



Autonomous Enterprise | SAP Sovereign Cloud

Digital Sovereignty in the Cloud Era

Securing innovation without compromise

Table of contents

3	The rise of digital sovereignty
4	Why digital sovereignty matters
5	The four pillars of digital sovereignty
7	SAP's approach to digital sovereignty
9	Sovereign AI: innovation without compromise
10	Why SAP?
11	Migrating with confidence
12	Next steps

The rise of digital sovereignty

Control, resilience, and continuity are now strategic concerns for organizations everywhere

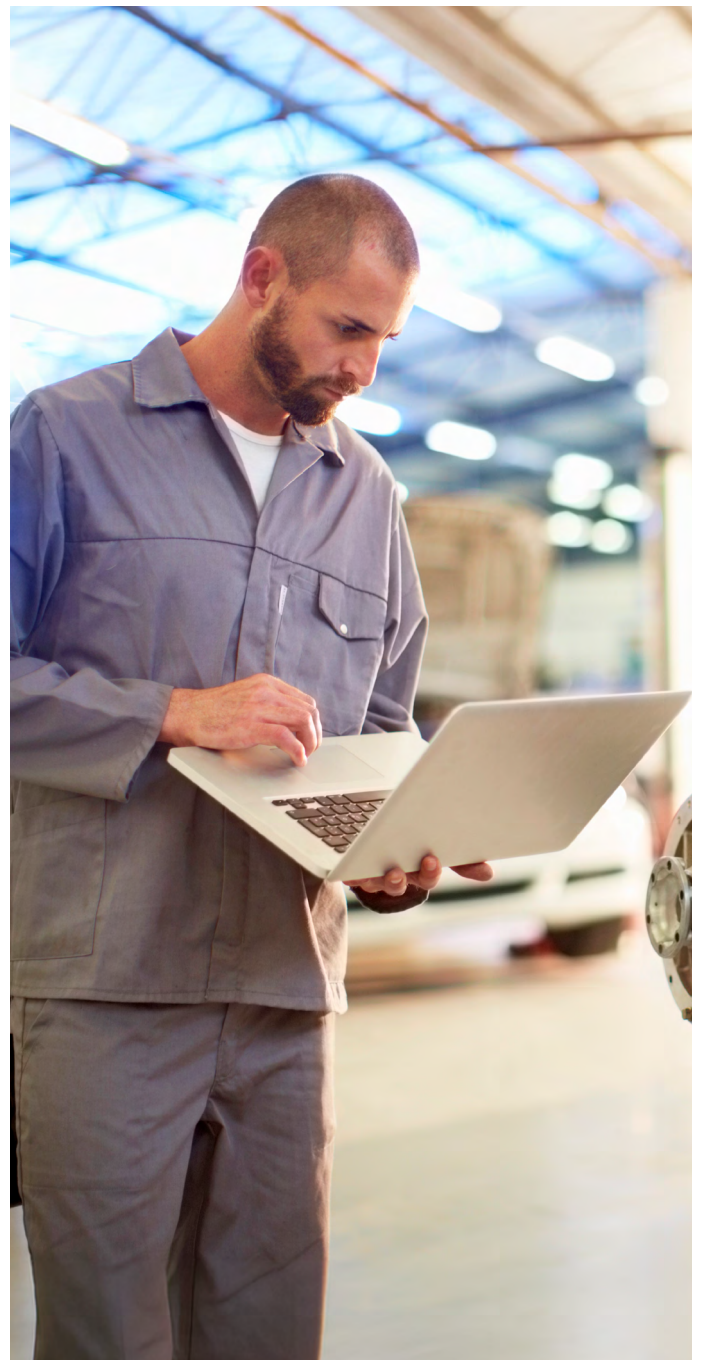
Digital sovereignty is now a top-level strategic priority. Leaders across industries and public-sector organizations are rethinking their cloud strategies, asking how to protect sensitive data, maintain operations during disruption, and stay resilient amid geopolitical uncertainty. These aren't temporary concerns. They reflect a fundamental shift toward cloud models that prioritize control, continuity, and trust.

Why regulatory demands are raising the bar for cloud

The digital economy is at an inflection point. Organizations worldwide face rising regulatory pressure, escalating cyberthreats, and growing geopolitical uncertainty. While the cloud has accelerated innovation, its global scale and shared infrastructure have also introduced new risks, particularly where sensitive data is involved.

Digital sovereignty has emerged as the strategic response—not as a move toward isolation, but as a way to ensure that sensitive data and mission-critical operations remain under the right legal and governance frameworks. The goal is trusted conditions for innovation, not independence from global connectivity.

This paper introduces a practical framework for digital sovereignty built on four pillars—data, operational, technical, and legal sovereignty. It also outlines what sovereign cloud truly requires, along with SAP's approach, including deployment options, sovereign AI, and migration.



Why digital sovereignty matters

The forces that make sovereignty a strategic imperative

Four converging forces are driving digital sovereignty to the top of the enterprise agenda:

A more complex regulatory landscape

The regulatory landscape is growing more complex. Across more than 137 countries, governments have [enacted](#) data protection and sovereignty laws. Some of these include:

- General Data Protection Regulation (GDPR) for the European Union
- Network and Information Security Directive (NIS2) for the European Union
- Security of Critical Infrastructure (SoCI) in Australia
- Data localization requirements in Canada

Organizations that embed sovereignty into their cloud architectures are better positioned to meet these requirements proactively and adapt as landscapes continue to evolve.

Geopolitical fragmentation

Extraterritorial laws such as the U.S. CLOUD Act and the Foreign Intelligence Surveillance Act (FISA) raise legitimate concerns for organizations operating on infrastructure subject to foreign jurisdiction. For defense, critical infrastructure, and public-sector organizations, the drive for sovereignty often goes beyond current legal requirements to focus on building resilience and strategic autonomy for whatever the future may bring.

Cybersecurity and resilience

Ransomware and state-sponsored threats require resilient cloud environments designed to withstand disruption.

Trust and public accountability

Governments, customers, and partners expect data to remain protected and local. Demonstrable sovereign data practices strengthen trust and competitive positioning.



The four pillars of digital sovereignty

A coordinated framework spanning data, operational, technical, and legal dimensions

Digital sovereignty is multidimensional. It can't be achieved by addressing data residency alone. It requires a coordinated approach across four pillars, each reinforcing the others.



Data sovereignty

Your organization retains authority over how data is classified, accessed, and processed, not just where it resides. Local laws and policies govern its full lifecycle, with automated controls that prevent unauthorized cross-border transfers.



Technical sovereignty

True technical control means being able to verify exactly how your environment operates, not simply trust that it does. That requires physical data center security, robust tenant isolation, strong encryption, and governed control-plane operations that your organization can independently audit.



Operational sovereignty

Operational sovereignty defines the boundaries of trust around your cloud environment—who can administer it, who can access it, and under what circumstances. Incident response, maintenance, and escalation stay within approved jurisdictions, handled only by local nationals or personnel from trusted countries with the required security clearance.



Legal sovereignty

Legal sovereignty grounds your digital operations in local law. Clear jurisdictional structures, transparent organizational ownership, and enforceable contractual safeguards work together to mitigate foreign access obligations, ensuring the rules that govern your data carry real legal force in the jurisdictions that matter.



Cutting through the confusion

So, what does digital sovereignty actually mean? Simply put, it's the ability to exercise autonomous control over your digital operations—your data, infrastructure, organizational processes, and the legal and technical frameworks governing them. It isn't a binary state but a spectrum organizations can adopt based on their risk appetite, regulatory environment, and strategic objectives.

Digital sovereignty vs. data sovereignty

Data sovereignty—the principle that data is subject to the laws of the country where it's collected or stored—is a critical foundation. But SAP's definition goes further, encompassing legal jurisdiction, operational independence, and technical control. A comprehensive approach spans all four pillars: data, operational, technical, and legal sovereignty.

Sovereignty and the Autonomous Enterprise

As organizations modernize their sovereign strategy, AI can move beyond supporting individual tasks to helping coordinate and optimize processes. Embedded assistants and agents operate within established business contexts, governance frameworks, and operational workflows, helping organizations progress toward an Autonomous Enterprise where people and AI work together to maintain sovereignty and improve outcomes.



SAP's approach to digital sovereignty

Flexibility across the sovereign spectrum without sacrificing innovation

Sovereign cloud isn't a checkbox. It's an architecture, a governance model, and an operational discipline. While a credible sovereign cloud offering must address the four dimensions of sovereignty (data, operational, technical, and legal), translating sovereignty principles into cloud architecture means asking questions like these:

- Where does data reside, and under which legal framework is it processed?
- Who administers the environment, and are those personnel cleared and locally based?
- How is tenant isolation enforced, and can governance and auditability be independently verified?
- How does the legal structure of the cloud provider itself, its ownership, jurisdiction, and contractual commitments, protect against foreign access obligations?

Organizations that address only one or two of these questions expose themselves to gaps across the others.

Not every organization requires the same level of sovereignty. Requirements vary by industry, regulatory environment, risk appetite, and technological context. Some organizations must meet strict security requirements across every layer of their cloud environment. Others need to demonstrate regulatory compliance in specific areas while preserving the flexibility to innovate.



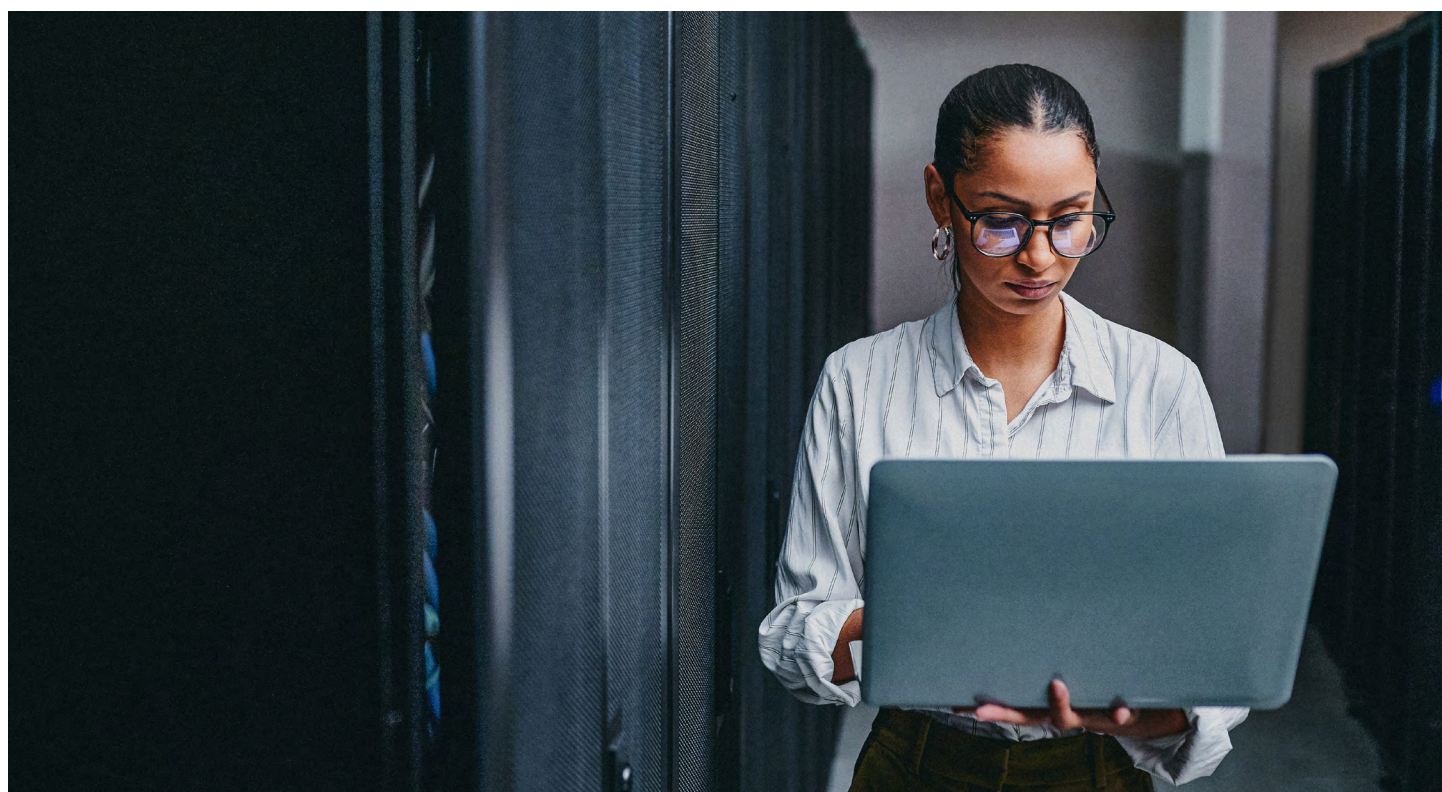
Multiple sovereign deployment models

SAP Sovereign Cloud is designed to meet organizations where their requirements fall on this spectrum. Built on the principle that sovereignty and innovation should reinforce one another, SAP delivers different deployment models for our hardened portfolio, each providing verifiable sovereignty across the full stack from IaaS, PaaS, to SaaS:

- **Hyperscaler-based sovereign regions.** SAP partners with premium hyperscalers, including AWS, Microsoft Azure, and Google Cloud, to deliver jurisdictional data residency, local operations, and regulatory compliance, combining scalability with sovereign controls.
- **SAP Cloud Infrastructure.** SAP's own platform provides EU customers with scalable infrastructure-as-a-service built on open-source technologies. Data remains within the EU under national and EU law, with no hyperscaler involvement.
- **SAP Sovereign Cloud On-Site.** For organizations requiring maximum assurance, SAP operates cloud infrastructure within customer-owned or customer-selected data centers, maintaining SAP cloud innovation while placing data and control planes behind the customer's firewall.

Portfolio-wide sovereignty

SAP Sovereign Cloud spans the SAP application portfolio—including SAP Cloud ERP, HCM, supply chain management, and more—so organizations on the path to becoming an Autonomous Enterprise can pursue end-to-end transformation within sovereign guardrails.



Sovereign AI: innovation without compromise

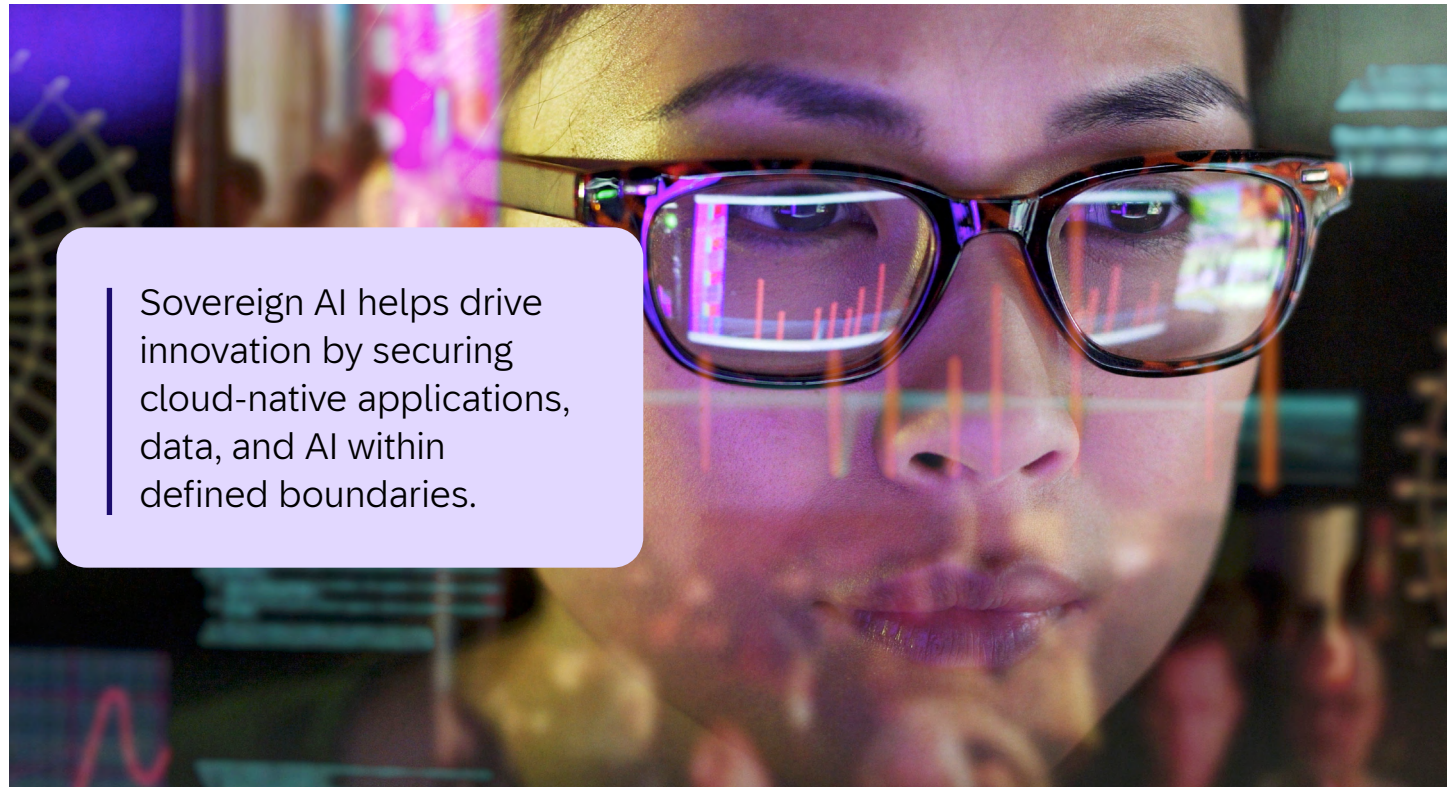
Deploying artificial intelligence within sovereign guardrails

One of the most common concerns about sovereign cloud is whether it limits access to artificial intelligence. But AI innovation and sovereignty are interdependent. Organizations that address both are better positioned to deploy AI responsibly, maintain compliance, and build trust with customers and regulators.

SAP's sovereign AI initiatives

SAP continues to invest in AI capabilities that operate within the same compliance guardrails as its sovereign cloud environments. SAP's ambition is to deliver full sovereignty across AI offerings, powered by locally deployed LLMs, according to your rules, along with other key initiatives, including:

- **EU AI Cloud and sovereign AI partnerships:** SAP supports applied AI with sovereign capabilities through the EU AI Cloud, in partnership with Cohere and Mistral AI, delivering EU AI Act-compliant large language model capabilities and AI workflows within EU data centers.
- **Industrial AI Cloud:** Advanced AI models run on SAP's secure cloud platform with NVIDIA GPU acceleration, deployed in T-Systems' data center. Industrial AI Cloud offers enterprise-grade scalability and security, and full governance and auditability in compliance with data protection standards.
- **Sovereign OpenAI for Germany:** In partnership with OpenAI, SAP is developing AI solutions built in Germany to meet the country's sovereignty, security, and legal requirements.



Sovereign AI helps drive innovation by securing cloud-native applications, data, and AI within defined boundaries.

Why SAP?

Beyond compliance: sovereignty as a source of competitive advantage

Digital sovereignty is often framed as a defensive measure—a response to risk, regulation, and geopolitical pressure. But Gartner predicts that more than 75% of all enterprises will have a digital sovereignty strategy by 2030, signaling that it has moved from a niche concern to a strategic imperative. For organizations that adopt a comprehensive strategy, digital sovereignty is about more than compliance. It's about building a source of resilience, innovation, and trust.

- **Compliance with confidence:**

Sovereignty embedded into cloud architecture means meeting regulatory requirements proactively. As new legislation emerges, systems are already positioned, reducing the cost of compliance retrofits.

- **Resilience by design:**

Sovereign cloud environments are engineered with operational continuity as a design principle, giving organizations greater autonomy over infrastructure, personnel, and data when external conditions shift.

- **Innovation without compromise:**

Access to cloud-native applications, data platforms, and AI within sovereign guardrails means organizations no longer need to choose between modernization and compliance.

- **Trust at scale:**

For governments, sovereign cloud underpins citizen trust and democratic accountability. For enterprises, it builds confidence with customers, regulators, and partners.

- **Long-term agility:**

Addressing sovereignty now avoids the technical debt and vendor lock-in that come from deferring the decision.

Sector-specific impact

- **Public sector:** Supports national security, data protection, and citizen trust by ensuring that public records, personal data, and government systems remain within national jurisdiction, while enabling digital modernization.
- **Critical infrastructure (utilities, telecoms, energy):** Safeguards the systems societies depend on, with operational resilience built in.
- **Regulated industries (banking, healthcare, insurance):** Protects sensitive data while accelerating competitive digital transformation.
- **Defense and security:** Delivers maximum assurance for classified and mission-critical workloads through the on-site deployment model.

Migrating with confidence

A proven path from on-premises to sovereign cloud

For public-sector and regulated organizations, the move to sovereign cloud often begins on-premises. Concerns about disruption, sovereignty, cost, and risk are valid—but SAP addresses them with a proven, flexible methodology.

A structured approach: RISE with SAP*

RISE with SAP provides a standardized framework built on best practices from thousands of customer transformations, with clear milestones and built-in sovereignty controls. Key components include:

- **Proven methodology:** A standardized path through discovery, planning, migration, and optimization, adapted for sovereign requirements.
- **Expert guidance:** SAP onboarding advisors and enterprise architects who understand sovereign compliance and operational requirements.
- **Agent-led toolchain:** Streamlined collaboration, efficient project execution, and continuous innovation support.
- **Sovereign cloud operations:** Built-in security, automated monitoring, and issue resolution, tailored to meet sovereign compliance standards.
- **Investment protection:** Transformation incentives, flexible licensing, and predictable pricing.

Governance-first planning

Start by clarifying sovereignty requirements across all four pillars before selecting a deployment model—ensuring technical decisions are grounded in legal and compliance reality from the outset.

Deployment flexibility

SAP's deployment options—sovereignty hyperscaler-based, SAP Cloud Infrastructure, and SAP Sovereign Cloud On-Site—allow organizations to start where they are and evolve as requirements mature.

*The RISE with SAP journey may be limited based on your region and choice of SAP Sovereign Cloud deployment.



Next steps

Your sovereignty journey starts here

Digital sovereignty is no longer a question of if, but how. Those that act now gain first-mover advantage; those that delay will face rising regulatory pressure and growing technical debt.

SAP provides the foundation for a sovereignty strategy that doesn't force a choice between control and innovation—with deployment options spanning the sovereign spectrum, a proven migration methodology, and sovereign AI built into the platform.



Start your sovereignty journey

Discover [SAP Sovereign Cloud](#) and watch the [explainer video](#) to learn more.