My Deep Research Analysis of Digital Sovereignty on GCP, Azure, and AWS for EU/German regulated Workloads

Executive Summary

This report provides a precise, source-verified analysis of the digital sovereignty solutions offered by Google Cloud Platform (GCP), Microsoft Azure, and Amazon Web Services (AWS) for organizations operating within the European Union (EU), with a specific focus on Germany. The assessment is based exclusively on official provider documentation and evaluates offerings against a standardized eight-level sovereignty framework.

- **Google Cloud Platform (GCP)** employs a multi-tiered, software-defined strategy that allows customers to layer sovereignty controls onto its standard global cloud infrastructure. Its foundational offering, **Assured Workloads**, provides configurable data residency and EU-only support personnel. For the highest levels of control, GCP combines technical features like **Confidential Computing** and **Cloud External Key Manager (EKM) with Key Access Justifications (KAJ)**. For maximum assurance in Germany, it offers **Sovereign Controls by T-Systems**, a partner-operated model that guarantees data storage in Germany and adds local operational oversight. This approach offers the most flexible and granular set of sovereignty controls available today.

- **Microsoft Azure** centers its strategy on the **EU Data Boundary**, a broad contractual and operational commitment to store and process customer data for most of its core services within the EU. This "sovereignty by default" posture is designed for ease of adoption across its extensive service portfolio. This commitment is reinforced by a strong portfolio of technical controls, particularly **Azure Confidential Computing**, which protects data while in use. However, the boundary has documented exceptions for certain global services and allows for remote operational access from outside the EU, creating specific areas for due diligence.
- **Amazon Web Services (AWS)** is pursuing a long-term strategy of "sovereignty through isolation," culminating in the announced **AWS European Sovereign Cloud**. This future offering, set to launch its first region in Germany by the end of 2025, will be a physically and operationally separate cloud, managed exclusively by EU-resident personnel. In the interim, AWS relies on strong, currently available technical controls within its standard EU regions, such as the hardware-level isolation of the **AWS Nitro System** and **AWS KMS with External Key Store (XKS)**. This strategy presents the strongest future promise of isolation but requires customers to navigate the current gaps and plan for a future migration.
- **Comparative Verdict:** GCP currently offers the most flexible, tiered approach, allowing customers to tailor controls to specific workload requirements. Azure provides the broadest and simplest contractual data residency boundary, though it is not absolute. AWS offers powerful foundational security today with the promise of the most stringent isolation model in the future, contingent on its roadmap.
- **Primary Trade-Offs:** The central decision for EU/German customers revolves around adopting mature, feature-rich, but integrated sovereign solutions available now (GCP, Azure) versus committing to a future, highly isolated, but initially more limited sovereign cloud (AWS). This choice involves weighing the benefits of granular software-defined controls against the assurance of physical and operational separation, and balancing immediate compliance needs against long-term strategic roadmaps.

Section 1: Google Cloud Platform (GCP) Digital Sovereignty Posture

Google Cloud's approach to digital sovereignty is characterized by a flexible, multi-layered framework rather than a single, monolithic "sovereign cloud." It leverages its standard global infrastructure and applies progressively stronger sets of software-defined controls and partner-led operational models to meet a spectrum of regulatory requirements. This strategy of "sovereignty through configuration" allows customers to select the precise level of assurance needed for a given workload, from basic data residency to cryptographically enforced data access control and partner-operated environments.
The core of this strategy is **Assured Workloads**, a service that applies pre-defined compliance packages to specific folders within a customer's GCP organization.[1] These

packages enforce guardrails using organization policies. For the highest level of assurance, particularly in Germany, GCP collaborates with local partners like T-Systems to deliver a **Sovereign Controls by Partners** offering, which adds external operational oversight and stricter data residency guarantees.[3] These foundational offerings are complemented by a robust portfolio of technical controls, including the **Confidential Computing** suite for protecting data-in-use and advanced key management services like **Cloud External Key Manager (EKM)** with **Key Access Justifications (KAJ)**, which provide customers with ultimate control over their encryption keys and data access.[4]

1.1 Offerings Overview

GCP's sovereignty offerings are structured in tiers of increasing control and assurance, all of which are generally available (GA).

- **Assured Workloads:** This service acts as the primary mechanism for configuring sovereign environments. It is not a separate cloud but a governance layer that enforces controls on resources created within a designated folder.[2] Key control packages for the EU include:
  - **EU Data Boundary:** This package enforces data residency by restricting the creation of new resources to a specified list of EU regions using the gcp.resourceLocations organization policy.[6] A critical limitation of this baseline package is that technical support is handled by Google's global support personnel.[6]
  - **EU Data Boundary and Support:** This package builds upon the data residency controls by adding an operational sovereignty guarantee: technical support cases for workloads in this environment are handled exclusively by EU personnel who are physically located within the EU.[1] This offering requires an active Enhanced or Premium Support subscription.[8]
  - **EU Data Boundary with Access Justifications:** Formerly known as "Sovereign Controls for EU," this is the highest tier of Google-managed controls.[2] It combines the EU data and support boundaries with powerful cryptographic control over data access. This is achieved by mandating the use of Cloud External Key Manager (EKM) and Key Access Justifications (KAJ), which allows a customer to programmatically approve or deny every access request to their externally held encryption keys based on a justification provided by Google.[1]
- **Sovereign Controls by Partners (T-Systems Sovereign Cloud):** For customers in Germany with the most stringent requirements, GCP offers a partner-operated model.[2] The **T-Systems Sovereign Cloud** guarantees that customer data is stored exclusively in Germany (specifically, the europe-west3 region in Frankfurt).[3] T-Systems manages the external encryption keys, provides EU-based technical support, and adds a layer of local supervision, including a security operations center and physical security monitoring of the data centers.[3] This model represents a shared responsibility

framework where a trusted local partner provides an additional layer of oversight and control.

- **Confidential Computing Portfolio:** This suite of GA products provides technical protection for data-in-use by encrypting it in memory, rendering it inaccessible to the cloud provider or any other tenant on the host machine.[4] The portfolio includes **Confidential VMs** (leveraging AMD SEV/SEV-SNP and Intel TDX technologies), **Confidential GKE Nodes** for containerized workloads, and confidential options for data processing services like **Dataflow** and **Dataproc**.[4]
- **Key Management Services:** GCP offers a tiered approach to key management, a critical component of control sovereignty.
    - **Cloud KMS and Cloud HSM:** These services provide customer-managed software keys and FIPS 140-2 Level 3 validated hardware security module (HSM) keys, respectively, managed within the GCP environment.[5]
    - **Cloud External Key Manager (Cloud EKM):** This GA service allows customers to protect their data in GCP using encryption keys that are stored and managed in a third-party key management system outside of Google's infrastructure.[5] Google only receives a key reference and never has access to the key material itself, providing a strong guarantee of key provenance and control.[14]

1.2 EU/Germany Availability

GCP has a significant infrastructure footprint in the EU, providing multiple options for data residency and low-latency performance.

- **EU Regions:** GCP operates numerous regions across the EU, including locations in Belgium (europe-west1), Frankfurt (europe-west3), Netherlands (europe-west4), Zurich (europe-west6), Milan (europe-west8), Paris (europe-west9), Berlin (europe-west10), Madrid (europe-southwest1), and Warsaw (europe-central2).[15]
- **Germany-Specific Regions:** GCP has two distinct regions in Germany: Frankfurt (europe-west3) and Berlin (europe-west10), offering in-country redundancy and choice for German customers.[15]
- **Assured Workloads Availability:** The EU Data Boundary control packages are available across a curated list of EU regions, which customers select during folder setup.[6] This list includes both German regions.
- **Sovereign Controls by T-Systems Availability:** This premier offering for Germany is specifically anchored to the Frankfurt (europe-west3) region, providing a contractual guarantee of data storage within German borders.[3]
- **Service Availability:** The availability of specific GCP services can vary by region. Furthermore, not all GCP services are supported within Assured Workloads environments. The official documentation provides a comprehensive list of in-scope products for each control package, which must be consulted during architectural planning to avoid deploying unsupported services.[7]

1.3 GCP Controls Matrix

The following table maps Google Cloud's sovereignty offerings to the defined sovereignty levels, providing a detailed breakdown of their capabilities and dependencies.

Offering/Feature	Level(s) Covered	EU/DE Availability	Dependencies	Operational/Support Bounds	Legal/Contractual Notes	Status	Source
Assured Workloads: EU Data Boundary	1. Data Residency 2. Data Localization	All specified EU regions, including DE.	None. This is the baseline package.	Support provided by global personnel. No restrictions on support staff location.	Part of Assured Workloads Free tier. Governed by Google Cloud Data Location Service Specific Terms.	GA	[6]
Assured Workloads: EU Data Boundary and Support	1. Data Residency 2. Data Localization 4. Operational Sovereignty	All specified EU regions, including DE.	Enhanced or Premium Support subscription is required.	Technical support provided exclusively by EU personnel located within the EU.	Paid add-on to standard support plans.	GA	[1]
Assured Workloads: EU Data Boundary with Access Justifications	1. Data Residency 2. Data Localization 3. Data Access Sovereignty 4. Operational Sovereignty 5. Control Sovereignty	All specified EU regions, including DE.	Requires Cloud EKM, Key Access Justifications, and Enhanced/Premium Support.	EU-only support personnel. Customer must approve/deny key access requests from Google.	Combines data boundary terms with cryptographic access control commitments.	GA	[1]
Sovereign Controls by T-Systems	1. Data Residency 2. Data Localization 3. Data Access Sovereignty 4. Operational Sovereignty 5. Control Sovereignty 6.Legal/Contractual Posture 7. Isolation Model	Germany (Frankfurt, europe-west3) only.	Contract with T-Systems. Uses Cloud EKM managed by T-Systems.	Support from EU-based T-Systems staff. T-Systems provides SOC and physical security oversight.	Separate contractual agreement with T-Systems, in addition to GCP terms. Guarantees data storage in Germany.	GA	[3]

	(Partner-operated)						
Confidential Computing (VMs, GKE Nodes, etc.)	5. Control Sovereignty (Data-in-use protection)	Available in most EU/DE regions, but specific machine types may have limited availability.	Requires selecting specific Confidential VM machine series (e.g., N2D, C3).	Protects data in memory from access by Google operators or the hypervisor.	Standard service terms apply.	GA	[4]
Cloud External Key Manager (Cloud EKM)	5. Control Sovereignty (Key custody)	Available as a multi-regional (eu) or regional service in EU/DE.	Requires a compatible external key manager (on-premises or partner-hosted).	Customer retains full control and custody of keys. Google never possesses the key material.	Customer is responsible for the availability and durability of the external key manager.	GA	[5]
Key Access Justifications (KAJ)	3. Data Access Sovereignty 5. Control Sovereignty	Available as a multi-regional (eu) service.	Must be used with Cloud EKM.	Provides a mechanism for the customer to approve or deny every Google request for an external key.	Covered by Google's integrity commitments.	GA	[1]

1.4 Limitations and Gaps

Despite its comprehensive and flexible offerings, GCP's approach has several limitations and constraints that require careful consideration.

- **Dependency on Global Internal Services:** GCP's architecture is built upon a set of globally distributed internal services (such as Spanner for databases, Colossus for storage, and Borg for orchestration).[17] While customer data residency is enforced by Assured Workloads, metadata, operational data, and internal service-to-service communications required to run the platform may cross regional boundaries. The platform is not architected to be fully isolated within a single region.
- **Reduced Functionality in Sovereign Environments:** To maintain a strict data boundary, Assured Workloads disables or limits certain features within supported services. For example, within an EU Data Boundary folder, BigQuery does not support interaction with remote data sources, GDrive export, or the use of Gemini in BigQuery.[6] Similarly, Cloud Run loses its integration with Cloud Trace.[18] Customers must perform a thorough feature-level analysis to ensure their applications do not depend on these restricted capabilities.
- **Conditional Operational Sovereignty:** Achieving operational sovereignty is not a default feature; it is an explicit, paid add-on. The baseline EU Data Boundary package still routes support cases to global personnel.[6] Only by purchasing an Enhanced or Premium Support plan and enabling the specific EU Data Boundary and Support package can a customer ensure their support interactions are handled by EU-based

staff.[8] This significantly impacts the total cost of ownership (TCO) for achieving this level of sovereignty.

- **Complexity and Shared Responsibility:** The layered approach, while flexible, introduces complexity. A high-assurance deployment requires correctly configuring multiple distinct services: Assured Workloads, Cloud EKM, KAJ, and Confidential Computing. Misconfiguration can undermine the intended sovereignty posture. The T-Systems partner model, while providing the highest level of assurance, introduces a third-party dependency, additional contractual overhead, and a shared responsibility model for operations and availability that differs from the standard cloud paradigm.[3]
- **Data Residency is Not Absolute for All Data Types:** The data residency guarantees provided by Assured Workloads apply to "Customer Data" at rest.[19] This definition explicitly excludes resource identifiers, attributes, and other data labels (metadata).[19] Furthermore, certain services, like Gemini Enterprise when connected to Google Drive, only guarantee data residency for the data within Google Cloud, not for the data sourced from Drive itself.[20]

1.5 Implementation Patterns

Based on GCP's offerings, organizations can adopt several patterns to meet varying levels of sovereignty requirements.

- **Baseline EU Data Residency and Operations:** The most common pattern involves creating an **Assured Workloads folder** with the **EU Data Boundary and Support** control package. All project resources are deployed into one or more specified EU regions (e.g., europe-west3 in Frankfurt). Encryption keys are managed using the standard **Cloud KMS**. This architecture provides strong, auditable guarantees for data residency at rest and ensures that all technical support is handled by EU personnel, satisfying key requirements of regulations like GDPR and NIS2.[1]
- **High-Assurance with Cryptographic Control:** For workloads handling highly sensitive data, organizations can build upon the baseline pattern by implementing a zero-trust approach to data access. This involves replacing Cloud KMS with **Cloud External Key Manager (EKM)**, connecting to an on-premises or partner-managed HSM.[14] By enabling **Key Access Justifications (KAJ)**, the customer gains the ability to cryptographically approve or deny every attempt by Google to access the data.[5] To protect data-in-use, all compute workloads are deployed on **Confidential VMs** or **Confidential GKE Nodes**.[4] This pattern establishes sovereignty across the data lifecycle: at rest, in transit, and in use.
- **Maximum German Sovereignty via Partnership:** For public sector entities or industries in Germany with the strictest data localization and operational control mandates, the recommended pattern is to engage with T-Systems and deploy into the **T-Systems Sovereign Cloud** offering.[3] This pattern leverages the europe-west3 (Frankfurt) region and outsources external key management and Level 1/2 support directly to T-Systems. This provides the strongest possible guarantee of in-country data

storage and local operational oversight but requires managing a direct relationship with the partner in addition to Google.[3]

Section 2: Microsoft Azure Digital Sovereignty Posture

Microsoft Azure's strategy for digital sovereignty in the EU is anchored by the **EU Data Boundary**, a broad, cross-service commitment to store and process customer data within the European Union. This approach aims to make sovereignty a default characteristic of using Azure in the EU, rather than a configurable add-on, thereby simplifying compliance for a wide range of customers. This contractual and operational promise is the cornerstone of its value proposition, covering not only Azure but also Microsoft 365, Power Platform, and Dynamics 365 services.

This "sovereignty by default" posture is supported by a deep portfolio of technical controls designed to give customers granular control over their data. The **Azure Confidential Computing** portfolio is a key pillar, providing hardware-based protection for data while it is being processed, which serves as a powerful mitigation against unauthorized provider access.[22] This is complemented by a range of key management solutions, from the multi-tenant **Azure Key Vault** to the single-tenant **Azure Managed HSM** and **Dedicated HSM** offerings, allowing customers to choose the appropriate level of key isolation and control.[24] While the EU Data Boundary is comprehensive, it is not absolute; Microsoft transparently documents exceptions for certain globally architected services and specific data flows, which requires careful customer due diligence.

2.1 Offerings Overview

Azure's sovereignty offerings are a combination of a foundational commitment, a portfolio of technical security features, and specific partner-led initiatives.

- **Microsoft EU Data Boundary:** This is the central pillar of Azure's EU sovereignty strategy. It is a GA commitment to store and process customer data exclusively within the EU for all in-scope Azure, Microsoft 365, Dynamics 365, and Power Platform services.[26] It is not a separate product or SKU but the default operational mode for customers in the EU. The boundary applies to customer data at rest, including all content, and processing activities are also kept within the EU.[26]
- **Microsoft Cloud for Sovereignty:** This is a conceptual framework and set of capabilities, not a distinct product. It is designed to help public sector customers implement sovereign environments on Azure.[26] It combines features like data residency, confidential computing, customer-managed keys, and governance tools like Azure Policy to create "sovereign landing zones." It emphasizes using standard Azure services with stricter, policy-driven guardrails to meet specific compliance and sovereignty

requirements.[28]

- **Azure Confidential Computing:** Azure offers a comprehensive, GA portfolio of services that protect data-in-use by processing it within a hardware-based Trusted Execution Environment (TEE). This prevents access by the host OS, hypervisor, and cloud administrators.[22] Key offerings include:
  - **Confidential VMs:** Based on AMD SEV-SNP and Intel TDX technologies, these VMs provide infrastructure-level memory encryption for lift-and-shift workloads without code changes.[23] GPU-enabled confidential VMs are also available for secure AI/ML workloads.[31]
  - **Confidential Containers on AKS:** Allows containerized applications to run within secure enclaves on Azure Kubernetes Service.[23]
  - **Azure SQL Always Encrypted with secure enclaves:** Protects sensitive data in SQL databases, allowing for rich computations on encrypted data within a server-side TEE.[30]
  - **Azure Confidential Ledger:** A tamper-proof, blockchain-based ledger service that runs entirely within TEEs to guarantee data integrity.[32]
- **Key Management Services:** Azure provides a tiered set of GA key management solutions to meet different control and compliance needs.
  - **Azure Key Vault:** A service for managing cryptographic keys, secrets, and certificates. It offers two tiers: Standard (software-protected keys) and Premium, which stores keys in FIPS 140-2 Level 3 validated, multi-tenant HSMs.[24]
  - **Azure Managed HSM:** A fully managed, single-tenant, FIPS 140-2 Level 3 validated HSM service. It provides customers with greater control and isolation for their keys compared to the shared Premium tier of Key Vault, making it suitable for highly regulated workloads.[33]
  - **Azure Dedicated HSM:** A bare-metal HSM service providing a dedicated physical device (Gemalto SafeNet Network HSM 7) in the Azure cloud.[25] The customer has complete administrative and cryptographic control. However, a key limitation is that it does not integrate with other Azure services that support customer-managed keys (CMK), limiting its use cases primarily to custom applications.[25]

2.2 EU/Germany Availability

Microsoft maintains a robust and expanding infrastructure footprint across Europe, with specific sovereign initiatives and long-standing investments in Germany.

- **EU Regions:** Azure operates numerous regions within the EU Data Boundary, including Germany West Central (Frankfurt), Germany North (Berlin), France Central (Paris), North Europe (Ireland), West Europe (Netherlands), Sweden Central, and others.[35] Microsoft has also announced plans for new regions in Austria, Spain, Italy, and Poland.[35]
- **Germany-Specific Regions:** Azure has two primary regions in Germany: Germany

West Central (Frankfurt) and Germany North (Berlin). Historically, Microsoft also operated a separate "Azure Germany" cloud under a data trustee model to meet strict sovereignty requirements. While this model is being superseded by the standard regions now governed by the EU Data Boundary, it demonstrates a long-term commitment to the German market.[38]

- **EU Data Boundary Scope:** The boundary commitment applies to customer workloads deployed in any of the Azure regions located within the EU geography.[27]
- **Sovereign Partnerships:** Microsoft has announced a sovereign cloud initiative in France through a joint venture named "Bleu" with Capgemini and Orange.[40] It has also noted a partnership in Germany, though the specific operational details are less publicly defined than the French model or the previous German data trustee model.[40]

2.3 Azure Controls Matrix

This table maps Microsoft Azure's sovereignty offerings to the defined levels, clarifying the scope of its commitments and the role of its technical controls.

Offering/Feature	Level(s) Covered	EU/DE Availability	Dependencies	Operational/Support Bounds	Legal/Contractual Notes	Status	Source
Microsoft EU Data Boundary	1. Data Residency 2. Data Localization (for in-scope services) 6. Legal/ Contractual Posture	All Azure regions in the EU, including DE.	None. This is the default posture for EU customers.	Remote operations by non-EU personnel are permitted, but access to customer data requires authorization.	A contractual commitment to store and process customer data within the EU. Known exceptions for non-regional services.	GA	[26]
Microsoft Cloud for Sovereignty	1, 2, 5, 8 (as a framework)	All EU/DE regions.	Azure Policy, Azure Blueprints, and other standard Azure services.	Defined by customer configuration (e.g., support plans, access controls).	Not a separate product; it's a set of best practices and reference architectures.	GA	[26]
Azure Confidential Computing (VMs, Containers, etc.)	5. Control Sovereignty (Data-in-use protection)	Available in most EU/DE regions; specific VM SKUs may vary.	Requires selection of confidential computing VM series (DCasv5/ECasv5 for AMD, DCsv3/CC for Intel).	Protects data in memory from access by Microsoft operators, hypervisor, and host OS.	Standard service terms apply.	GA	[22]
Azure Key Vault (Premium Tier)	5. Control Sovereignty (Key custody)	All EU/DE regions.	Requires selection of the Premium pricing tier.	Keys are stored and processed in FIPS 140-2 Level 3 validated,	Standard Key Vault SLA applies.	GA	[24]

				multi-tenant HSMs.			
Azure Managed HSM	5. Control Sovereignty (Key custody)	Available in select EU/DE regions (e.g., North Europe, West Europe, Germany West Central).	None. It is a standalone service.	Provides a single-tenant, FIPS 140-2 Level 3 validated HSM pool under customer control.	Higher SLA and cost than Key Vault Premium.	GA	[24]
Azure Dedicated HSM	5. Control Sovereignty (Key custody)	Limited availability in EU regions.	Requires specific onboarding and configuration.	Customer has full administrative and cryptographic control of a dedicated physical HSM.	No integration with most Azure PaaS services (e.g., CMK). No SLA provided by Microsoft.	GA	[25]

2.4 Limitations and Gaps

While the EU Data Boundary is a strong commitment, it is crucial to understand its documented limitations and the areas where sovereignty is not absolute.

- **Exclusions for Non-Regional Services:** The EU Data Boundary guarantee does not apply to certain services that are architected globally. **Microsoft Entra ID** may store directory data globally to ensure scalability and availability.[26] **Azure Content Delivery Network (CDN)**, by its nature, caches data at edge locations around the world.[26] These services are foundational to many applications, representing a known and accepted data outflow from the EU.
- **Cross-Geo Network Traffic and Telemetry:** Microsoft's data residency documentation states that to maintain resiliency, network paths for service traffic may sometimes cross geographic boundaries, although customer data replication for disaster recovery remains within the designated geo.[26] Additionally, pseudonymous identifiers and service traces may be processed globally to operate and improve the services, for billing, and for fraud protection.[26]
- **Remote Operations and Support:** The EU Data Boundary allows for remote operation of data processing systems within the EU by Microsoft personnel (including subprocessors) located outside the EU.[26] Access to customer data by these personnel is not permitted without customer authorization, but the operational access itself is not restricted to EU persons. This is a significant distinction from offerings that guarantee all operational and support functions are performed by staff located within the EU.
- **Risks with Preview Services:** Any service in a preview, beta, or other pre-release state is explicitly excluded from data residency guarantees. These services typically store customer data in the United States but may store it globally, regardless of the region in which they are deployed.[41] Organizations using preview features for innovation must accept this compliance risk.
- **Limited Scope of Dedicated HSM:** The Azure Dedicated HSM offering provides the highest level of cryptographic control, giving the customer exclusive access to a

physical HSM. However, its utility is severely limited by its lack of integration with the majority of Azure services that support Customer-Managed Keys (CMK). This restricts its use to custom applications that can integrate directly with the HSM, making it unsuitable for protecting data at rest in most Azure PaaS and SaaS offerings.[25]

2.5 Implementation Patterns

Organizations can leverage Azure's capabilities through several architectural patterns to address their sovereignty needs.

- **Standard EU Data Boundary Compliance:** The most straightforward pattern is to deploy all application resources into Azure regions within the EU (e.g., Germany West Central, West Europe). Use **Azure Policy** to enforce the "Allowed locations" policy, preventing accidental deployment of resources outside the EU. This pattern relies on the broad contractual guarantees of the **EU Data Boundary** for all in-scope services and is suitable for workloads with standard data residency requirements.[26]
- **Enhanced Control with Managed HSM:** For workloads requiring stronger cryptographic assurances, this pattern builds on the first by centralizing all critical encryption keys in **Azure Managed HSM**.[33] This provides a single-tenant, FIPS 140-2 Level 3 environment that is fully controlled by the customer. All supported Azure services (such as Azure Storage, Azure SQL Database, and Azure Cosmos DB) should be configured to use Customer-Managed Keys (CMK) pointing to the Managed HSM instance. This ensures that while Microsoft manages the HSM infrastructure, the customer retains sole control over the key lifecycle.
- **Zero-Trust Data Processing:** To achieve the highest level of technical assurance and mitigate risks associated with provider access, this pattern focuses on protecting data-in-use. All sensitive compute workloads are deployed on **Azure Confidential VMs** or as **Confidential Containers on AKS**.[23] For database operations, **Azure SQL Always Encrypted with secure enclaves** is used to process queries on encrypted data without exposing plaintext data to the database administrator or cloud operator.[30] This architecture minimizes the trust placed in the cloud provider's operational environment, as sensitive data remains encrypted even while being processed in memory.

Section 3: Amazon Web Services (AWS) Digital Sovereignty Posture

Amazon Web Services (AWS) is pursuing a dual-pronged strategy for digital sovereignty. For the present, it emphasizes the robust, "sovereign-by-design" technical controls available in its existing global cloud infrastructure, such as its EU regions. For the future, it is making a significant strategic investment in "sovereignty through isolation" with the announced **AWS European Sovereign Cloud**. This long-term vision aims to create a new, independent cloud that is physically and operationally separate from the existing AWS global infrastructure, designed to meet the most stringent European sovereignty requirements.
Currently, customers in the EU can leverage a powerful set of GA features outlined in the **AWS Digital Sovereignty Pledge**.[44] The cornerstone of its technical assurance is the **AWS Nitro System**, a custom-designed hardware and hypervisor combination that provides a strong, verifiable security boundary to prevent operator access to data in use.[44] This is complemented by advanced cryptographic controls like **AWS Key Management Service (KMS) with External Key Store (XKS)**, which allows customers to maintain sovereign control over their encryption keys outside of AWS.[46] Governance is enforced through services like **AWS Control Tower**, which offers a specific set of controls for data residency.[47] This current approach relies heavily on technical enforcement and customer configuration, while the future European Sovereign Cloud promises to add comprehensive operational and administrative isolation.

3.1 Offerings Overview

AWS's sovereignty offerings consist of a future flagship product and a set of powerful, currently available features and commitments.

- **AWS European Sovereign Cloud (Announced):** This is AWS's strategic answer to the highest level of sovereignty requirements. It is an announced, new, independent cloud for Europe.
    - **Isolation Model:** It will be physically and logically separate from existing AWS Regions, requiring a new AWS account to use.[48]
    - **Data & Metadata Residency:** All customer data and all customer-created metadata (such as IAM roles, permissions, and resource tags) will be stored within the EU.[48] It will feature its own independent billing and metering systems.[48]
    - **Operational Sovereignty:** All operations and support will be controlled and performed exclusively by AWS employees who are EU residents and are physically located within the EU.[48]
    - **Timeline and Location:** The first region is set to launch in the State of Brandenburg, Germany, by the end of 2025.[44]

- **AWS Digital Sovereignty Pledge (Current Framework):** This GA commitment outlines

AWS's ongoing investment in sovereignty features on its existing global cloud. It is built on four pillars:

1. **Control over the location of your data:** Customers choose the AWS Region for their data.[44]
2. **Verifiable control over data access:** Centered on the AWS Nitro System.[44]
3. **The ability to encrypt everything everywhere:** Highlighting services like AWS KMS and XKS.[44]
4. **Resilience of the cloud:** Emphasizing the multi-AZ architecture of AWS Regions.[44]

- **AWS Nitro System (Current Technical Control):** This GA feature is the foundation for all modern Amazon EC2 instances. It is a combination of dedicated hardware and a lightweight hypervisor that offloads network, storage, and security functions.[55] Its security design provides a strong boundary that is engineered to prevent any system or person, including AWS employees, from accessing customer data or code while it is being processed on an EC2 instance.[44] The security claims of the Nitro System have been independently validated by a third-party security firm, NCC Group.[44]
- **AWS Nitro Enclaves (Current Technical Control):** A feature of the Nitro System, Nitro Enclaves allows customers to create isolated compute environments from within an EC2 instance.[55] These enclaves are highly restricted virtual machines with no persistent storage, no network access, and no interactive access, making them ideal for processing highly sensitive data.[55]
- **AWS Key Management Service (KMS) with External Key Store (XKS):** This GA feature enables customers to protect their data in AWS using cryptographic keys that are stored and managed in a key management system outside of AWS's control.[46] AWS KMS communicates with an external key store proxy that the customer controls, ensuring that AWS never has access to the plaintext key material. This provides the highest level of customer control over encryption keys.[46]
- **AWS Control Tower:** This GA governance service helps customers set up and manage a secure, multi-account AWS environment. It includes a specific category of over 245 preventative and detective controls for "digital sovereignty," which can be used to enforce data residency policies, restrict access to services, and ensure encryption standards are met across the organization's AWS accounts.[45]
- **AWS Dedicated Local Zones:** This is a GA infrastructure offering where AWS builds and manages a Local Zone for the exclusive use of a single customer or community in a location they specify.[44] This can be used to meet specific regulatory needs, including requirements for operating personnel to hold certain security clearances.[45]

3.2 EU/Germany Availability

AWS provides customers with multiple regional choices in Europe today, with a clear roadmap for its sovereign offering centered on Germany.

- **Current EU Regions:** AWS operates eight regions in Europe: Frankfurt (eu-central-1), Ireland (eu-west-1), London (eu-west-2), Paris (eu-west-3), Stockholm (eu-north-1), Milan (eu-south-1), Spain (eu-south-2), and Zurich (eu-central-2).[59]
- **Germany Region:** The Frankfurt region (eu-central-1) is the primary AWS location in Germany, offering a full suite of services and consisting of three Availability Zones.[59]
- **Future Sovereign Region:** The first region of the **AWS European Sovereign Cloud** will be located in the State of Brandenburg, Germany. It is announced to launch by the end of 2025 and will also consist of multiple Availability Zones.[48]

3.3 AWS Controls Matrix

The following table distinguishes between the sovereignty capabilities available in AWS's standard EU regions today and those promised for the future AWS European Sovereign Cloud.

Offering/Feature	Level(s) Covered	EU/DE Availability	Dependencies	Operational/Support Bounds	Legal/Contractual Notes	Status	Source
AWS in EU Regions (Current)	1. Data Residency	All 8 EU regions, including Frankfurt.	Customer configuration to select a region.	Support is a global operation. Enterprise Support offers some local language capabilities but no personnel location guarantee.	AWS Digital Sovereignty Pledge is a commitment, not a contractual guarantee for all points. Data processing agreement covers GDPR.	GA	[44]
AWS Nitro System	3. Data Access Sovereignty 5. Control Sovereignty (Data-in-use protection)	Available on all modern EC2 instances in all EU/DE regions.	N/A. It is the default foundation for modern EC2.	Technically designed to prevent AWS operator access to data in memory on EC2 instances.	Security design validated by a third-party report. Contractual assurance in AWS Service Terms.	GA	[44]
AWS KMS with External Key Store (XKS)	5. Control Sovereignty (Key custody)	Available in all EU/DE regions.	Requires a customer-managed external key manager and an XKS proxy.	Customer retains full control and custody of keys outside of AWS.	Customer is responsible for the availability, durability, and performance of the external key system.	GA	[46]

AWS Control Tower (Digital Sovereignty Controls)	1. Data Residency 2. Data Localization 8. Ecosystem/ Compliance	Available for managing accounts in all EU/DE regions.	Requires setup of AWS Control Tower and enabling the specific control set.	N/A. It is a governance and policy enforcement tool.	Provides an auditable way to enforce customer-defined policies.	GA	[44]
AWS European Sovereign Cloud	1, 2, 3, 4, 5, 6, 7, 8 (All levels)	First region in Brandenburg, Germany.	Will require a new, separate AWS account.	All operations and support performed exclusively by EU residents located in the EU.	Will have its own independent terms, billing, and metering systems.	Announced (Launch by end of 2025)	[45]

3.4 Limitations and Gaps

The primary limitations of AWS's current sovereignty posture stem from the gap between its present capabilities and its future vision.

- **Roadmap Dependency for Full Sovereignty:** AWS's most comprehensive solution, the European Sovereign Cloud, is not yet available. It is an announced offering with a target launch date of late 2025.[44] Customers with immediate, stringent operational sovereignty requirements cannot be served by this offering today and must rely on the controls available in the standard regions.
- **Lack of Operational Sovereignty (Current):** In the existing AWS EU regions, there is no native service or support plan that guarantees technical support and cloud operations are performed exclusively by EU personnel. AWS Support is a global organization.[60] While AWS Dedicated Local Zones can offer this control, it is a niche, single-tenant solution and not part of the general-purpose public cloud.[45] This is the most significant gap compared to the future sovereign cloud's promise.
- **Global Services and Metadata (Current):** While customers control the location of their primary data (content), certain AWS services are global by nature (e.g., IAM, Route 53). Furthermore, operational metadata, such as account and billing information, is aggregated and processed globally.[48] The fact that the European Sovereign Cloud is being designed specifically to keep all customer-created metadata within the EU underscores that this is a limitation of the current regional model.[48]
- **Initial Service Parity (Future):** The AWS European Sovereign Cloud will launch with a core set of services, but it will not have the full breadth of the 200+ services available in mature regions like Frankfurt or Ireland on day one.[48] The initial service list includes key categories like AI, compute, containers, and databases, but customers with applications relying on more niche or newer services will need to carefully track the service roadmap and may face delays in migration.[50]
- **Confidential Computing Nuances:** While the AWS Nitro System provides strong hypervisor-level isolation for all workloads on modern instances, AWS's application-level confidential computing story, via Nitro Enclaves, requires more developer effort to implement compared to the more straightforward "lift-and-shift" confidential VM

offerings from competitors. It is a powerful feature for specific use cases rather than a general-purpose VM encryption solution.[55]

3.5 Implementation Patterns

Organizations can implement different patterns on AWS to address sovereignty, keeping in mind the distinction between current and future capabilities.

- **Maximizing Sovereignty on AWS Today (Technical Controls):** This pattern focuses on leveraging all available technical controls in a standard AWS EU region like Frankfurt (eu-central-1). Workloads are deployed on modern, **Nitro-based EC2 instances** to benefit from hardware-level isolation. All sensitive data is encrypted using **AWS KMS with an External Key Store (XKS)**, ensuring keys remain under sovereign customer control outside of AWS.[46] Governance is enforced using **AWS Control Tower** to apply the **Digital Sovereignty** control set, which restricts actions to allowed regions and enforces encryption policies.[47] This pattern provides strong data residency, data access, and control sovereignty.
- **Hybrid Sovereignty for Edge and On-Premises Needs:** For workloads that must remain in a specific physical location due to latency or data processing laws, this pattern uses **AWS Outposts** or **AWS Dedicated Local Zones**. These offerings extend AWS infrastructure and services into a customer's data center or a specified location.[44] The infrastructure is parented to a full AWS EU region (e.g., Frankfurt), so the control plane resides in the EU, but the data processing and storage occur at the customer's site, providing physical control over the data.
- **Strategic Planning for the European Sovereign Cloud (Future):** This pattern is for organizations whose requirements can only be met by the future isolated cloud. The approach involves architecting applications in a standard AWS EU region today using Infrastructure as Code (IaC) tools like AWS CloudFormation. The architecture should prioritize the use of services that have been announced as part of the initial service portfolio for the European Sovereign Cloud.[50] This "build-and-wait" strategy prepares the organization for a more streamlined migration to the new, independent cloud once it launches in 2025 and they can create a new, dedicated account for it.[48]

Section 4: Cross-Hyperscaler Comparative Analysis

The digital sovereignty landscape in the EU is defined by three distinct strategic approaches from the major cloud providers. Google Cloud offers a flexible, configurable model; Microsoft Azure champions a broad, default boundary; and Amazon Web Services is building a future based on complete isolation. Each strategy presents a unique set of strengths, weaknesses, and critical trade-offs for European organizations, particularly those in Germany navigating stringent regulatory requirements.

The choice between these providers is not merely technical but strategic, hinging on an organization's specific risk tolerance, operational model, budget, and long-term compliance roadmap. The decision requires a nuanced understanding of the differences between contractual promises, technical enforcement, operational realities, and future commitments. While all three providers offer powerful tools for data residency and cryptographic control, their core philosophies on how to deliver sovereignty lead to vastly different implementation paths and levels of assurance.

4.1 Summary Comparison Table

This table provides a succinct, comparative verdict on how GCP, Azure, and AWS address each key dimension of digital sovereignty based on their current and announced offerings for the EU/Germany.

Sovereignty Dimension	GCP Verdict & Rationale	Azure Verdict & Rationale	AWS Verdict & Rationale
1. Data Residency	**Strong:** Assured Workloads provides explicit, policy-enforced control over resource location in specified EU regions. [6]	**Strong:** The EU Data Boundary provides a broad, default contractual commitment for in-scope services to reside in the EU. [26]	**Strong:** Customers have always had full control to select an EU region for their data. [44]
2. Data Localization *(Strict in-region metadata)*	**Limited:** While customer data is resident, some operational metadata may be processed globally. The T-Systems offering provides stronger guarantees for Germany. [3]	**Limited:** The EU Data Boundary has documented exceptions for global services like Entra ID and for operational telemetry. [26]	**Announced Only:** The future European Sovereign Cloud is explicitly designed to keep all customer-created metadata in the EU, acknowledging this is a gap today. [48]
3. Data Access Sovereignty *(Technical access controls)*	**Strong:** Key Access Justifications (KAJ) with EKM provides a unique, customer-controlled cryptographic	**Moderate:** Relies on contractual commitments and authorization policies for provider access. Strong technical	**Strong:** The AWS Nitro System is designed at the hardware level to prevent provider access to data in use on EC2, with

	approval/denial mechanism for provider access. [5]	mitigation via Confidential Computing is available. [22]	third-party validation. [44]
4. Operational Sovereignty *(EU-only personnel/support)*	**Strong:** The "EU Data Boundary and Support" package explicitly guarantees support by EU personnel located in the EU, as does the T-Systems offering. [3]	**Limited:** The EU Data Boundary allows for remote operations by non-EU personnel, though data access requires authorization. No default EU-only support guarantee. [26]	**Announced Only:** The European Sovereign Cloud is the only offering that will guarantee operations and support exclusively by EU-resident personnel. This is a key gap in current offerings. [48]
5. Control Sovereignty *(Keys, Confidential Compute)*	**Strong:** Comprehensive portfolio including Cloud EKM, Confidential VMs/GKE, and Cloud HSM. [4]	**Strong:** Comprehensive portfolio including Confidential VMs/Containers, Managed/Dedicated HSM, and SQL Always Encrypted. [22]	**Strong:** Offers AWS KMS with XKS for external keys and the Nitro System for data-in-use protection. [44]
6. Legal/Contractual Posture	**Tiered:** Offers different levels of assurance through specific Assured Workloads packages and partner contracts. [1]	**Broad:** The EU Data Boundary is a sweeping contractual commitment that serves as the primary legal guarantee for customers. [26]	**Pledge-Based:** Currently relies on the Digital Sovereignty Pledge. The future ESC will have its own independent contractual framework. [44]
7. Isolation Model	**Configured:** Sovereignty is achieved by applying software-defined controls and policies to the standard global cloud. [2]	**Configured:** Sovereignty is a default operational posture on the standard global cloud, defined by a contractual boundary. [27]	**Announced Isolated:** The future European Sovereign Cloud will be a physically and logically separate, independent cloud. [45]
8. Ecosystem/ Compliance	**Strong:** Extensive list of supported services in Assured Workloads and a mature partner ecosystem (e.g., T-Systems). [3]	**Strong:** The EU Data Boundary applies to a very broad set of services across Azure, M365, and Dynamics. Extensive compliance certifications. [26]	**Strong:** Mature partner network and compliance posture in existing regions. The ESC will launch with key partner support. [44]

4.2 Strategic Analysis and Recommendations

Each provider's strategy presents a distinct value proposition and set of trade-offs for customers in the EU and Germany. **Google Cloud** is strongest in its flexibility and the granularity of its controls. The ability to layer different Assured Workloads packages, combined with technical tools like KAJ and Confidential Computing, allows organizations to engineer a precise sovereignty posture. The T-Systems partnership provides a unique,

high-assurance solution for the German market that is available today. GCP's primary weakness is the resulting complexity; achieving high levels of sovereignty requires configuring and managing multiple, interdependent services, and its foundation on a globally integrated infrastructure means absolute isolation is not the goal of its native offerings.

Microsoft Azure is strongest in its simplicity and the breadth of its EU Data Boundary commitment. For many organizations, the "sovereignty by default" approach reduces the overhead of configuration and provides a clear contractual basis for compliance across a vast portfolio of services. Its weakness lies in the transparency of its exceptions. The reliance on global services like Entra ID and the allowance for remote operations by non-EU personnel create known gaps in the boundary that require careful risk assessment. The strength of its promise is directly tied to the customer's trust in Microsoft's operational and legal safeguards rather than verifiable technical isolation for all data types.

Amazon Web Services is strongest in its foundational hardware security with the Nitro System and its uncompromising long-term vision for the AWS European Sovereign Cloud. The promise of a fully isolated cloud, operated solely by EU personnel, is designed to be the definitive answer to the most stringent sovereignty demands. Its primary weakness is timing and the current reality. The European Sovereign Cloud is a future product, and its current offerings in standard EU regions, while technically secure at the hypervisor level, lack the comprehensive operational and metadata sovereignty controls that its competitors offer through specific packages today. Committing to AWS for maximum sovereignty is a bet on their roadmap and an acceptance of a future migration effort.

Organizations in EU/Germany must weigh these strategic trade-offs carefully. The choice between **configuration vs. boundary vs. isolation** is central. An organization comfortable with managing a complex but powerful set of software-defined controls may favor GCP. An organization that prioritizes ease of adoption and a broad contractual guarantee across a wide service portfolio may prefer Azure. An organization for whom complete operational and physical isolation is a non-negotiable future requirement, and that has the resources to plan for a 2025+ migration, will find AWS's strategy most compelling.

Section 5: 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.

Section 6: Due Diligence Checklist for Implementation

To move beyond marketing claims and ensure a chosen cloud solution meets specific regulatory and security requirements, organizations should use the following checklist to conduct rigorous due diligence with providers.

- **Data Residency & Localization:**
  - [ ] Request a complete data-flow diagram for a representative workload, detailing the geographic path of not only customer content but also all associated metadata (e.g., IAM roles, resource tags, monitoring metrics, billing data, support case data).
  - [ ] Obtain a written list of all services that are non-regional or have dependencies that transmit data (content or metadata) outside the EU.
  - [ ] Clarify the provider's data destruction policies (crypto-shredding vs. physical destruction) and the timelines for data removal upon contract termination.

- **Operational & Access Sovereignty:**
  - [ ] Demand contractual guarantees and audit rights to verify the physical location and legal residency/citizenship of *all* personnel with potential privileged access, including L1-L3 support, Site Reliability Engineers (SREs), and on-call engineers for emergency response.
  - [ ] Document the complete support case escalation path. Under what specific circumstances (e.g., service outage, security incident) can a case be accessed by non-EU personnel? What are the controls and logs for such an event?
  - [ ] If an EU-only support model is offered, verify if this applies 24/7/365 and for all severity levels.
- **Control Sovereignty:**
  - [ ] Require a live demonstration of the "break-glass" capability using an External Key Store (EKM/XKS). Can the customer verifiably and instantly render all cloud data cryptographically inaccessible to the provider by revoking keys in their external system?
  - [ ] What is the measured performance latency impact of cryptographic operations when using an EKM/XKS compared to the native KMS?
  - [ ] For Confidential Computing offerings, request the detailed attestation process. How can a customer remotely and cryptographically verify that a VM or container is running on genuine confidential hardware with the correct, untampered software image before releasing secrets to it?
- **Service Scope & Limitations:**
  - [ ] For every AWS/Azure/GCP service intended for use, require a written confirmation that it is fully covered by the relevant sovereignty boundary or control package (e.g., Assured Workloads, EU Data Boundary).
  - [ ] Obtain a precise list of any service features that will be disabled, degraded, or operate differently when deployed within the sovereign environment.
  - [ ] Clarify how new services or features are brought into compliance with the sovereignty offering. What is the typical time lag between a new feature's general availability and its availability within the sovereign configuration?
- **Roadmap & GA Status:**
  - [ ] For any feature cited as part of the sovereignty solution that is currently in Preview, request the committed General Availability (GA) date, the expected GA Service Level Agreement (SLA), and the final GA pricing.
  - [ ] For announced offerings like the AWS European Sovereign Cloud, request the detailed service availability roadmap for the first 24 months post-launch. Which specific services, instance types, and features will be available at launch versus 6, 12, and 24 months later?
  - [ ] What are the provider's contractual commitments and remedies if announced roadmap timelines for critical sovereignty features are not met?

Works cited

1. Data Boundary via Assured Workloads | Sovereign Cloud - Google Cloud, https://cloud.google.com/security/products/assured-workloads
2. Overview of Assured Workloads - Google Cloud Documentation, https://docs.cloud.google.com/assured-workloads/docs/overview
3. T-Systems Sovereign Cloud | Google Cloud, https://cloud.google.com/t-systems-sovereign-cloud
4. Confidential Computing | Google Cloud, https://cloud.google.com/security/products/confidential-computing
5. Cloud Key Management | Google Cloud, https://cloud.google.com/security/products/security-key-management
6. EU Data Boundary | Assured Workloads - Google Cloud Documentation, https://docs.cloud.google.com/assured-workloads/docs/control-packages/eu-data-boundary
7. EU Data Boundary | Assured Workloads - Google Cloud, https://cloud.google.com/assured-workloads/docs/control-packages/eu-data-boundary
8. Getting support | Assured Workloads - Google Cloud, https://cloud.google.com/assured-workloads/docs/getting-support
9. Enhanced Support overview | Cloud Customer Care - Google Cloud Documentation, https://docs.cloud.google.com/support/docs/enhanced
10. Sovereign Controls by Partners locations | Google Cloud, https://cloud.google.com/sovereign-controls-by-partners/docs/locations
11. Confidential Computing overview - Google Cloud, https://cloud.google.com/confidential-computing/docs/confidential-computing-overview
12. Confidential VM overview - Google Cloud Documentation, https://docs.cloud.google.com/confidential-computing/confidential-vm/docs/confidential-vm-overview
13. Cloud Key Management Service overview | Google Cloud Documentation, https://docs.cloud.google.com/kms/docs/key-management-service
14. Cloud External Key Manager | Cloud Key Management Service - Google Cloud, https://cloud.google.com/kms/docs/ekm
15. Europe (regions) - Google Cloud Service Health, https://status.cloud.google.com/regional/europe
16. EU Data Boundary and Support | Assured Workloads - Google Cloud, https://cloud.google.com/assured-workloads/docs/control-packages/eu-data-boundary-support
17. Geography and regions | Get started - Google Cloud Documentation, https://docs.cloud.google.com/docs/geography-and-regions
18. EU Data Boundary with Access Justifications | Assured Workloads - Google Cloud, https://cloud.google.com/assured-workloads/docs/control-packages/eu-data-bo

undary-access-justifications
19. Service Specific Terms | Google Cloud, https://cloud.google.com/legal/archive/terms/service-terms/index-20250828
20. Connect to Google Drive | Gemini Enterprise, https://docs.cloud.google.com/gemini/enterprise/docs/connect-google-drive
21. Engineering Deutsche Telekom's sovereign data platform | Google Cloud Blog, https://cloud.google.com/blog/topics/customers/engineering-deutsche-telekoms-sovereign-data-platform
22. Azure Confidential Computing – Protect Data In Use, https://azure.microsoft.com/en-us/solutions/confidential-compute
23. Key foundations for protecting your data with Azure confidential computing, https://azure.microsoft.com/en-us/blog/key-foundations-for-protecting-your-data-with-azure-confidential-computing/
24. Key Vault pricing - Microsoft Azure, https://azure.microsoft.com/en-us/pricing/details/key-vault/
25. Azure Dedicated HSM pricing, https://azure.microsoft.com/en-us/pricing/details/azure-dedicated-hsm/
26. Data Residency in Azure | Microsoft Azure, https://azure.microsoft.com/en-us/explore/global-infrastructure/data-residency
27. Data Residency, Data Sovereignty, and Compliance in the Microsoft Cloud - Microsoft Azure, https://azure.microsoft.com/mediahandler/files/resourcefiles/data-residency-data-sovereignty-and-compliance-in-the-microsoft-cloud/Data_Residency_Data_Sovereignty_Compliance_Microsoft_Cloud.pdf
28. What are public, private, and hybrid clouds? - Microsoft Azure, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-are-private-public-hybrid-clouds
29. What is a Hybrid Cloud? | Microsoft Azure, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-hybrid-cloud-computing
30. Introducing Azure confidential computing | Microsoft Azure Blog, https://azure.microsoft.com/en-us/blog/introducing-azure-confidential-computing/
31. Azure confidential computing with NVIDIA GPUs for trustworthy AI, https://azure.microsoft.com/en-us/blog/azure-confidential-computing-with-nvidia-gpus-for-trustworthy-ai/
32. Confidential ledger – Distributed Ledger Technology | Microsoft Azure, https://azure.microsoft.com/en-us/products/azure-confidential-ledger
33. Azure Cloud HSM - Pricing, https://azure.microsoft.com/en-us/pricing/details/azure-cloud-hsm/
34. Protecting Azure Infrastructure from silicon to systems | Microsoft Azure Blog, https://azure.microsoft.com/en-us/blog/protecting-azure-infrastructure-from-silicon-to-systems/
35. Choose the Right Azure Region for You - Microsoft Azure, https://azure.microsoft.com/en-in/explore/global-infrastructure/geographies/

36. Choose the Right Azure Region for You - Microsoft Azure, https://azure.microsoft.com/en-us/explore/global-infrastructure/geographies
37. Choose the Right Azure Region for You - Microsoft Azure, https://azure.microsoft.com/en-ca/explore/global-infrastructure/geographies
38. Microsoft Cloud coming to France | Microsoft Azure Blog, https://azure.microsoft.com/en-us/blog/microsoft-cloud-coming-to-france/
39. Pricing – Azure SQL Managed Instance Pools, https://azure.microsoft.com/en-us/pricing/details/azure-sql-managed-instance/pools/
40. Announcing new innovations for SAP on Microsoft Cloud | Microsoft Azure Blog, https://azure.microsoft.com/en-us/blog/announcing-new-innovations-for-sap-on-microsoft-cloud/
41. Supplemental Terms of Use for Microsoft Azure Previews, https://azure.microsoft.com/en-us/support/legal/preview-supplemental-terms
42. Enabling Data Residency and Data Protection in Microsoft Azure Regions, https://azure.microsoft.com/mediahandler/files/resourcefiles/achieving-compliant-data-residency-and-security-with-azure/Enabling_Data_Residency_and_Data_Protection_in_Azure_Regions-2021.pdf
43. Azure Governance, https://azure.microsoft.com/en-au/solutions/governance
44. AWS Digital Sovereignty, https://aws.amazon.com/compliance/digital-sovereignty/
45. European Digital Sovereignty – Amazon Web Services, https://aws.amazon.com/compliance/europe-digital-sovereignty/
46. External key stores - AWS Key Management Service - AWS Documentation, https://docs.aws.amazon.com/kms/latest/developerguide/keystore-external.html
47. View control details - AWS Control Tower - AWS Documentation, https://docs.aws.amazon.com/controltower/latest/controlreference/control-details.html
48. In the Works – AWS European Sovereign Cloud | AWS News Blog, https://aws.amazon.com/blogs/aws/in-the-works-aws-european-sovereign-cloud/
49. AWS Digital Sovereignty Pledge: Announcing a new, independent sovereign cloud in Europe, https://aws.amazon.com/blogs/security/aws-digital-sovereignty-pledge-announcing-a-new-independent-sovereign-cloud-in-europe/
50. Announcing initial services available in the AWS European Sovereign Cloud, backed by the full power of AWS | AWS Security Blog, https://aws.amazon.com/blogs/security/announcing-initial-services-available-in-the-aws-european-sovereign-cloud-backed-by-the-full-power-of-aws/
51. Establishing a European trust service provider for the AWS European Sovereign Cloud, https://aws.amazon.com/blogs/security/establishing-a-european-trust-service-provider-for-the-aws-european-sovereign-cloud/
52. AWS plans to invest €7.8B into the AWS European Sovereign Cloud, set to launch by the end of 2025 | AWS Security Blog,

https://aws.amazon.com/blogs/security/aws-plans-to-invest-e7-8b-into-the-aws-european-sovereign-cloud-set-to-launch-by-the-end-of-2025/
53. AWS Digital Sovereignty Pledge: Control without compromise, https://aws.amazon.com/blogs/security/aws-digital-sovereignty-pledge-control-without-compromise/
54. How AWS is helping customers achieve their digital sovereignty and resilience goals, https://aws.amazon.com/blogs/security/how-aws-is-helping-customers-achieve-their-digital-sovereignty-and-resilience-goals/
55. AWS Silicon Innovation – Amazon Web Services, https://aws.amazon.com/silicon-innovation/
56. AWS Nitro Enclaves, https://aws.amazon.com/ec2/nitro/nitro-enclaves/
57. Create an external key store - AWS Key Management Service - AWS Documentation, https://docs.aws.amazon.com/kms/latest/developerguide/create-xks-keystore.html
58. Search for controls with Amazon Q - AWS Control Tower, https://docs.aws.amazon.com/controltower/latest/controlreference/q-search.html
59. AWS Regions and Availability Zones - AWS Documentation, https://docs.aws.amazon.com/global-infrastructure/latest/regions/aws-regions.html
60. AWS Premium Support FAQs - Amazon.com, https://aws.amazon.com/premiumsupport/faqs/
61. Global Infrastructure Regions & AZs - AWS, https://aws.amazon.com/about-aws/global-infrastructure/regions_az/
62. Azure gains 100th compliance offering—protecting data with EU Cloud Code of Conduct, https://azure.microsoft.com/en-us/blog/azure-gains-100th-compliance-offering-protecting-data-with-eu-cloud-code-of-conduct/
63. Empowering European Innovation: Partner Solutions for the AWS European Sovereign Cloud | AWS Partner Network (APN) Blog, https://aws.amazon.com/blogs/apn/empowering-european-innovation-partner-solutions-for-the-aws-european-sovereign-cloud/