PUBLICATION

Rethinking Digital Sovereignty: What SaaS, Cloud, and AI Customers Should Be Asking Providers Now

Authors: Javier Becerra, John S. Ghose
July 15, 2026

Digital sovereignty has become one of the most consequential issues in enterprise technology procurement. For years, the term was treated largely as data residency: simply a question of where servers are located. That framing is no longer adequate. Geopolitical volatility, the rapid expansion of AI infrastructure, and growing regulatory pressure across the European Union (EU) and other jurisdictions have elevated digital sovereignty into a multidimensional business risk.

Today, the question is not only where data sits, but who controls the infrastructure it runs on, who can access it and under what legal authority, whether services can continue during geopolitical disruption, and whether an organization can exit, migrate, or localize workloads without operational disruption. For businesses purchasing Software as a Service (SaaS), cloud, and artificial intelligence (AI) services, digital sovereignty is not something providers simply deliver; it is something customers must actively secure in the contract.

Digital Sovereignty Extends Beyond Data Residency

Organizations in regulated industries have long focused on data residency obligations under frameworks such as the EU's General Data Protection Regulation (GDPR), the Digital Operational Resilience Act (DORA), the Network and Information Security Directive 2 (NIS2), and sector-specific rules. Residency matters, but it addresses only one dimension of control. For example, an organization may store data within the EU, yet use a provider headquartered in the United States, which may still be subject to U.S. legal process, including under the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act, regardless of where the data is located.

A complete sovereignty assessment must address not only data residency, but also the following layers:

- **Operational control**: Who operates the infrastructure supporting the service and has authority to manage, restrict, or suspend it?
- **Administrative access**: Who within the provider can access customer systems or data, and what authority do they have to view, modify, or extract it?
- **Encryption and key management**: Who controls the encryption keys, where are they held, and can the provider access or decrypt customer data?
- **Support personnel location**: Where are engineers who access customer environments located, and are they subject to compelled-disclosure laws in those jurisdictions?
- **Subcontractor and hyperscaler dependencies**: What third-party infrastructure underlies the service, and how are those providers required to meet the same sovereignty requirements?
- **Portability and exit rights**: Can the customer retrieve its data in a usable format and migrate to another provider without significant disruption?
- **Resilience during geopolitical or regulatory disruption**: What happens to service availability if the provider's home country imposes sanctions, export controls, or other restrictions?

The EU Is Reshaping Cloud and AI Markets Around Digital Sovereignty

Regulatory pressure is accelerating the sovereignty conversation. On June 3, 2026, the European Commission published a proposal for the Cloud and AI Development Act (CADA), a flagship component of its broader Tech

Sovereignty Package. The proposal aims to strengthen EU cloud capacity and digital sovereignty, including by tripling EU data center capacity by 2030 and supporting secure cloud capacity for critical use cases.

CADA is not yet binding law and must proceed through the EU legislative process, including review and approval by the European Parliament and the Council. However, it reflects a clear policy direction aligned with the EU's broader regulatory posture under GDPR, the EU Data Act, DORA, NIS2, the Cyber Resilience Act, and the EU AI Act.

Taken together, these frameworks impose increasingly detailed requirements that map directly onto sovereignty concerns:

- GDPR and the EU Data Act govern data control and portability;
- DORA requires financial entities to manage third-party information and communication technology (ICT) risk and maintain operational continuity;
- NIS2 imposes incident reporting and supply-chain security obligations for critical sectors;
- the Cyber Resilience Act addresses security requirements for connected products; and
- the EU AI Act introduces governance obligations for high-risk AI systems.

A sovereign cloud offering that does not demonstrably satisfy these requirements offers compliance risk, not compliance relief.

The structural stakes are significant. EU cloud providers currently hold only approximately 15 percent of their own market, with three U.S. hyperscalers controlling the majority. That dependency creates not only regulatory exposure but economic and resilience risk, as non-EU providers may be subject to third-country laws that can compel access to customer data regardless of where it is stored.

The sovereignty requirement is already showing up as a mandatory criterion rather than a preference in some procurement contexts. EU public-sector bodies in France and Germany have begun requiring certified sovereign cloud solutions for sensitive workloads, and financial regulators applying DORA have signaled that reliance on non-EU hyperscalers without contractual resilience protections will face heightened supervisory scrutiny.

Providers Are Responding With Sovereign Cloud Offerings

Major providers have recognized the commercial opportunity and are adapting accordingly. Microsoft has announced a comprehensive suite of sovereignty solutions for European organizations, organized into three tiers: Sovereign Public Cloud, Sovereign Private Cloud, and National Partner Clouds in France and Germany, reflecting increasing levels of localization, customer control, and separation from global infrastructure.

Among the specific features announced are Data Guardian, which restricts remote system access to Microsoft personnel residing in Europe; External Key Management, enabling customers to maintain encryption keys on their own hardware security modules; and Microsoft 365 Local, which allows certain productivity workloads to run entirely within a customer's own data center.

Google positions its "Sovereign Controls for Google Workspace" as enabling customer-managed encryption and access transparency; Oracle promotes its "EU Sovereign Cloud" as physically and logically separate from its global infrastructure; and TCS offers a managed sovereign cloud model targeting regulated European enterprises. These offerings vary considerably in scope, technical architecture, operational model, and the specific regulatory certifications they claim to support.

Independent industry analysis has raised questions about whether some sovereign cloud commitments represent genuine operational transformation or instead reflect "sovereignty-washing," layering localized controls onto existing hyperscale infrastructure without fully addressing underlying jurisdictional and control risks. The distinction matters because not all sovereignty commitments are equal: those that can be modified unilaterally by the provider, or that rely primarily on contractual assurances, offer materially weaker protection than those supported by enforceable and auditable technical controls.

Contract Issues Customers Should Revisit

Sovereign cloud is ultimately a contract issue. Vendor commitments made in press releases, blog posts, or sales materials do not create enforceable obligations. Customers should review their current and upcoming SaaS, cloud, and AI agreements with the following issues in mind:

- **Data location and transfer restrictions**: Are the jurisdictions in which data will be stored and processed identified specifically in the contract, and are cross-border transfers restricted by an identified mechanism?
- **Government access request procedures**: What does the provider commit to do if it receives a governmental demand to access customer data, including whether the customer is notified and whether the provider is obligated to challenge overbroad requests?
- **Audit and reporting rights**: Does the customer have the right to audit the provider's sovereignty controls or receive third-party audit reports on a regular basis?
- **Encryption and customer-managed keys**: Does the customer retain control of encryption keys, or can the provider decrypt customer data without customer authorization?
- **Subcontractor approval and transparency**: Does the contract identify subcontractors and hyperscale infrastructure dependencies, and does the customer have approval rights over material changes?
- **Disaster recovery and business continuity**: What commitments does the provider make regarding service availability during geopolitical disruption, regulatory action, or infrastructure failure?
- **Service suspension rights**: Under what circumstances can the provider suspend service, and what notice is required?
- **Exit assistance and data portability**: Is the customer guaranteed the right to retrieve data in a usable format at termination, with migration assistance and transition periods specified?
- **AI model and data use restrictions**: Does the contract prohibit use of customer data to train or improve the provider's models, and are AI-generated outputs subject to any sovereignty or localization controls?
- **Flow-down obligations for regulated customers**: Do the provider's sovereignty commitments flow through to subcontractors, with provisions addressing the customer's obligations under applicable frameworks?

Practical Takeaways

Customers should approach sovereign cloud claims with rigor rather than accepting them at face value. The key discipline is converting vendor representations into contract commitments that are specific, auditable, and enforceable. Providers should be able to describe their sovereignty controls in technical and operational terms, identify the jurisdictions in which personnel with system access are located, and agree to contractual provisions reflecting those representations. For regulated organizations, this evaluation must be tied directly to compliance requirements, including the ability to demonstrate adherence under frameworks such as GDPR, DORA, and NIS2, particularly as sovereignty expectations are increasingly incorporated into public procurement criteria.

Because these issues sit at the intersection of complex and evolving regulatory frameworks, technical architecture, and contract drafting, engaging experienced privacy attorneys early is critical to translating

sovereignty representations into enforceable terms and avoiding costly gaps. Our Data Privacy and Cybersecurity Team can help assess provider commitments, benchmark them against applicable regulatory obligations, and negotiate contract language that secures the sovereignty protections your organization needs. Organizations that have not recently reviewed their SaaS, cloud, and AI agreements should consider doing so now, before new commitments are made and before the regulatory framework hardens.

If you have questions about digital sovereignty requirements in your SaaS, cloud, or AI arrangements, or how to protect against unauthorized data access, please reach out to Javier Becerra, John S. Ghose, or any member of our Data Privacy and Cybersecurity Team.