



White paper | SAP Sovereign Cloud

# Sovereignty and innovation

## Insights from a webinar on sovereign cloud technology

# Table of contents

- 3    Sovereignty, redefined**
- 4    A framework for thinking clearly**
- 5    The tension resolves**
- 6    What sovereign cloud  
     really requires**

## Sovereignty, redefined

### Why stepping back from the cloud is the wrong response to regulatory pressure

Across boardrooms and policy circles in Europe and beyond, digital sovereignty is often understood as a tradeoff: that cloud innovation and regulatory control cannot coexist. That view is understandable—but mistaken. This paper distills insights from a recent webinar exploring how sovereign cloud technology challenges that assumption.

#### The infrastructure myth

For many organizations, digital sovereignty still means local infrastructure: building data centers and keeping servers on home soil. On the surface, this makes sense. But when sovereignty is pursued through infrastructure ownership, organizations often end up with aging technology and reduced access to the continuous innovation cloud environments provide. They trade real capability for an illusion of control.

As Heiko Mauersberg, SAP's business lead for Sovereign Cloud in Europe, noted during the webinar, local investment alone does not ensure sovereignty—and can slow innovation. True digital sovereignty is not about owning the server room, but about strategic control over data, operations, technology choices, and compliance.



# A framework for thinking clearly

## Separate perceived risks from real requirements—and make better cloud decisions

The problem with “digital sovereignty” as a term is that it is too broad to act on. Organizations need a way to understand what they are actually trying to protect—and this requires breaking the concept into its component parts.

SAP defines digital sovereignty according to four core dimensions: Data, Operational, Technical, and Legal. Not every organization will weigh these equally. A government ministry and a defense contractor may share the same broad sovereignty goal while having very different priorities within it. The value of the framework is not that it produces the same answer every time—it’s that it gives decision-makers the right questions to ask.

### Data sovereignty

The first question is where your data lives—and who can touch it. Compliant residency in an approved geography is the baseline; beyond that, handling must meet the elevated standards of critical infrastructure and regulated industries, and controls must exist to prevent unauthorized transfer across national or system boundaries.

### Operational sovereignty

The second question is who runs the environment. Personnel must be located in approved geographies, hold appropriate security clearances, and be dedicated exclusively to sovereign operations. Anyone who works with these environments works only with these environments.

### Technical sovereignty

The third question is how the environment is governed and how it changes over time. Hardware is managed separately, with distinct access controls. Critically, innovation does not flow freely into sovereign environments—it passes through a controlled clearing process, a dedicated control plane that validates what enters before customers can access it.

### Legal sovereignty

The fourth question is which laws apply. The entity delivering services in a given market is subject to that market’s legal framework. Personnel are citizens or residents of the relevant countries or regions. The goal is to ensure that what you build in a sovereign environment cannot be reached or disrupted by the legal reach of another jurisdiction.

Four dimensions, each distinct, each actionable. Together, they replace a vague aspiration with a structured basis for decision-making.

## The tension resolves

### Bring control, compliance, and innovation into lasting alignment

Once sovereignty is understood in these terms—strategic control rather than hardware geography—a second misconception becomes easier to address: the fear that operating in a sovereign environment means accepting innovation on a slower timeline than everyone else.

SAP Sovereign Cloud covers the entire suite of SAP solutions: ERP, analytics, line-of-business solutions, SAP Business Technology Platform, and embedded AI services. This is not a reduced offering for organizations that have traded capability for compliance. It's a complete solution, operated under sovereign conditions.

On the question of how quickly new capabilities reach sovereign customers, Mauersberg was direct: “We’re not talking about months, we’re talking about days and weeks to make sure that it’s almost synchronous that customers have this innovation available inside a sovereign environment when we ship it to the general market.”

The clearing house model does introduce a stage between general availability and sovereign availability. But that stage is engineered to be short. The practical difference, for most customers, is negligible.

The same logic extends to AI. Generative and agentic AI is reshaping how work gets done—and regulated organizations watching this shift might reasonably wonder whether sovereignty puts it out of reach. It doesn't. Business AI is embedded across SAP's suite of solutions and available in sovereign environments. The Business Technology Platform connects data from SAP applications and external sources, providing the contextual layer that makes AI useful across an entire business rather than isolated to individual functions. And through global partnerships with Mistral, Cohere, and OpenAI, SAP extends AI capability beyond its own applications—including through the European AI Cloud Initiative, which brings language model access within European borders for customers whose sovereignty requirements extend to the AI layer itself.

Organizations in sovereign environments do not face a choice between compliance and capability. They face a question of deployment model—and here too, genuine choice exists. SAP Sovereign Cloud is available through leading hyperscalers, including Delos Cloud in Germany, as well as through SAP Cloud Infrastructure. For those whose requirements go further still, SAP Sovereign Cloud On-Site brings the full sovereign stack into a customer's selected or owned data center.

# What sovereign cloud really requires

## The essential capabilities and controls

The framing that has done most damage to the sovereignty conversation is the one that treats it as a compromise—something you accept in exchange for control, at the cost of agility.

Judith Schade closed the webinar with a different framing, and it is the right one: “Sovereignty, as we look at it at SAP, is about responsible governance. And we truly think that organizations will succeed that treat sovereign cloud not as a constraint but as a strategic enabler.”

Responsible governance is not a limitation on ambition. For organizations operating in the public sector, regulated industries, and critical infrastructure, it is the precondition for sustained ambition—the basis on which everything else can be built with confidence.

The organizations that get this right will not be the ones that built the most elaborate local infrastructure, but the ones that understood what digital sovereignty actually requires, chose their deployment model accordingly, and used it as a foundation rather than treating it as a ceiling.



### Watch the webinar

See the full conversation with Judith Schade and Heiko Mauersberg on demand.

[View now](#)



### Explore SAP Sovereign Cloud

Dive into deployment options and sovereign cloud capabilities available in your region.

[Learn more](#)