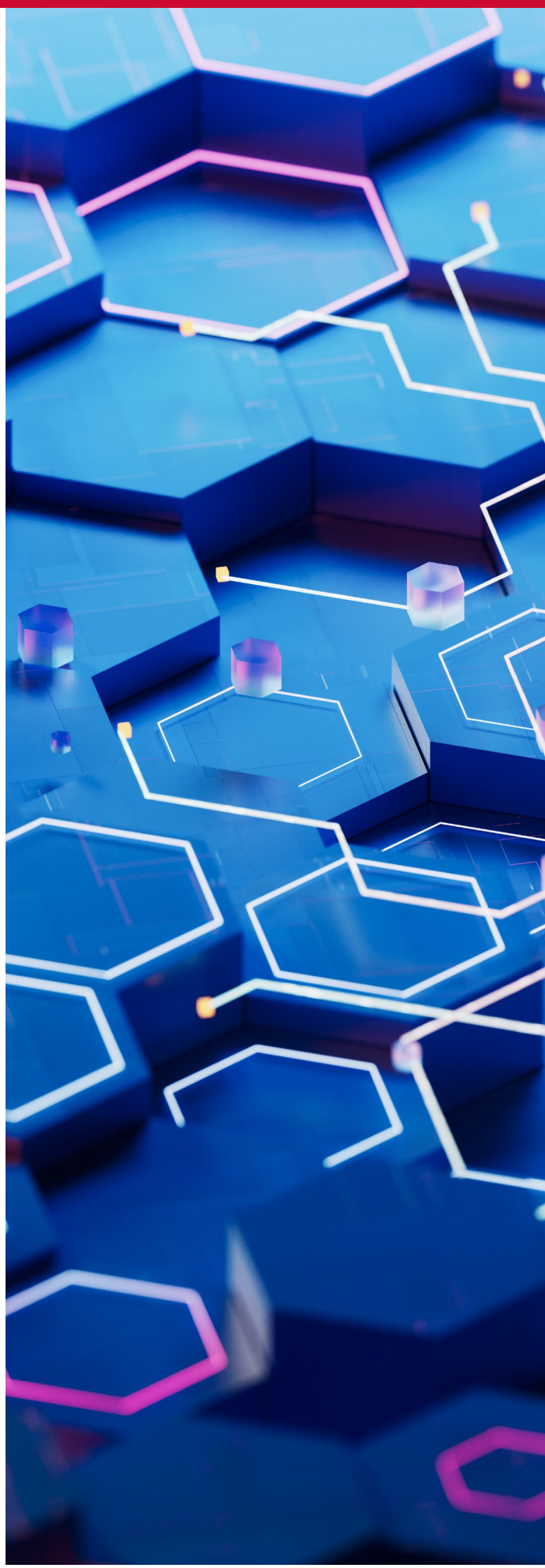
BROADCOM | Queen Mary University of London

Sovereign Cloud for Europe

EXECUTIVE SUMMARY



Global spending on sovereign cloud solutions is projected to reach nearly USD $260 bn by 2027. This is driven primarily by European concerns over data privacy and government access. But what is sovereign cloud? How does it relate to foreign government access? And why should European organisations care about this now, in 2025?

In this report, commissioned by Broadcom, Johan David Michels analyses sovereign cloud, based on research conducted for the Cloud Legal Project at the Centre for Commercial Law Studies, Queen Mary University of London, and a series of expert interviews. The report looks at what sovereign cloud means and what drives demand for sovereign services. It explains how the market for sovereign cloud is hampered by mixed messages and legal uncertainty – calling for industry to come together voluntarily to establish clear standards for both cloud providers and customers as part of a new Sovereign Cloud Code of Conduct.

The definition of sovereign cloud

Based on a series of interviews, the report unpacks how sovereign cloud means different things to different people. Different providers use the term to promote different types of services. For clarity, the report considers sovereignty from different perspectives:

FOR CUSTOMERS

For customers, sovereign cloud addresses the evolving concerns of enterprises about public cloud services. As organisations move beyond initial enthusiasm for cost and scalability, they have become concerned about data control, security, and autonomy. The concept of sovereign cloud focuses on **giving customers greater control** over their cloud resources, including data residency, access limitations, increased transparency, and reduced vendor lock-in.

Sovereign cloud also entails a high level of protection from foreign government access. In this respect, the report points out that data localisation alone can be insufficient, if the cloud provider is subject to a foreign jurisdiction. For example, the US government can order a US cloud provider to disclose European customer data, even if the data are stored in Europe by a European subsidiary.

FOR EUROPEAN POLICYMAKERS

For European policymakers, sovereign cloud represents a strategic initiative to **reduce dependence on US technology** services and enhance Europe's digital autonomy. This also forms part of the European Commission's industrial policy, which aims to develop a robust European cloud ecosystem that supports local businesses and protects European data.

FOR CLOUD PROVIDERS

European cloud providers view sovereignty as a **service differentiator**, while US hyperscalers market their own 'sovereign' services, which feature data residency and encryption. However, according to the report, the latter approach has limitations. The metadata may still be transferred across borders, encryption doesn't protect all data use cases, and providers may still need access to data in the clear for advanced functionality.

At the same time, US companies can also work together with European providers to create sovereign cloud solutions. For example, Broadcom supplies VMware software to European cloud providers, who then focus on secure and isolated deployment, delivery, and customer management. Such arrangements advance customer choice and benefit European customers by providing access to US software (which is often industry-standard and cutting-edge), while protecting data from foreign government access.

The key drivers for sovereign cloud

The report concludes that European customers are primarily driven to adopt sovereign cloud solutions by **regulatory requirements** and **security concerns**. At the EU level, there are questions about whether US cloud providers can adequately protect European personal data under the GDPR. When US cloud providers share European personal data with US authorities, they typically do so without customer instructions or a legal basis in EU law, often being legally barred from notifying customers - actions that appear to conflict with GDPR requirements. Further, individual member states like France also impose additional requirements, such as the SecNumCloud certification which mandates cloud providers be free from foreign control.

Beyond regulatory compliance, many organisations have strategic reasons for wanting to shield their data from foreign government access. These range from intelligence and defence agencies protecting national security information, to universities conducting sensitive research in fields like AI and encryption, to companies seeking to protect valuable trade secrets from foreign access.

THE CHALLENGES INVOLVED

An organisation that wants to adopt sovereign cloud as part of a hybrid or multi-cloud solution can face three main challenges:

1. Organisations must first assess their workloads and **classify their data** based on sensitivity levels, determining which information requires enhanced protection either due to GDPR requirements or for business confidentiality reasons.

2. Secondly, they need to select the most suitable IT services, potentially using multiple providers, but face challenges when different providers' services don't work well together because of a **lack of interoperability**, which can result in siloed rather than integrated workload deployments.

3. Lastly, organisations must consider data and application **portability**, as the inability to easily move workloads between cloud providers can limit their flexibility to switch services and take advantage of better offerings elsewhere.

To reduce legal uncertainty, Michels proposes the development of an industry-driven **Sovereign Cloud Code of Conduct**. This approach would establish clear legal standards for protecting data from foreign government access under GDPR, allowing cloud providers to demonstrate compliance and giving customers confidence in compliant sovereign cloud services. It would recognise different approaches to reducing foreign access risk. Michels acknowledges that developing the Code would require a complex process of industry collaboration, consultation, and regulatory approval, but the end result would provide legal certainty for both providers and customers while ensuring protection of European data rights.