codesphere

Sovereignty in practice: How the UK can create secure public services

The UK's approach to sovereignty

Digital sovereignty has become a major driver of technology policy in the UK over the past 18 months. This reflects the confluence of a number of trends: a longstanding priority to diversify technology suppliers to government, especially in cloud; turbulent geopolitics underlining the importance of a "sovereign edge" and the risks of over dependence on a single supplier, and; a desire to ensure that public funds spent via public procurement provide wider benefits to the UK's economy and society, including by supporting UK scale ups.

The Government is now introducing a more strategic approach to how government buys and builds technology. The steps it has taken include a recognition by the Cabinet Office that AI procurement is a matter of national security, investment in domestic AI capabilities via SovAI and the development of the NCIP programme.

This approach is both ambitious and pragmatic in that the government has recognised that legacy architecture cannot be unwound overnight. Existing workloads built on proprietary infrastructure represent sunk investment, and wholesale replacement is neither realistic nor necessary. However, rethinking tech procurement represents an opportunity to learn from past experience, restore negotiating leverage, and deliver real choice and competition, enabling the UK to access the best technology on its own terms.

The problem

Vendor lock-in

Investment in cloud services is integral to the delivery of a modern, digital state, with procurement through the G-Cloud framework averaging c. £4 billion per year since 2021 and the Government set to commit a further £40 billion with the forthcoming NCIP programme. However, procurement processes have historically favoured a small group of US providers to deliver essential public services. This has, by the government's own admission,[1] contributed to poor value for money for the taxpayer and, at times, a total absence of competition, with some recent major cloud procurements having attracted a single bidder.[2]

The central risk of modern cloud adoption lies in the structural bonds created by architecture, business models, and software integration. The more heavily an organisation relies on proprietary platform services provided by hyperscalers – databases, identity management, serverless function calls, observability tools – the higher the technical, organisational, and economic barriers to switching provider. Migration no longer just means moving data, but often a complete redevelopment of applications, the cost of which is often prohibitive.

[1] https://committees.parliament.uk/oralevidence/16745/pdf/
[2] https://www.publictechnology.net/2026/03/24/business-and-industry/hmrc-greenlights-sole-bidder-aws-for-500m-cloud-migration-deal/

Implications

An increasingly uncertain geopolitical context has sharpened these concerns, meaning vendor lock-in is no longer solely a competition and value-for-money issue.

The most immediate risk is operational. In June, the US Commerce Department forced the abrupt suspension of access to Anthropic's most advanced AI models for all foreign nationals, demonstrating the vulnerability to over reliance on AI cloud services provided from outside of Europe.

The US CLOUD Act adds a further layer of exposure. Under the Act, American authorities can compel US companies to hand over data held anywhere in the world, including on servers physically located in the UK. The legal exposure follows the company, not the server, and no contractual arrangement between a UK public body and a US provider can override a lawful US court order.

The solution

The structural nature of vendor lock-in – rooted in proprietary platform services, data architecture, and the software integration choices made at the point of procurement – necessitates a technical model that allows government systems to operate on commercial cloud infrastructure without becoming architecturally bound to any single provider.

One such model is the Virtual Cloud Provider (VCP) approach. The core principle is that an application's entire architecture – compute resources, databases, network rules, deployment logic – is defined in a single portable configuration file rather than through the proprietary service layer of a specific cloud provider. This means the application can be moved to different infrastructure without rewriting code, and without changing the developer environment. This resolves one of the most significant practical barriers to migration – the reluctance of development teams to retrain on a new platform.

In concrete terms, this approach enables:

- **Infrastructure flexibility**: The same software environment can run on AWS, Microsoft Azure, Google Cloud, or sovereign bare-metal servers in a government data centre. Engineers use the same platform interface regardless of what sits underneath.
- **Air-gapped operation**: For the most sensitive workloads, systems can operate with no internet connection and no external dependencies, with data remaining entirely within the organisation's own network.
- **Negotiating leverage**: Where exit from a cloud provider is technically straightforward, the government is no longer structurally compelled to accept the pricing and terms of an incumbent. Budget overruns in cloud procurement typically arise not from compute costs but from egress fees and proprietary services for which there is no viable alternative once lock-in has set in. A portable architecture restores the conditions under which competition can function.

- **Capital efficiency**: Where digital transformation investment is tied to proprietary platform logic, changing supplier tends to duplicate the initial capital cost. A standardised, portable technical environment eliminates procurement decisions being guided by sunk cost fallacy.

The model also enables safer development practice. Each proposed code change can be tested in an isolated, production-identical environment before deployment, reducing the risk of a failed update affecting live citizen-facing services, a meaningful risk in public sector contexts where service disruption carries political and operational consequences.

None of this requires the government to abandon US infrastructure wholesale, nor does it depend on the existence of a British alternative of equivalent scale. It addresses the sovereignty problem not by replacing incumbent providers but by changing the structural relationship with them, ensuring that the architecture of government systems does not confer leverage on any external party.

Case study – GovTech Deutschland: sovereign infrastructure at national scale

In 2025, Codesphere signed a framework agreement worth €30.8 million with GovTech Deutschland, the technology procurement body of the German federal government, to provide the central infrastructure component of the Deutschlandplattform, Germany's national digital platform for public sector modernisation.

The challenge: Federal and state governments across Germany manage large portfolios of legacy applications built for proprietary, often US-hosted infrastructure. Migrating to a sovereign stack required a platform capable of hosting complex, heterogeneous workloads without requiring each ministry to rebuild its applications, while also providing a shared environment through which new digital services could be procured, deployed, and operated to common standards across all levels of government.

The solution: Codesphere delivers the PaaS layer for the platform, a standardised, modular runtime environment sitting above and across multiple underlying infrastructure providers. Its Landscape architecture ensures that legacy application definitions are ported to the sovereign stack without redevelopment: the code does not change, only the underlying infrastructure on which it runs. The platform is infrastructure-agnostic, capable of running on hyperscalers, local cloud providers, or bare metal, and can reduce workloads to generate up to 90% cost savings. Entities that need to retain some on-premise infrastructure for security reasons can do so while still accessing the full platform, preserving flexibility without sacrificing participation.

The result: Complex legacy applications can be migrated without refactoring, reducing timelines from years to months. But the platform's significance extends beyond migration. By providing a single shared environment accessible to federal government, states, and municipalities, it gives central government real-time oversight of usage and needs across public bodies, enabling unified national commissioning and materially greater commercial leverage over cloud providers. For smaller software vendors, it provides a single point of entry to a national public sector market; once an application is built and deployed, it can run across the entire platform without rebuilding, dramatically lowering the barriers to competing at scale.

UK parallel: NCIP presents an equivalent opportunity. Both the AI Opportunities Action Plan and the Blueprint for Modern Digital Government recognise that fragmented infrastructure prevents the UK from realising the benefits of AI, which a centralised platform directly addresses. Structured on similar principles to Deutschlandplattform, NCIP could give the UK government materially greater leverage with cloud providers, reduce the structural barriers that prevent British startups and scaleups from competing on equal terms with large incumbents, and eliminate the duplicated procurement costs that fragmentation across hundreds of separate public bodies currently generates.

Case study – MEDI:CUS: Sovereign health data infrastructure for Baden-Württemberg

MEDI:CUS is a state-funded health platform for Baden-Württemberg, supported by **25.6 million euros** in public funding, that gives 17 clinical institutions access to specialised health applications through a shared, secure infrastructure.

The challenge: Health data carries the highest regulatory sensitivity in European law. The platform needed to support a diverse set of clinical applications – through an "app store" model for different hospital systems – on infrastructure that demonstrably remains under German sovereign control.

The solution: Codesphere was selected as the central infrastructure component, providing the runtime environment for deploying and managing clinical applications. Because application definitions are portable through the *Landscape* model, clinical institutions are not tied to a specific hyperscaler: the platform can be moved to other underlying infrastructure without the need to rebuild applications. The built-in air-gapped mode means that sensitive patient data never leaves the facility's network.

The result: MEDI:CUS provides 17 institutions with access to a shared, sovereign runtime platform through an app store model. When policies, regulations, or contract conditions change, the underlying infrastructure can be swapped without the need to redevelop clinical applications.

UK parallel: The government's £10 billion investment in NHS digitisation, centred on the creation of a Single Patient Record, will embed digital infrastructure at the core of clinical operations across England. The procurement decisions made now will determine whether the NHS emerges from that programme with full control over patient data. MEDI:CUS demonstrates that shared, sovereign health data infrastructure is achievable at scale.

About Codesphere

Codesphere is a German Virtual Cloud Provider (VCP) which reduces workloads to generate up to 90% cost savings. It delivers a sovereign software layer that sits on top of any infrastructure - proprietary servers, European or U.S. cloud providers, or a combination of the two – and makes organisations independent of individual cloud providers. This developer tier gives developers the same work experience regardless of what's running in the underlying infrastructure. It's not a new cloud provider, it is the technology that makes it easier for developers to switch between cloud providers and/or their own hardware, and then provides the environment to build, manage, and deploy applications.