My Deep Research Analysis of Digital Sovereignty on EU Cloud IONOS and STACKIT for EU/German regulated Workloads

Executive Summary

- **STACKIT's Technical Superiority:** STACKIT offers a more comprehensive and technically advanced suite of sovereignty controls, including a dedicated Key Management Service (KMS) with Bring Your Own Key (BYOK) capabilities, generally available Confidential Computing offerings, and a contractually guaranteed EU-only support model.
- **IONOS's Market Presence:** IONOS demonstrates a strong market position in the German public sector, evidenced by its partnership with ITZBund, but its platform currently lacks advanced control and operational sovereignty features equivalent to STACKIT.
- **The Control Plane Divide:** A fundamental differentiator lies in encryption control; STACKIT provides platform-level, customer-controlled encryption via its KMS, whereas IONOS's model largely relies on provider-managed encryption for infrastructure or application-level encryption managed by the customer.
- **Compliance Nuances:** While both providers hold key certifications, STACKIT's BSI C5

Type 2 attestation for its core infrastructure offers a higher level of assurance (operational effectiveness over time) compared to IONOS's C5 Type 1 attestation (design effectiveness at a point in time).

- **Contractual Scrutiny Required:** STACKIT's marketing emphasizes a strict EU data boundary, yet its Data Processing Agreement (DPA) includes clauses permitting data transfers outside the European Economic Area (EEA) under specific GDPR-compliant conditions, a critical detail requiring customer due diligence.
- **Operational Sovereignty Gap:** STACKIT explicitly offers an "Ultimate Support" plan with guaranteed EU-only personnel. IONOS's official documentation lacks a comparable, contractually defined offering, representing a significant potential gap for customers concerned with non-EU personnel access.
- **The Customer's Dilemma:** The choice represents a strategic trade-off: IONOS offers proven market tenure and public sector adoption with foundational sovereignty features, while STACKIT provides a technologically superior sovereignty posture, albeit with some of its most advanced services being newer to the market.

Section 1: IONOS Digital Sovereignty Posture

1.1 Sovereignty Offerings Overview

IONOS SE is a major European web hosting and cloud provider with a strong German foundation, positioning itself as a GDPR-compliant alternative to US-based hyperscalers.[1] The company's sovereignty narrative is built upon its core Infrastructure-as-a-Service (IaaS) offerings—Compute Engine, Cloud Cubes, and S3 Object Storage—which serve as the foundation for its value proposition to regulated industries and the public sector.[2] IONOS makes public commitments to "robust privacy and data protection," "no data monetization or reselling," and explicit protection against the US CLOUD Act for services hosted within its German data centers.[1]

A significant proof point of its suitability for sensitive workloads is its engagement with ITZBund, the central IT service provider for the German federal government. This partnership underscores IONOS's focus on providing a sovereign digital infrastructure for Germany.[2] All core services relevant to this analysis, including the Compute Engine, Object Storage, and Backup Service, are presented as Generally Available (GA) across the provider's official documentation and product pages.[1]

1.2 EU/Germany Availability

The physical location of data centers is the cornerstone of IONOS's data residency and localization guarantees. The provider offers customers a choice of several locations within Germany and the broader European Union.

- **German Locations:** IONOS operates multiple data centers in Germany, with key cloud regions located in Frankfurt am Main and Berlin. These facilities are the primary choice for customers requiring the strictest level of data localization under German law.[4]
- **EU Locations:** Beyond Germany, IONOS maintains a presence in other European markets with data centers in Paris (France), London and Worcester (UK), and Logroño (Spain).[4]
- **Customer Choice and Control:** A critical feature of the IONOS Cloud platform is the Data Center Designer (DCD), a tool that allows customers to select the specific geographic location where their virtual data center (VDC) and associated data will be provisioned. IONOS makes a contractual commitment in its Data Processing Agreement (DPA) not to move customer data to other locations without explicit consent, providing a direct mechanism for enforcing data residency.[3]

1.3 IONOS Controls Matrix

The following table maps IONOS's features to the defined digital sovereignty levels, providing a granular, evidence-based assessment of its capabilities as of June 28, 2024.

Offering/Feature	Level(s) Covered	EU/DE Availability	Dependencies	Operational/Support Bounds	Legal/Contractual Notes	Status	Source
Data Center Selection	1. Data Residency 2. Data Localization	Frankfurt, Berlin (DE); Paris, London, Logroño (EU)	Customer must select the desired region in the Data Center Designer (DCD).	No explicit EU-only operational bounds stated.	DPA states data is not moved without customer consent.	GA	[3]
Compute Engine & Block Storage	1. Data Residency 2. Data Localization	All DE/EU regions.	N/A	Provider-managed encryption keys are inaccessible to root users and bound to IONOS infrastructure.	Stated GDPR compliance and protection from US CLOUD Act when hosted in Germany.	GA	[2]
Block Storage Encryption at Rest	(Limited) 5. Control Sovereignty	All DE/EU regions.	N/A	Provider-managed AES-XTS 256-bit encryption. Keys are not customer-controlled or viewable.	Secure deletion process is tied to the destruction of provider-managed metadata/key.	GA	[5]
Backup Service (Customer-Side Encryption)	5. Control Sovereignty	All DE/EU regions.	Customer must enable and manage a password for each backup plan.	Customer holds the password/key; IONOS cannot recover it.	DPA outlines shared responsibility for security.	GA	[3]
Object	(Limited) 5.	All DE/EU S3	N/A	Refers to	N/A	GA	[7]

Storage (S3) Key Management	Control Sovereignty	endpoints.		customer-managed Access/Secret keys for API authentication, not data encryption keys (BYOK).			
Legal Posture & DPA	6. Legal/ Contractual	All EU contracts.	A DPA must be in place for processing personal data.	DPA is based on GDPR Art. 28.	Commits to GDPR compliance. Customer is the controller, IONOS is the processor.	GA	[3]
Compliance & Certifications	8. Ecosystem/ Compliance	Data centers and specific services.	N/A	Audits performed by third parties.	ISO 27001 for data centers. BSI C5 (Type 1) for Compute Engine, Cloud Cubes, S3 Object Storage.	GA	[4]
Professional Support	(Limited) 4. Operational Sovereignty	Global	N/A	No explicit commitment to EU-only support personnel found in official sources. Support is available 24/7.	N/A	GA	[2]

1.4 Limitations & Gaps

While IONOS provides a strong foundation for data residency, a critical analysis of its official documentation reveals several gaps in the higher tiers of digital sovereignty. For customers with stringent requirements, the ambiguity around operational controls is a significant concern. A common risk in the cloud industry is the "follow-the-sun" support model, where a support ticket containing sensitive diagnostic data could be accessed by an engineer in a non-EU jurisdiction, making that data subject to foreign laws. Without a contractual guarantee of EU-only support staff, full operational sovereignty cannot be assured, placing the burden on the customer to seek specific contractual assurances that may or may not be granted.

- **No Centralized KMS/BYOK:** The platform lacks a dedicated Key Management Service for IaaS. The term "customer-managed keys" in the context of IONOS Object Storage refers to Access and Secret Keys used for API authentication, not customer-provided encryption keys (BYOK) for data at rest.[7] This prevents customers from centrally controlling and auditing the cryptographic lifecycle of their data, falling short of true Control Sovereignty.
- **No Confidential Computing:** Official sources do not mention any offerings for confidential computing, such as services based on Intel SGX or AMD SEV/SNP technologies.[12] This means data-in-use remains accessible to the cloud provider's infrastructure, a critical gap for workloads processing highly sensitive information.
- **Limited Operational Sovereignty Guarantees:** As noted, there is no documented,

public commitment to an EU-only support or operations model.[2] This leaves a potential vector for non-EU/EEA data access for administrative and support functions.
- **BSI C5 Type 1 Attestation:** While valuable, the BSI C5 Type 1 attestation for core services only validates the *design* of security controls at a specific point in time. It does not provide assurance of their *operational effectiveness* over a period, which is covered by a more rigorous Type 2 report.

1.5 Implementation Patterns

To maximize digital sovereignty on the IONOS platform, customers should adopt a multi-layered strategy that leverages available controls while compensating for existing gaps.
- **Strict Region Pinning:** The primary and most effective pattern is to exclusively provision all cloud resources within German data centers (Frankfurt, Berlin) using the Data Center Designer. This ensures data at rest and data in processing are strictly localized within Germany.[3]
- **Leverage Backup Service Encryption:** For sensitive data where customer-held keys are paramount, the recommended pattern is to use the IONOS Backup Service and enable the customer-side encryption feature. This ensures the customer retains sole control over the password-derived key required for backup decryption.[6]
- **In-VM/Application-Level Encryption:** Given the absence of a platform-level KMS for IaaS, customers must implement their own encryption solutions within their virtual machines or application code. This requires customers to manage the entire key lifecycle independently, adding operational overhead but ensuring cryptographic control.
- **Contractual Clarification:** Customers with strict operational sovereignty requirements must engage directly with IONOS legal and sales teams to seek specific contractual addenda that explicitly define the jurisdictional location of all personnel (including sub-processors) involved in support and operations.

Section 2: STACKIT Digital Sovereignty Analysis

2.1 Sovereignty Offerings Overview

STACKIT is the cloud and colocation provider of the Schwarz Group, the German retail giant that owns Lidl and Kaufland. Its market positioning is explicitly focused on delivering a "sovereign cloud for Europe," built on a foundation of economic, technological, and political independence.[14] The core tenets of its strategy include the exclusive use of its own data centers in Germany and Austria, a deep commitment to open-source technologies like OpenStack to prevent vendor lock-in, and its status as a German company not subject to extraterritorial laws like the US CLOUD Act.[16]

STACKIT offers several services specifically designed to provide higher levels of sovereignty:

- **STACKIT Key Management Service (KMS):** A dedicated, managed service for creating, managing, and using cryptographic keys. Crucially, it supports the import of customer-owned keys (BYOK), enabling a separation of duties between the cloud provider and the data owner.[18] This service is Generally Available (GA).
- **STACKIT Confidential Computing:** This family of services includes **STACKIT Confidential Server**, which provides Confidential Virtual Machines (CVMs) based on AMD SEV technology, and **STACKIT Confidential Kubernetes**, an end-to-end encrypted Kubernetes environment based on Edgeless Systems Constellation. These services protect data while it is in use (in-memory).[19] Confidential Kubernetes is presented as GA, while Confidential Server is available "on request," indicating a preview or limited offering status.[20]
- **STACKIT Ultimate Support:** A premium support tier that contractually guarantees service delivery by personnel located exclusively within the European Union, directly addressing operational sovereignty concerns.[21] This service is GA.

2.2 EU/Germany Availability

STACKIT's geographic footprint is intentionally focused and limited to ensure a high degree of control and compliance with EU regulations.

- **Regions:** The provider operates two distinct regions: **Germany-South (EU01)**, with data centers in Neckarsulm and Ellhofen, and **Austria-West (EU02)**, with a data center in Ostermiething.[22]
- **Service Parity Gap:** A critical limitation exists in service availability between these regions. The most advanced sovereignty-enabling services—including Confidential Computing, the Key Management Service, and most Database and Runtime services—are currently available *only* in the Germany-South (EU01) region.[23] This requires customers seeking the highest levels of sovereignty to deploy their workloads exclusively in Germany.

2.3 STACKIT Controls Matrix

The following table maps STACKIT's features to the defined digital sovereignty levels, highlighting its strengths in providing advanced technical and operational controls as of June 28, 2024.

Offering/Feature	Level(s) Covered	EU/DE Availability	Dependencies	Operational/Support Bounds	Legal/Contractual Notes	Status	Source
EU Data Centers	1. Data Residency 2. Data Localization	Germany-South (EU01), Austria-West (EU02)	N/A	Data centers are owned and operated by STACKIT/Schwarz Group.	DPA commits to EEA processing by default, but allows for non-EEA	GA	[16]

					transfers with notice and SCCs.		
Ultimate Support	3. Data Access Sovereignty 4. Operational Sovereignty	Available for all regions.	Premium support subscription.	**Support is explicitly and "fully provided from within the EU."** Personnel are located in Europe.	SLA includes 15-min reaction time.	GA	[21]
Key Management Service (KMS)	5. Control Sovereignty	Germany-South (EU01) only.	N/A	Customer can generate, manage lifecycle, and import their own keys (BYOK).	Enables separation of duties between data storage and key control.	GA	[18]
Confidential Server	5. Control Sovereignty	Germany-South (EU01) only.	Based on AMD SEV-ES hardware. Customer must provide their own OS image.	Provides hardware-based memory encryption to isolate VM from hypervisor/provider.	Customer is solely responsible for OS management, patching, and backups.	Preview / On Request	[20]
Confidential Kubernetes	5. Control Sovereignty	Germany-South (EU01) only.	Based on Confidential Server (AMD SEV) and Edgeless Systems Constellation.	End-to-end encryption (rest, transit, use). Cluster is isolated from provider access.	Customer is responsible for Day-2 operations (backup, recovery, upgrades).	GA	[19]
Legal Posture & DPA	6. Legal/ Contractual	All EU contracts.	DPA is part of the main agreement.	DPA allows for non-EEA sub-processors with customer notification and right to object.	German company, states no obligation to comply with US CLOUD Act.	GA	[17]
Compliance & Certifications	8. Ecosystem/ Compliance	Data centers and specific services.	N/A	Audits performed by third parties (e.g., TÜV SÜD).	ISO 27001, ISO 20000. **BSI C5 (Type 2)** for core infrastructure.	GA	[27]
Open Source Foundation	7. Isolation Model	Entire platform.	Based on OpenStack.	Aims to prevent vendor lock-in and increase transparency.	GA	[14]	

2.4 Limitations & Gaps

Despite STACKIT's strong technical posture, a balanced assessment reveals constraints and areas that require careful customer due diligence. The most significant of these is a potential contradiction between the company's marketing, which strongly implies an absolute EU-only data processing boundary, and its binding legal agreements. The official Data Processing Agreement explicitly includes clauses that permit data processing outside the European Economic Area (EEA), provided that GDPR-compliant mechanisms like Standard Contractual Clauses (SCCs) are used and the customer is notified.[26] This creates a "sovereignty escape hatch" that could be a point of concern for public sector or critical infrastructure clients who

require an unbreakable guarantee of EEA-only processing for all data, including metadata and support data. It shifts the burden of risk management to the customer, who must monitor notifications of new sub-processors and be prepared to object or terminate their contract.

- **Uneven Regional Service Availability:** The most compelling sovereignty features, including the KMS and Confidential Computing, are exclusively available in the Germany-South (EU01) region.[23] This limits options for customers seeking geographic redundancy in Austria while maintaining the highest level of control.
- **Maturity and Operational Overhead:** Advanced features like Confidential Server and Confidential Kubernetes are designed for maximum provider isolation, which places significant operational responsibility on the customer for OS management, patching, backups, and Day-2 operations.[24] This increases the customer's total cost of ownership and demands a higher level of technical maturity compared to more traditional managed services.
- **Preview Status of Key Services:** The STACKIT Confidential Server is still listed as available only "on request," suggesting it may not be a standard, fully productized offering. This could impact scalability, support, and ease of adoption for new customers.[20]

2.5 Implementation Patterns

To achieve the highest degree of digital sovereignty on the STACKIT platform, customers should adopt an architecture that fully utilizes its specialized services.

- **Germany-Centric Deployment:** Deploy all workloads in the Germany-South (EU01) region to gain access to the complete suite of sovereignty-enabling services, including KMS and Confidential Computing.[23]
- **Mandatory Use of KMS with BYOK:** Utilize the STACKIT KMS for all sensitive applications. The strongest security posture is achieved by importing customer-generated keys (BYOK), ensuring that STACKIT never has access to the plaintext key material.[18]
- **Tiered Workload Placement:** Deploy the most sensitive workloads, such as those processing personal health information or performing cryptographic operations, on STACKIT Confidential Server or Confidential Kubernetes. This ensures data is protected while in use through hardware-based memory encryption.[19]
- **Procure Ultimate Support:** Subscribe to the Ultimate Support plan to obtain a contractual guarantee that all support interactions are handled exclusively by EU-based personnel, thereby closing the operational sovereignty loop.[21]
- **DPA Scrutiny and Negotiation:** Proactively engage with STACKIT's legal team to gain clarity on the circumstances under which non-EEA sub-processors might be used. Customers with absolute requirements should seek to negotiate a contractual addendum that restricts or eliminates the use of the non-EEA processing clause.

Section 3: Cross-Provider Comparison and Strategic Recommendations

3.1 Sovereignty Dimensions Summary Table

This table provides a comparative summary of IONOS and STACKIT across the eight defined sovereignty dimensions, distilling the detailed findings into a clear verdict for at-a-glance evaluation.

Sovereignty Dimension	IONOS Verdict	STACKIT Verdict
1. Data Residency	**Strong:** Customer has full control to select DE/EU data center locations. [3]	**Strong:** Customer has full control to select DE/AT data center locations. [23]
2. Data Localization	**Strong:** Contractual guarantee not to move data from chosen region without consent. [3]	**Strong:** Data centers are provider-owned and operated exclusively in DE/AT. [16]
3. Data Access Sovereignty	**Limited:** No explicit, documented controls to limit non-EU personnel access.	**Strong:** "Ultimate Support" plan contractually guarantees EU-only support personnel. [21]
4. Operational Sovereignty	**Limited:** No explicit commitment to jurisdiction-bounded operations or support models found.	**Strong:** "Ultimate Support" plan provides a contractually defined EU-only operational model for support. [21]
5. Control Sovereignty	**Limited:** Lacks KMS/BYOK and Confidential Computing. Control is limited to application-level (e.g., Backup Service password). [6]	**Strong:** Comprehensive offering with dedicated KMS (BYOK support) and Confidential Computing (Server/Kubernetes) for data-in-use protection. [18]
6. Legal/Contractual Posture	**Moderate:** Strong GDPR commitment and stated protection from CLOUD Act, but lacks specificity on operational controls in DPA. [2]	**Moderate:** Strong German legal foundation, but DPA contains clauses allowing for potential non-EEA processing, requiring scrutiny. [17]
7. Isolation Model	**Moderate:** Standard shared public cloud model with customer-chosen regional isolation.	**Strong:** Offers advanced isolation via Confidential Computing, creating a "private cloud" experience on public infrastructure. [19]
8. Ecosystem/Compliance	**Moderate:** Key certifications including ISO 27001 and BSI C5 (Type 1). [2]	**Strong:** Extensive certifications including ISO 27001 and a more rigorous BSI C5 (Type 2) attestation. [27]

3.2 Comparative Analysis & Customer Guidance

As of June 28, 2024, STACKIT's primary strength lies in its purpose-built, technically deep sovereignty features, offering superior control through its KMS and Confidential Computing services, and greater operational assurance via its EU-only support model. It is the clear leader for customers whose threat model includes sophisticated state-level actors or who require the highest levels of cryptographic control and verifiable operational isolation.
IONOS's strength is its established market presence, particularly its adoption by the German public sector via the ITZBund contract, and its straightforward, foundational data residency guarantees. Its primary weakness is a significant lag in the advanced technical controls necessary to meet the highest tiers of digital sovereignty. This makes IONOS more suitable for workloads where strict data localization is the primary requirement and the risk from provider-level administrative access is considered lower or can be mitigated through other means.
For EU and German customers, the choice between these providers represents a strategic trade-off between **proven incumbency and advanced capability**. Selecting IONOS means choosing a mature platform with high-profile government contracts, but it requires accepting a less robust technical sovereignty posture. This may necessitate significant customer-side effort and operational overhead to build and manage missing controls, such as in-VM encryption and key management. Conversely, opting for STACKIT provides a "sovereignty-as-a-service" model with state-of-the-art controls, but it requires accepting a provider with a newer cloud offering, uneven service distribution across its regions, and contractual clauses in its DPA that demand careful navigation. The decision ultimately hinges on the customer's specific risk appetite, technical maturity, and whether their compliance needs are satisfied by data localization alone or demand verifiable operational and cryptographic control.

Section 4: 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 5: Due-Diligence Checklist

Customers evaluating IONOS or STACKIT for regulated workloads should use the following checklist to ensure a thorough assessment:

- **Contractual Verification:** Request and review the full Data Processing Agreement (DPA) and all referenced terms. For STACKIT, specifically question the conditions under which the non-EEA processing clause would be invoked. For IONOS, demand a contractual addendum specifying the jurisdictional location of all support and operations personnel.
- **Proof of Operations:** Demand evidence or attestation that support and operational procedures for a given plan (e.g., STACKIT Ultimate Support) are handled exclusively by EU-resident, EU-based personnel.
- **Metadata Residency:** Inquire about the residency of all metadata, including billing information, support tickets, monitoring logs, and control plane telemetry. Confirm this is also bound to the EU.
- **Key Custody Model:** For STACKIT's KMS, verify the technical process for BYOK and the guarantees that the provider cannot access the imported key material. For IONOS, confirm the exact scope of "customer-side encryption" for the Backup Service.
- **Audit Artifacts:** Request access to the full BSI C5 attestation reports (Type 1 for IONOS, Type 2 for STACKIT) and the accompanying system descriptions to understand the exact scope and limitations of the audit.
- **Service GA Status and Roadmap:** For STACKIT, confirm the GA status, support model, and roadmap for Confidential Computing services. For IONOS, inquire about any roadmap plans for a dedicated KMS, Confidential Computing, or an EU-only support model.
- **Incident Response & JML Controls:** Inquire about the provider's incident response procedures and their Joiners, Movers, Leavers (JML) process for privileged administrators to ensure ongoing security hygiene and control over personnel with access to sensitive systems.

Works cited

1. IONOS Cloud: No compromise cloud performance, https://cloud.ionos.com/
2. ITZBund trusts IONOS, https://cloud.ionos.de/itzbund-vertraut-ionos/en
3. Data protection and data security - IONOS Cloud, https://cloud.ionos.com/protection
4. Our data centers in the US and other locations | IONOS Cloud, https://cloud.ionos.com/data-centers
5. Data Security | Products - IONOS Cloud Documentation, https://docs.ionos.com/cloud/storage-and-backup/block-storage/overview/data-security
6. Data Security | Products - IONOS Cloud Documentation, https://docs.ionos.com/cloud/storage-and-backup/backup-service/overview/data-security
7. Key Management | Products - IONOS Cloud Documentation, https://docs.ionos.com/cloud/storage-and-backup/ionos-object-storage/concepts/key-management
8. IONOS Object Storage API for user-owned buckets (2.0.15, https://api.ionos.com/docs/s3-user-owned-buckets/v2/
9. Contract for Data Processing - IONOS Help, https://www.ionos.co.uk/help/data-protection/overview-of-the-general-data-protection-regulation-gdpr/contract-for-data-processing/
10. Accso & IONOS: Your partners for secure and customized software solutions in the cloud, https://accso.com/partner/ionos
11. International availability of IONOS products - IONOS Help, https://www.ionos.com/help/default-title/international-availability-of-ionos-products/
12. Increasing the Security of Your IONOS Account - IONOS Help, https://www.ionos.com/help/web-security/protecting-your-account/increase-the-security-of-your-11-ionos-account/
13. IT Security - Reporting security threats - IONOS, https://www.ionos.com/it-security
14. Meet STACKIT GmbH & Co. KG: A Sovereign Cloud Powering Europe | Blog, https://openinfra.org/blog/openinfra-member-stackit/
15. About STACKIT, https://www.stackit.de/en/about-us/
16. Data sovereignty with STACKIT - STACKIT Cloud, https://www.stackit.de/en/data-sovereign-cloud/
17. What is the CLOUD Act? - STACKIT, https://www.stackit.de/en/knowledge/cloud-act/
18. STACKIT Key Management Service (KMS) - STACKIT, https://www.stackit.de/en/product/stackit-key-management-service-kms/
19. STACKIT Confidential Kubernetes - STACKIT, https://www.stackit.de/en/product/stackit-confidential-kubernetes/

20. Confidential Server | Secure Data Storage | STACKIT, https://www.stackit.de/en/product/stackit-confidential-server/
21. STACKIT Ultimate Support: Always available for you, https://www.stackit.de/en/ultimate-support/
22. STACKIT Colocation - Data centers with ISO certification, https://www.stackit.de/en/colocation/
23. STACKIT regions and availability zones - STACKIT, https://www.stackit.de/en/regions/
24. Service Certificate – STACKIT Confidential Server, https://www.stackit.de/wp-content/uploads/2025/09/V1.1_Confidential-Server_EN-valid-from-12.09.2025.pdf
25. Service Certificate - STACKIT Confidential Kubernetes, https://www.stackit.de/wp-content/uploads/2025/09/V1.1_Confidential-Kubernetes_EN-valid-from-12.09.2025.pdf
26. Data Processing Agreement | STACKIT, https://www.stackit.de/wp-content/uploads/2024/11/Data-Processing-Agreement_STACKIT-Cloud_Version-2.0.pdf?x44034
27. GDPR-compliant cloud certificates - STACKIT, https://www.stackit.de/en/cloud/certificates/