD Act) and operational dependency (e.g., a US outage affecting German resources).

1.2 Oracle's Strategic Response: The Realm Architecture

Oracle's fundamental response to this challenge is the concept of a **Realm**. A realm is a logical collection of regions that are isolated from each other. They share no physical infrastructure, accounts, data, resources, or network connections with other realms.[1]

- **OC1:** The Commercial Public Cloud realm (Global).
- **OC19:** The EU Sovereign Cloud realm (EU-only).
- **Government Realms:** Separate realms for US (OC2, OC3), UK (OC4), and Australian defense sectors.[2]

This architectural decision means that OC19 is not just a "policy wrapper" around OC1; it is a distinct cloud ecosystem.

2. Oracle EU Sovereign Cloud: The Public Sovereign Option

The **Oracle EU Sovereign Cloud** is the flagship public offering for European organizations requiring strict adherence to EU data privacy and sovereignty laws. Launched in 2023, it is designed to host sensitive data and applications for both public and private sectors.[3]

2.1 Offerings Overview

The EU Sovereign Cloud is a comprehensive cloud platform that provides the same services as Oracle's commercial regions but with stricter residency and operational controls.

- **Status:** Generally Available (GA) as of July 31, 2023.[4]
- **Core Promise:** Data residency, data localization, and operations restricted to EU residents and EU legal entities.[3]
- **Pricing:** Oracle maintains standard public cloud pricing for this offering, avoiding the "sovereignty premium" often charged by managed service providers overlaying sovereign controls.[6]

2.2 EU/Germany Availability and Infrastructure

The physical footprint of the EU Sovereign Cloud is entirely contained within the European Union.

2.2.1 Region Specifications

The cloud operates out of two dedicated regions. It is crucial to note that these are **distinct** from the commercial regions in the same cities.

Feature	EU Sovereign Central (Germany)	EU Sovereign South (Spain)
Location	Frankfurt, Germany	Madrid, Spain
Region Identifier	eu-frankfurt-2	eu-madrid-2
Region Key	STR	VLL
Realm Key	OC19	OC19
Availability Domains	1 (with 3+ Fault Domains)	1 (with 3+ Fault Domains)
Physical Isolation	Separate data halls and caging from Commercial Frankfurt (eu-frankfurt-1).	Separate data halls and caging from Commercial Madrid (eu-madrid-1).
Source	[4]	[4]

2.2.2 The "Split-Region" Dynamic in Frankfurt

For a German customer, the existence of eu-frankfurt-1 (Commercial) and eu-frankfurt-2 (Sovereign) offers strategic flexibility but requires careful configuration management.

- **Commercial (eu-frankfurt-1):** Operated by Oracle Corporation (Global). Subject to follow-the-sun support.
- **Sovereign (eu-frankfurt-2):** Operated by Oracle EU Sovereign Cloud entities. Restricted to EU-resident support.
- **Connectivity:** There is **no automatic or readily established data path** connecting these two regions. They exist in parallel universes. Cross-region communication must be explicitly engineered by the customer, typically via peering at a telecommunications provider or through on-premises routing, ensuring no accidental data leakage occurs between the sovereign and commercial environments.[5]

2.3 Operational Sovereignty: The Human Element

The EU Sovereign Cloud addresses the "Operational Sovereignty" (Level 4) requirement through strict personnel controls.

- **EU-Resident Restriction:** Physical and logical access to the infrastructure is restricted

to **EU residents**. This applies to the Data Center Operations (DCO) teams racking servers in Frankfurt and the remote Site Reliability Engineers (SREs) managing the control plane.[3]

- **Legal Entity Structure:** The hardware and assets are owned by dedicated **EU Sovereign Cloud legal entities**. These are incorporated in EU member states (Germany, Spain, Ireland, Romania, Poland, Czech Republic). This structure is designed to create a corporate veil, arguing that the data is not under the control of a US entity, thereby attempting to mitigate the reach of US extraterritorial warrants, although the ultimate parent remains Oracle Corporation.[3]
- **No Non-EU Data Transfers:** The operational governance model ensures that monitoring data, logs, and ticketing information do not leave the EU boundary, aligning with Schrems II requirements regarding data transfers to "non-adequate" jurisdictions.[5]

3. OCI Dedicated Region: The "Air-Gapped" Option

For organizations where even a sovereign public cloud carries unacceptable risk—or where data volume and latency dictate on-premises processing—Oracle offers the **OCI Dedicated Region**.

3.1 Overview and Architecture

OCI Dedicated Region (formerly Dedicated Region Cloud@Customer) places a full-scale Oracle Cloud region *inside* the customer's data center.

- **Status:** Generally Available (GA).[9]
- **Service Parity:** Unlike "Edge" solutions from other providers that offer a subset of services, Dedicated Region offers the **full OCI catalog** (150+ services), including Autonomous Database, Exadata, and SaaS applications like Fusion Cloud.[9]
- **Footprint:** The latest version ("Dedicated Region25") has a reduced footprint, starting at as few as three racks, making it accessible to a broader range of German enterprises beyond just hyperscale users.[11]

3.2 Sovereignty Implications

This model achieves the highest scores across the Sovereignty Framework:

- **Data Residency & Localization (Level 1 & 2):** Data never leaves the customer's physical premises. The "Region" is physically located in the customer's German data center.[10]
- **Isolation Model (Level 7):** The region is dedicated to a single customer (single-tenant). It creates a private "Realm" specifically for that customer.
- **Control Sovereignty (Level 5):** The customer controls physical access to the racks. Oracle manages the infrastructure remotely, but the customer acts as the "gatekeeper" for physical entry.[12]

3.3 Connected vs. Disconnected Modes

While typically managed via a connection to the Oracle control plane (for billing and patching), Oracle also offers **Isolated Region** configurations for national security purposes that can operate in a fully **disconnected (air-gapped)** mode. This is relevant for German defense and intelligence use cases requiring absolute isolation from the public internet.[2]

4. Oracle Alloy: The Partner-Led Sovereign Cloud

Oracle Alloy represents a strategic pivot to "Partner Sovereignty." It allows local entities—such as German telecommunications providers (e.g., Deutsche Telekom/T-Systems, though specific German Alloy partners are not explicitly named in the snippets, the model is designed for this profile)—to become cloud providers themselves.

4.1 The "Provider" Model

With Alloy, the partner does not just resell OCI; they **operate** it.

- **Status:** Generally Available (GA).[13]
- **Role Shift:** The partner takes over the "Level 1" support and operations. They act as the cloud provider for their region.
- **Branding & Commercials:** The partner sets the pricing, currency, and commercial terms. The console is branded with the partner's identity, not Oracle's.[13]

4.2 Sovereignty Benefits for Germany

- **Jurisdictional Control:** If a German public sector entity buys cloud services from a German Alloy partner, they are contracting with a German legal entity subject to German law. This creates a robust legal shield.[13]
- **Customization:** Partners can extend the platform with their own local services (e.g., specific German government compliance reporting tools) integrated directly into the console.[14]
- **Data Residency:** The Alloy instance runs in the partner's data center (in Germany), ensuring strict localization.[15]

5. Detailed Controls Matrix

The following matrix maps Oracle's features to the 8-Level Sovereignty Framework.

Feature / Offering	Sovereignty Level(s) Covered	EU/Germany Availability	Operational & Support Bounds	Legal/ Contractual Posture	Dependency	Status	Source
EU Sovereign Cloud (OC19)	**1, 2, 3, 4, 6, 7**	**Yes** (Frankfurt eu-frankfurt-2)	Ops & Support by EU residents only. Physical access restricted to EU citizens.	EU Legal Entities (Germany, Spain, etc.). Data stays in EU.	None (Standalone Realm)	**GA**	3
Dedicated Region	**1, 2, 5, 7**	**Yes** (Customer Premise)	Oracle remotely managed; Customer controls physical access.	Customer owns the site; Oracle provides service.	Customer Facility	**GA**	9
Oracle Alloy	**4, 6, 8**	**Yes** (Partner-led)	Partner controls Ops & Support.	Contract is between Customer & Partner (German entity).	Partner Infrastructure	**GA**	13
External Key Management (EKMS)	**5** (Control)	**Yes** (All Regions)	Customer holds keys (HYOK). Oracle has zero knowledge of key material.	Customer retains full cryptographic control.	Thales/External HSM	**GA**	16
Operator Access Control (OpCtl)	**3, 4** (Access)	**Yes** (Exadata, Autonomous)	Customer must Approve/Audit every operator access request.	Formal audit trail of all operator actions.	Exadata Infrastructure	**GA**	18
Confidential Computin	**5** (Control)	**Yes** (Frankfurt eu-frank	Hardware-level memory encryption (AMD	Protects data-in-use from hypervisor/	Specific Compute Shapes	**GA**	20

g		furt-2)	SEV-SNP).	admin access.			
EU-Only Support	**4** (Operational)	**Yes** (Default in OC19)	Support data & tickets processed only by EU staff.	Aligned with GDPR/Schrems II.	None	**GA**	[3]
Compliance (C5, etc.)	**8** (Ecosystem)	**Yes**	Audited by BSI-approved auditors.	C5 Type 2 Attestation.	None	**GA**	[22]

6. Technical Sovereignty Controls: A Deep Dive

Sovereignty is not achieved by policy alone; it requires rigorous technical enforcement. Oracle provides a suite of controls that allow customers to mathematically and architecturally enforce sovereignty.

6.1 Cryptographic Control: External Key Management (EKMS)

For "Control Sovereignty" (Level 5), Oracle allows customers to move beyond "Bring Your Own Key" (BYOK)—where the provider eventually sees the key—to "Hold Your Own Key" (HYOK).

- **Mechanism:** Using the **External Key Management Service (EKMS)**, customers deploy a Key Management System (such as Thales CipherTrust) outside of OCI (e.g., on-premises in Munich or in a third-party colocation).
- **Operation:** When OCI needs to decrypt data (e.g., to start a Block Volume), it sends a request to the external HSM. The key material *never* enters OCI; the cryptographic operation happens externally.
- **The "Kill Switch":** If the customer revokes the connection to the external HSM, the data in OCI is instantly rendered inaccessible, effectively cryptographically shredding it. This provides a definitive exit strategy and control against compelled access.[16]

6.2 Access Governance: Operator Access Control (OpCtl)

One of the most profound fears in sovereign cloud adoption is the "Administrator Access" vector—the risk that a cloud provider employee could access sensitive memory or storage during maintenance.

- **The Solution: Operator Access Control (OpCtl)** is a compliance audit system designed for Exadata Cloud@Customer and Autonomous Database on Dedicated Infrastructure.
- **Workflow:**
  1. Oracle Operator requests access to a resource for maintenance.
  2. The Customer receives a notification.

3. The Customer **approves** or **denies** the request.
4. If approved, the operator is granted time-bound, scoped access.
5. All actions taken by the operator are logged and auditable by the customer.
6. The customer can **revoke** access at any moment.

- **Significance:** This effectively places an "airlock" between the Oracle control plane and the customer's data plane, enforcing **Data Access Sovereignty (Level 3)**.[18]

6.3 Hardware Isolation: Confidential Computing

To protect data *in use* (while being processed in memory), OCI offers **Confidential Computing** using AMD EPYC processors with Secure Encrypted Virtualization (SEV) and Secure Nested Paging (SNP).

- **Availability:** Confirmed available in the **EU Sovereign Central (Frankfurt)** region (eu-frankfurt-2).[20]
- **Function:** It encrypts the memory of the Virtual Machine. Even if a malicious actor (or a compromised hypervisor) attempts to dump the RAM, they would only see encrypted data. This removes the cloud provider from the "Trusted Computing Base" (TCB) for the memory stack.[17]

6.4 Network Isolation: The Realm Boundary

The concept of the **Realm** (OC19) is the primary network control.

- **DNS Isolation:** Sovereign regions utilize distinct DNS endpoints (e.g., *.oraclecloud.eu variants) that differ from the commercial public cloud.
- **No Peering:** There is no backbone peering between OC1 and OC19. Data cannot "accidentally" flow to the US because the routes do not exist in the software-defined network (SDN).
- **Interconnects:** Customers needing to connect to the Sovereign Cloud use **FastConnect**, specifically peering with the sovereign BGP ASN (11506 for EU Sovereign Cloud), ensuring traffic enters directly into the sovereign boundary without traversing the public internet.[7]

7. Operational & Legal Posture

7.1 Legal Entity Structure

Oracle has engineered a corporate structure to support sovereignty claims. The EU Sovereign Cloud is not operated by "Oracle Corporation" (US). It is operated by a network of **EU-domiciled legal entities**.

- **Locations:** These entities are incorporated in **Germany**, Spain, Ireland, Romania, Poland, and the Czech Republic.[5]

- **Personnel:** Employment contracts for staff accessing OC19 are held by these specific EU entities. This ensures that the staff are subject to EU labor and privacy laws.[5]

7.2 Compliance Ecosystem (Level 8)

Oracle OCI holds a **C5 (Cloud Computing Compliance Criteria Catalogue)** attestation from the BSI (German Federal Office for Information Security).

- **Status:** The C5 attestation covers a broad range of OCI services and is a critical requirement for German public sector usage.
- **EUCS:** Oracle aligns with the EU Cloud Code of Conduct and is positioning for the upcoming EU Cybersecurity Certification Scheme (EUCS).[22]
- **Schrems II:** The combination of EU-resident ops, EU-legal entities, and technical controls (OpCtl, EKMS) constitutes Oracle's supplementary measures to meet Schrems II requirements for international data transfers.[3]

8. Limitations & Gaps

While robust, the Oracle EU Sovereign Cloud solution is not without limitations that German customers must weigh.

- **Ecosystem Bifurcation (The "Marketplace" Gap):** Because OC19 is a separate realm, the vast ecosystem of third-party images and stacks available in the commercial OC1 Marketplace is not automatically available. ISVs must explicitly publish their solutions to the OC19 realm. This can lead to a "feature gap" where a specific firewall appliance or tool available in the commercial cloud is missing in the sovereign cloud.[26]
- **Service Release Latency:** While Oracle commits to service parity, the operational requirement to validate updates with EU-resident staff can introduce a latency in feature rollouts compared to the global commercial cloud. However, critical services like **Generative AI** are already available in eu-frankfurt-2, suggesting this lag is minimized for high-priority services.[27]
- **Migration Complexity:** There is no "easy button" to move a workload from eu-frankfurt-1 (Commercial) to eu-frankfurt-2 (Sovereign). Because they are different realms, migration requires a full backup/restore or a lift-and-shift operation, similar to migrating between two different cloud providers.[28]
- **Cost of Complexity:** Managing resources across two realms (if a customer has both sovereign and non-sovereign workloads) requires distinct identity management and governance strategies, increasing operational overhead.
- **Telemetry Data:** While customer content is strictly resident, certain low-level telemetry (e.g., aggregated billing data) typically must flow to a central global system for accounting. Customers should verify the specific "data definitions" in their contracts to understand exactly what metadata is excluded from the residency guarantee.[29]

9. Implementation Patterns for Germany

Based on the technical capabilities, we identify three primary implementation patterns for German organizations.

9.1 Pattern A: The "Fortress Germany" (Strict Sovereignty)

- **Target:** Federal agencies, Defense, Critical Infrastructure (KRITIS).
- **Architecture:**
  - Deploy all resources exclusively in **EU Sovereign Central (Frankfurt)** (eu-frankfurt-2).
  - Use **Dedicated Region** if the scale justifies it (> $1M/year commitment typically).
  - Enable **Operator Access Control (OpCtl)** on all database resources.
  - Use **External KMS** with an on-premises HSM in a German federal datacenter.
  - **Network:** Connect via FastConnect using BGP ASN 11506; block all public internet egress.

9.2 Pattern B: The "Sovereign Hybrid" (Balanced)

- **Target:** Regulated industries (Finance, Healthcare).
- **Architecture:**
  - Core sensitive data (PII, financial records) resides in **EU Sovereign Central (Frankfurt)**.
  - Less sensitive workloads (public web front-ends, non-sensitive analytics) reside in **Commercial Germany Central (Frankfurt)** (eu-frankfurt-1) to leverage the full Marketplace ecosystem.
  - **Identity:** Use distinct Identity Domains for each realm to prevent credential spillover.

9.3 Pattern C: The "Partner-Fronted" (Alloy)

- **Target:** SMEs or Municipalities needing managed services.
- **Architecture:**
  - Consume OCI services through a **German Service Provider** running **Oracle Alloy**.
  - The contract is with the German provider; Oracle acts merely as the technology licensor.
  - This shifts the "sovereignty" burden to the local partner's trusted infrastructure.[13]

10. Cross-Provider Comparison & Strategic Verdict

10.1 Summary Table

Sovereignty Dimension	Oracle OCI Verdict	Rationale & Source
Data Residency	**Very Strong**	"Realm" architecture (OC19) physically enforces residency better than policy overlays used by competitors.[5]
Data Localization	**Strong**	Specific EU legal entities ownership and EU-only operations teams provide robust localization.[3]
Operational Sov.	**Strong**	Guarantees EU-resident support staff for OC19 regions as a standard feature, not a premium add-on.[5]
Control Sov.	**Strong**	Robust EKMS (HYOK), OpCtl ("Glass Break" controls), and Confidential Computing availability in Frankfurt.[16]
Isolation Model	**Very Strong**	Range is unmatched: from Sovereign Public Regions to fully air-gapped Dedicated Regions on-premise.[9]
Ecosystem	**Moderate**	"Alloy" program is innovative, but the 3rd-party ISV ecosystem in OC19 is smaller than global commercial marketplaces.[13]
Legal Posture	**Strong**	Dual-region redundancy within EU (DE/ES) and specific EU corporate structure supports strong legal defensibility.[6]
EU/DE Availability	**Strong**	Dedicated Sovereign Region in Frankfurt (eu-frankfurt-2) separate from Commercial Frankfurt (eu-frankfurt-1).[7]

10.2 Strategic Analysis

Where Oracle is Strongest:
Oracle’s "Realm" architecture is the most technically honest approach to sovereignty among the US hyperscalers. Rather than trying to "filter" a global cloud to make it sovereign, Oracle built a separate cloud. The Operator Access Control (OpCtl) feature is a standout capability that directly addresses the "trust" deficit, giving customers a verified audit trail and veto power over provider access—a feature often missing or less granular in competitor offerings. Additionally, the ability to deploy a Dedicated Region with full feature parity (including GenAI) behind a customer's own firewall offers an "escape hatch" for workloads that simply cannot go to the public cloud, providing a level of isolation that "Outpost" style solutions from competitors often struggle to match in terms of service breadth.
Trade-offs for EU/Germany Customers:
The cost of this isolation is ecosystem friction. German customers must accept that OC19 is a smaller universe than OC1. They may find that a specific DevOps tool or security appliance they use in the commercial cloud is not yet published in the sovereign realm. Furthermore, the operational bifurcation—managing distinct identities and networks for sovereign vs. commercial workloads—adds a layer of complexity to IT governance. Customers must weigh the absolute assurance of the Sovereign Cloud against the seamless convenience of the global commercial cloud.

11. My Sovereignty Analysis Framework

This eight-level framework is an analytical model synthesized from the core principles and definitions used by European regulatory bodies, industry analysts, and the cloud providers themselves. It is designed to create a consistent and measurable "scorecard" to compare different sovereignty strategies.

Layer A [1,2]: Foundational Layers (Where is the data?)

This layer addresses the most fundamental questions of sovereignty: the physical and legal location of data.

[1] Data Residency

Data residency refers to the physical, geographic location where an organization's data is stored at rest. This is the most basic level of sovereignty control. An organization achieves data residency by choosing to deploy its applications and store its data in cloud data centers located within a specific country or region, such as Germany or the EU. This decision is often driven by the need to reduce latency for local users, but it is also the first step toward meeting regulatory requirements. All major cloud providers allow customers to select a specific region (e.g., Frankfurt, Paris, Dublin) for their primary data storage.

[2] Data Localization

Data localization is a stricter, legally mandated version of data residency. It refers to laws that require data generated within a country's borders to be initially collected, processed, and stored within that same country. While data residency is often a choice, data localization is a legal obligation. This concept is critical because it often extends beyond just customer content to include metadata (such as system logs, user permissions, and resource tags), which can be challenging for globally architected cloud platforms to keep entirely within one country's borders.

Layer B [3,4,5]: Control Layers (Who can access and manage the data and systems?)

This layer moves beyond the physical location of data to address the human and technical controls governing access to that data and the systems that run it.

[3] Data Access Sovereignty

This level involves the technical and organizational controls that limit access to data from outside a specified jurisdiction, particularly by the cloud provider's own personnel. The goal is to ensure that no one, including a cloud administrator, can access customer data without explicit, auditable authorization from the customer. This is often achieved through technical

means, such as Google's Key Access Justifications (KAJ), which requires a valid reason for every access request, or the hardware-level isolation of the AWS Nitro System, which is designed to prevent any operator access to data while it's being processed.

[4] Operational Sovereignty

Operational sovereignty focuses on who manages and operates the cloud infrastructure. It requires that all personnel involved—including technical support, system administrators, and on-call engineers—are located within a specific jurisdiction and are subject to its laws. This control is designed to mitigate the risk of foreign legal compulsion or unauthorized access through global "follow-the-sun" support models, where staff in different countries might have privileged access to systems. Examples include Google's "EU Data Boundary and Support" package, which guarantees support from EU-based personnel, and the announced AWS European Sovereign Cloud, which promises that all operations and support will be handled exclusively by EU residents.

[5] Control Sovereignty

This is the highest level of technical control, where the customer uses cryptographic technologies to gain ultimate authority over their data, making it verifiably inaccessible to the cloud provider. This is achieved through two primary mechanisms:

- **Customer-Controlled Keys:** Using services like an External Key Manager (EKM or XKS), customers can store and manage their encryption keys in a system completely outside of the cloud provider's infrastructure. The cloud provider never has access to the key material itself, only a reference to it, giving the customer a "kill switch" to revoke access at any time.
- **Confidential Computing:** This technology protects data *while it is in use* (i.e., being processed in memory). It uses a hardware-based Trusted Execution Environment (TEE), or "enclave," to create an isolated, encrypted space where code and data are protected from being viewed or modified by anyone, including the cloud provider's hypervisor or operators.

Layer C [6,7,8]: Assurance Layers (What are the surrounding guarantees?)

This final layer assesses the broader architectural, legal, and compliance frameworks that support a provider's sovereignty claims.

[6] Legal/Contractual Posture

This refers to the specific legal agreements, data processing addenda, and public commitments a provider offers. It is the legal foundation of their sovereignty promise. This includes contractual terms that define data boundaries, commitments to challenge government data requests, and addenda that help customers comply with regulations like GDPR and address the requirements of legal rulings such as Schrems II. Examples include

Microsoft's broad EU Data Boundary commitment and the specific service terms for Google's Assured Workloads.

[7] Isolation Model

This describes the fundamental architectural approach a provider takes to deliver sovereignty. There are two main models:

- **Configured Sovereignty on a Shared Cloud:** This model uses the provider's standard global infrastructure but applies software-defined controls, policies, and specific operational boundaries to create a sovereign environment. This is the approach taken by Google's Assured Workloads and Microsoft's EU Data Boundary. It offers broad service availability but relies on logical separation.
- **Dedicated/Isolated Sovereign Cloud:** This model involves building a physically and operationally separate, independent cloud for a specific jurisdiction. This is the approach of the announced AWS European Sovereign Cloud. It promises the highest level of isolation but may initially launch with a more limited set of services.

[8] Ecosystem/Compliance

This level evaluates a provider's alignment with recognized European and national compliance standards, as well as the strength of its partner ecosystem. Third-party certifications, such as Germany's BSI C5 (Cloud Computing Compliance Criteria Catalogue), provide independent validation of a provider's security claims. Furthermore, a mature ecosystem of local partners, like T-Systems in Germany for Google Cloud, is often essential for implementing and managing high-assurance sovereign solutions.12 This also includes a provider's engagement with pan-European initiatives like GAIA-X.

Works cited

1. Public Cloud Regions and Data Centers | Oracle, accessed on January 16, 2026, https://www.oracle.com/cloud/public-cloud-regions/
2. Sovereign Cloud - Oracle, accessed on January 16, 2026, https://www.oracle.com/cloud/sovereign-cloud/
3. EU Sovereign Cloud FAQ | Oracle, accessed on January 16, 2026, https://www.oracle.com/cloud/eu-sovereign-cloud/faq/
4. Oracle EU Sovereign Cloud is now available, accessed on January 16, 2026, https://docs.oracle.com/iaas/releasenotes/changes/f5a57de0-498c-40b0-8f80-b0e3b5d06863/index.htm
5. Learn About the Oracle European Union Sovereign Cloud, accessed on January 16, 2026, https://docs.oracle.com/en/solutions/learn-about-eusc/index.html
6. EU Sovereign Cloud | Oracle, accessed on January 16, 2026, https://www.oracle.com/cloud/eu-sovereign-cloud/
7. Oracle EU Sovereign Cloud, accessed on January 16, 2026, https://docs.oracle.com/en-us/iaas/Content/sovereign-cloud/eu-sovereign-cloud.htm
8. Offering a sovereign cloud designed for the European Union - Oracle Blogs, accessed on January 16, 2026, https://blogs.oracle.com/cloud-infrastructure/offering-a-sovereign-cloud-designed-for-the-european-union
9. Dedicated Cloud Region Overview - Oracle, accessed on January 16, 2026, https://www.oracle.com/cloud/cloud-at-customer/dedicated-region/
10. OCI Dedicated Region FAQ - Oracle, accessed on January 16, 2026, https://www.oracle.com/cloud/cloud-at-customer/dedicated-region/faq/
11. Oracle Cloud Infrastructure Enables More Customers to Rapidly Deploy AI and Cloud Services, accessed on January 16, 2026, https://www.oracle.com/de/news/announcement/ai-world-oracle-cloud-infrastructure-enables-more-customers-to-rapidly-deploy-ai-and-cloud-services-2025-10-14/
12. Oracle Cloud Infrastructure Enables More Customers to Rapidly Deploy AI and Cloud Services, accessed on January 16, 2026, https://www.oracle.com/news/announcement/ai-world-oracle-cloud-infrastructure-enables-more-customers-to-rapidly-deploy-ai-and-cloud-services-2025-10-14/
13. Oracle Alloy, accessed on January 16, 2026, https://www.oracle.com/cloud/alloy/
14. Oracle Alloy Enables du to Offer Sovereign Cloud Capabilities at Scale, accessed on January 16, 2026, https://www.oracle.com/europe/news/announcement/blog/oracle-alloy-enables-offer-sovereign-cloud-capabilities-2025-07-02/
15. Enhancing Cloud Security and Sovereignty with Thales & Oracle Alloy – Post-Webinar Recap, accessed on January 16, 2026, https://blogs.oracle.com/cloud-infrastructure/oracle-alloy-thales-cloud-security-

sovereignty-webinar-recap
16. External Key Management Service - Oracle Help Center, accessed on January 16, 2026, https://docs.oracle.com/en-us/iaas/Content/KeyManagement/Tasks/external_key_management.htm
17. Oracle Cloud Infrastructure Sovereign Cloud Principles, accessed on January 16, 2026, https://docs.oracle.com/iaas/Content/Resources/Assets/whitepapers/oracle-sovereign-cloud-principles.pdf
18. Oracle Operator Access Control, accessed on January 16, 2026, https://docs.oracle.com/en-us/iaas/operator-access-control/index.html
19. oci-soc-3-report.pdf - Oracle, accessed on January 16, 2026, https://www.oracle.com/a/ocom/docs/oci-soc-3-report.pdf
20. Confidential Computing - Oracle Help Center, accessed on January 16, 2026, https://docs.oracle.com/en-us/iaas/Content/Compute/References/confidential_compute.htm
21. Meta Llama 3.3 (70B) - Oracle Help Center, accessed on January 16, 2026, https://docs.oracle.com/en-us/iaas/Content/generative-ai/meta-llama-3-3-70b.htm
22. Oracle Cloud Infrastructure Earns Top Commercial Accreditation in Czech National Cloud Catalog, accessed on January 16, 2026, https://blogs.oracle.com/cloud-infrastructure/oci-earns-top-accreditation-in-czech-national-catalog-3
23. Overview of Vaults, Key Management, and Secret Management - Oracle Help Center, accessed on January 16, 2026, https://docs.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htm
24. Managing Infrastructure Access with Operator Access Control - Oracle Help Center, accessed on January 16, 2026, https://docs.oracle.com/en-us/iaas/operator-access-control/doc/managing-infrastructure-access.html
25. Creating an Instance - Oracle Help Center, accessed on January 16, 2026, https://docs.oracle.com/iaas/Content/Compute/Tasks/launchinginstance.htm
26. Required IAM Policy To View Listings - Oracle Help Center, accessed on January 16, 2026, https://docs.oracle.com/en-us/iaas/Content/Marketplace/iam-policy.htm
27. OCI Generative AI is available in the EU Sovereign Central (Frankfurt) region, accessed on January 16, 2026, https://docs.oracle.com/iaas/releasenotes/generative-ai/new-region-frankfurt-2.htm
28. Migration of EURA Environments to EU Sovereign Cloud (OC19) - Oracle Help Center, accessed on January 16, 2026, https://docs.oracle.com/en/cloud/saas/readiness/epm/2025/epm-jul25/25jul-epm-wn-f39551.htm
29. Health Monitor - Oracle Help Center, accessed on January 16, 2026, https://docs.oracle.com/en-us/iaas/mysql-database/doc/health-monitor.html