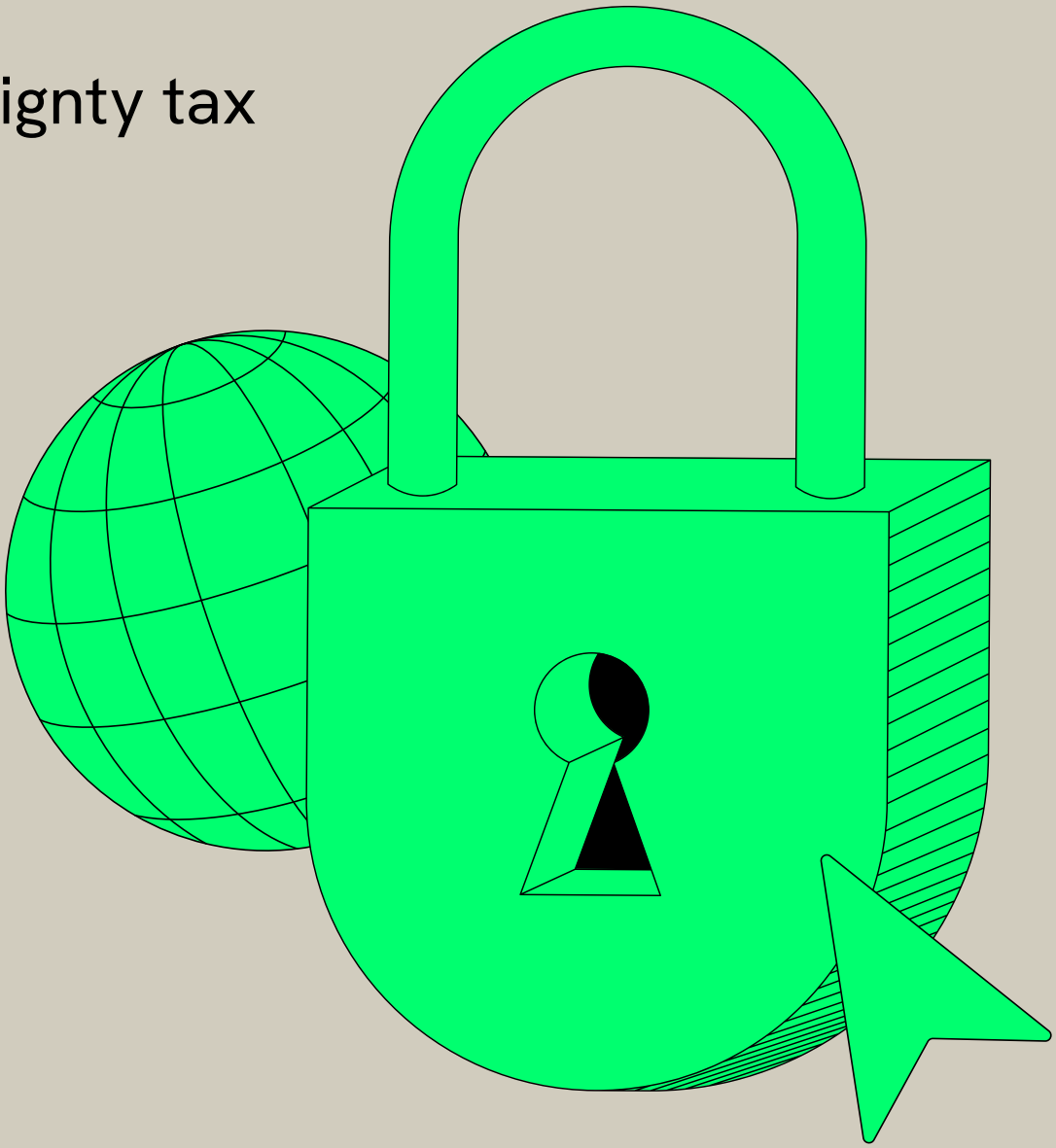
White paper 2026

civo

# The digital sovereignty revolution

## The sovereignty tax



Civo

# Foreword: A nation at a digital crossroads

A year on from our inaugural research, The Digital Sovereignty Revolution, UK organisations have moved beyond the debate on the potential perils of cloud dependence to the tangible realities. Sovereignty is now a strategic priority for 73% of organisations, up from 61%. But this isn't just talk; it's driven by the extraterritorial reach of foreign law, new AI security threats, and a broader sense of creeping dependency on Big Tech.


A strategic shift is underway, but here lies the problem: while 66% of leaders say they'd switch providers to gain greater control, many simply don't know that credible UK choices already exist, when, in reality, they do. The market exit options appear narrower than they are, undermining the UK's ability to future-proof its digital infrastructure and digital sovereignty.

With the trust gap widening and 43% of IT leaders now unsure how Big Tech handles their data, the extraterritorial reach of the US CLOUD Act only amplifies those concerns. The market is calling for change. Security and infrastructure leaders need more than another short-term hyperscaler fix. What's required now is a credible UK-based alternative that offers real, long-term control over vital data and infrastructure. The UK's digital future will only be secured if there is a collective willingness to match ambition with action.

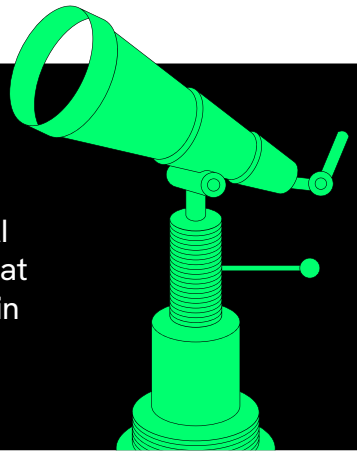
# Sovereignty defined

## The concept of digital sovereignty is relatively new and does not have a clear and universally accepted definition or legal definition. As such, it is open to interpretation and therefore subject to misinterpretation and exploitation.

In March 2026, the UK Government provided Parliament with a briefing on digital sovereignty. In this briefing, the UK Government framed digital sovereignty as the 'agency and capacity to make informed decisions that design the organisation's digital future.'

According to Minister Kanishka Narayan:

"The ability for the state to have strategic leverage in relation to AI such that it ensures continued access and continued assurance that its broader economic and national security goals can be satisfied in an ongoing manner."



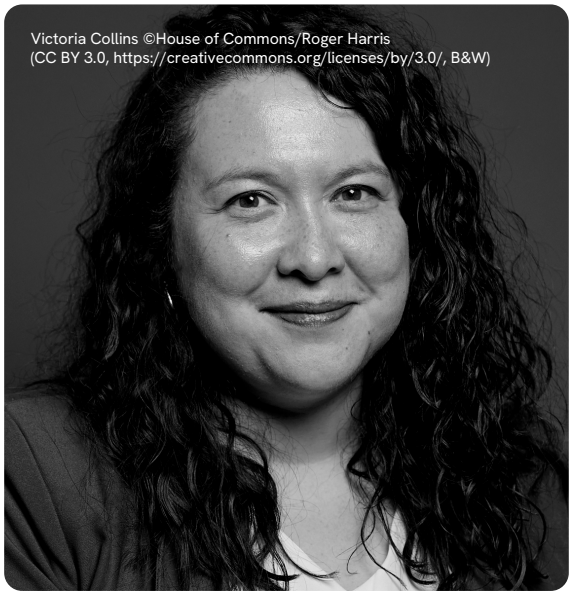
**Since there is no universally accepted or legally enforceable definition, the term has the potential to become a buzzword instead of an established standard.**

Some hyperscalers are promoting 'sovereign clouds' with little or no jurisdictional control, a practice that Clara Chappaz (former Minister of Digital for France) refers to as 'sovereignty washing'. While Europe has made progress toward establishing more clearly defined frameworks, organisations need to go beyond vendors' rhetoric about sovereignty and determine their own meaning for digital sovereignty concerning their data, infrastructure, and compliance obligations.

# Methodology

Commissioned by Civo, the 2026 iteration of The Digital Sovereignty Revolution examines whether growing geopolitical uncertainty is changing how UK organisations think about cloud infrastructure, particularly the trade-offs between hyperscale convenience, vendor dependency, and long-term sovereignty. Surveying 1,000 UK-based IT leaders (CTOs, CISOs, and Cloud Architects) across various businesses, the study expands on its 2025 baseline to present an empirical estimation of the "Sovereignty Tax" – an indication of the costs incurred as a result of vendor lock-in and being dependent on foreign providers. The framing of the conversation around these issues has become increasingly positive recently. But the data shows that the industry faces an immediate turning point, and it is time to take the matter seriously.

Our previous Digital Sovereignty report has already proved pivotal to the debate. Citing the 2025 research, Liberal Democrat MP Victoria Collins referenced these findings when calling for greater emphasis on the challenges of technology sovereignty during a Westminster Hall debate in March, which revealed that the majority of UK IT decision-makers consider data sovereignty a major priority in their strategies as geopolitical pressures continue to gather.




"A study by Civo, a UK provider of sovereign cloud, found that of 1,000 UK-based IT decision makers, 83% were worried about the impact of international developments on their data sovereignty"

*- Victoria Collins, Liberal Democrat MP*

By rooting these trends in trust and jurisdictional control, the report provides a granular and naturalistic view of the UK as a player on the global stage in 2026. The debate around digital sovereignty is intensifying, marking a promising shift as Parliament takes a positive step forward for the country. But what the data communicates – supported by both the findings and the wider debate – is that action is necessary. Digital sovereignty will require readiness for trade-offs, as well as tempered investment in the capabilities that deliver agile, long-lasting resilience.

# Key findings

**73%** of UK IT leaders now recognise data sovereignty as a strategic priority - a sharp 12-point rise since last year.

**61%** of those organisations cite escalating regulatory and compliance pressures as their primary operational driver.

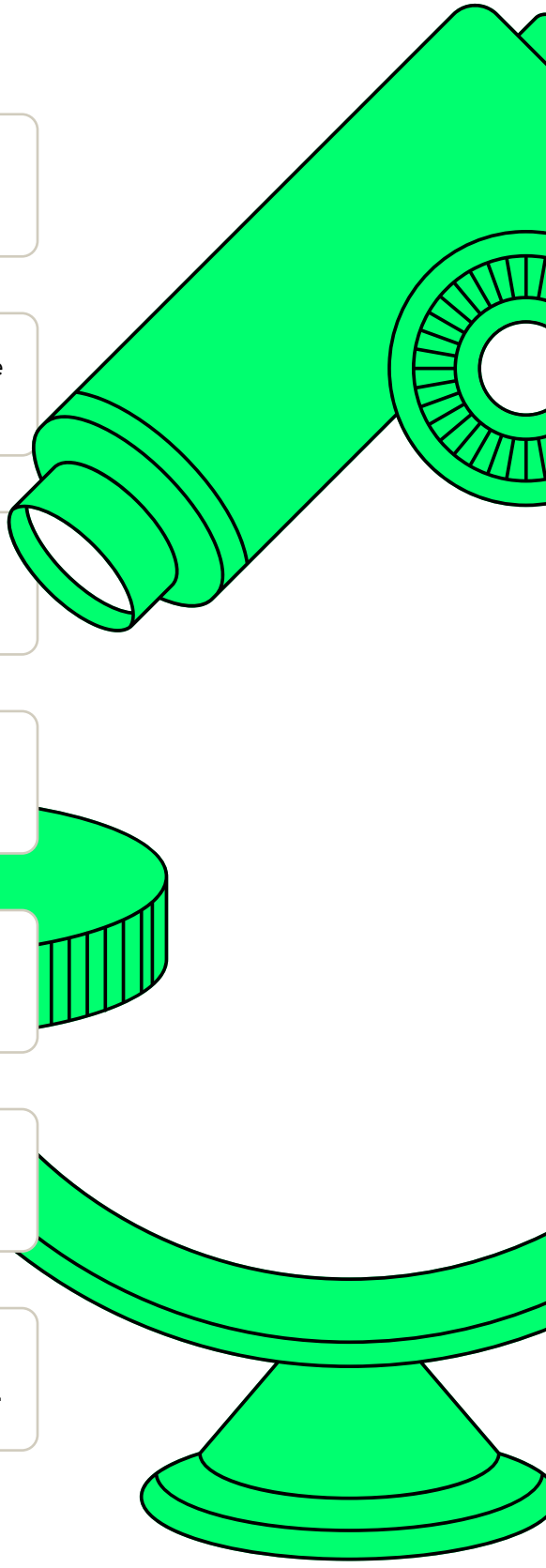
**77%** of UK IT leaders remain deeply concerned about the exposure of their data infrastructure to geopolitical risk.

**28%** of organisations expect to deepen their reliance on US hyperscalers, up from 12% last year.

**90%** of IT leaders are calling for a more proactive government stance to actively back British cloud technology.

**72%** agree that UK innovation requires domestic infrastructure, but **43%** cite high compute costs as a primary barrier to entry.

**66%** would consider switching cloud providers to regain control, yet successful migration to domestic alternatives has stalled at **15%.**



# Confronting the hyperscale monopoly

UK digital infrastructure is witnessing an operational shift. There's been an acceptance of US hyperscalers for years. Only now is the market seeing a more aggressive, strategic reaction from players in the industry. The threats perceived in 2025 around geopolitics have, in 2026, materialised to such a degree that boardrooms are actively involved. This isn't fear-driven; it's desire-driven. The UK needs to be resilient in the future, and this requires confronting these pressures head-on.

77%
of leaders
are *concerned*

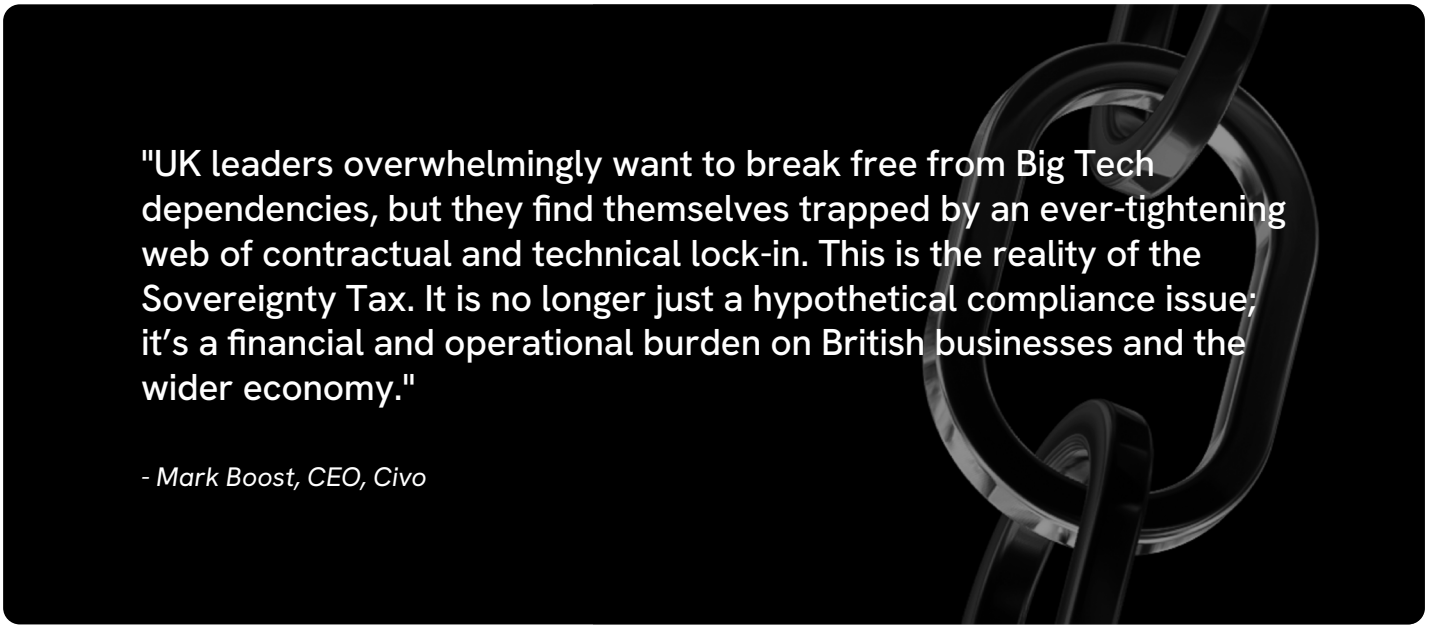
**The growing awareness of these risks across the UK is encouraging, but the data tells a more complicated story: 77% of leaders are concerned, and 64% feel that continued reliance on a small group of global cloud providers isn't sustainable.**

With US platforms capturing 80% of the market, what was once seen as commercial pragmatism is exposed as structural risk. Trust isn't enough; this is a strategic imperative. The UK must now consider digital infrastructure a national resilience challenge that cannot be extricated from its global geopolitical context.

# The sovereignty tax becomes reality

**What was once discussed hypothetically is now emerging as a documented consequence of relying on foreign cloud infrastructure. The Sovereignty Tax is not an official term, a regulated concept, or a single, calculable fee, but rather one that encapsulates the cumulative cost of delaying taking control.**

It is a price exacted from organisations that continue to build critical systems on platforms they cannot fully govern. It results in unpredictable costs, limited negotiating power, restricted portability, incomplete data visibility, operational disruption and exposure to legal or policy decisions made outside the UK.




This year's study shows this is no longer theoretical. In the past year, 39% of UK IT leaders experienced outages originating from US hyperscalers, with 15% experiencing them several times. Among those hit by outages, 29% reported a direct financial cost, 40% now report risk exposure above £50,000, and 5% report costs exceeding £1 million.

While the immediate symptoms may be unexpected bills, outages or operational disruption, the true underlying nature of the Sovereignty Tax is a lack of control.

This is the toll most organisations are already paying without seeing it on an invoice. Every year, proprietary API dependencies deepen, egress fees make exits more expensive, and migration complexity compounds.

The scale of the trap is visible in the data: three-quarters of IT leaders doubt their ability to exit a major US provider, with some even questioning their ability to do so at all. Organisations are not simply choosing to stay; in many cases, they have lost the practical ability to leave.

For UK organisations, this is now a board-level issue. Sovereignty is integral to business continuity, innovation, customer trust, and competitiveness. US tech policy dictates that access to hyperscaler platforms can be restricted or withdrawn for reasons outside a customer's control, so a single policy change can have serious repercussions for the entire UK digital economy.

The US CLOUD Act further grants US authorities the power to request access to data held anywhere in the world from providers subject to US jurisdiction, with no legal requirement for providers to inform customers. This is a structural condition of the infrastructure, not a theoretical risk, and it is difficult to assess: only 35% of UK organisations have full clarity on where their data is located and governed, meaning the majority cannot accurately quantify their exposure.

**Understanding the Sovereignty Tax makes visible the hidden cost of taking control for granted. It does not refer simply to the literal cost of relying on foreign cloud infrastructure, but to the accumulating cost of staying dependent on platforms that can’t be fully governed for longer than the business can justify.**

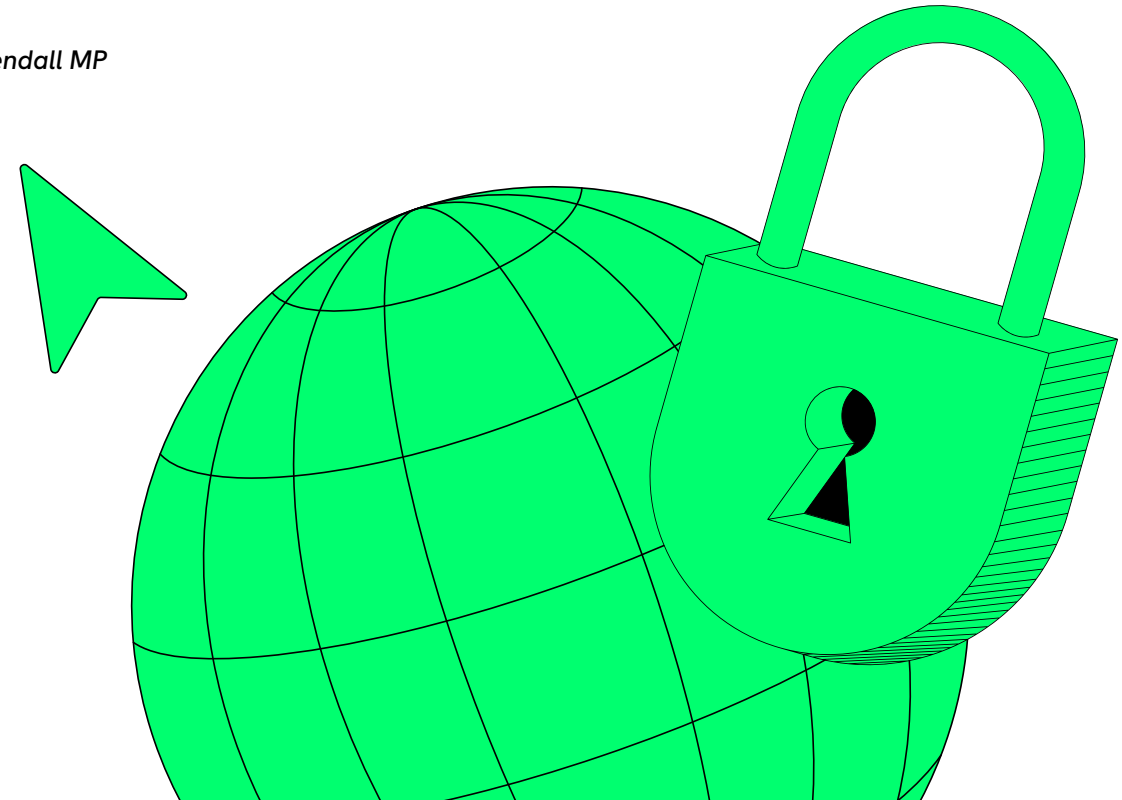
# The fight for UK AI sovereignty

The new frontier for AI is sovereign infrastructure, and the UK's appetite is clear. The nation's ambitions are bold and timely. But as industry leaders know, the growth of sustainable AI in the UK will depend not only on the ability to build technology but also on maintaining unbroken, clear visibility and control over the data and infrastructure on which the economy relies. Domestically controlled infrastructure is now seen as critical to the UK's AI future by 72% of leaders. But nearly half still identify unpredictable compute costs as the aspect of AI's trajectory that poses the biggest threat to innovation. The debate has moved from who owns the data to the nuances of transparency, cost certainty, and jurisdictional control.

It's telling that 58% of leaders now cite the legal jurisdiction of their AI provider as a concern, with 43% saying their AI workloads must be under UK jurisdiction. The risk of access by foreign governments, which the US CLOUD Act raises, only strengthens the case for sovereign infrastructure under the UK's control.

**"Control over where AI systems are built, how they operate and who ultimately controls them is now fundamental to economic security, energy security and defence security... For Britain, AI sovereignty is about reducing over-dependencies and increasing resilience in key national strategic priorities."**

*- The Rt Hon Liz Kendall MP*

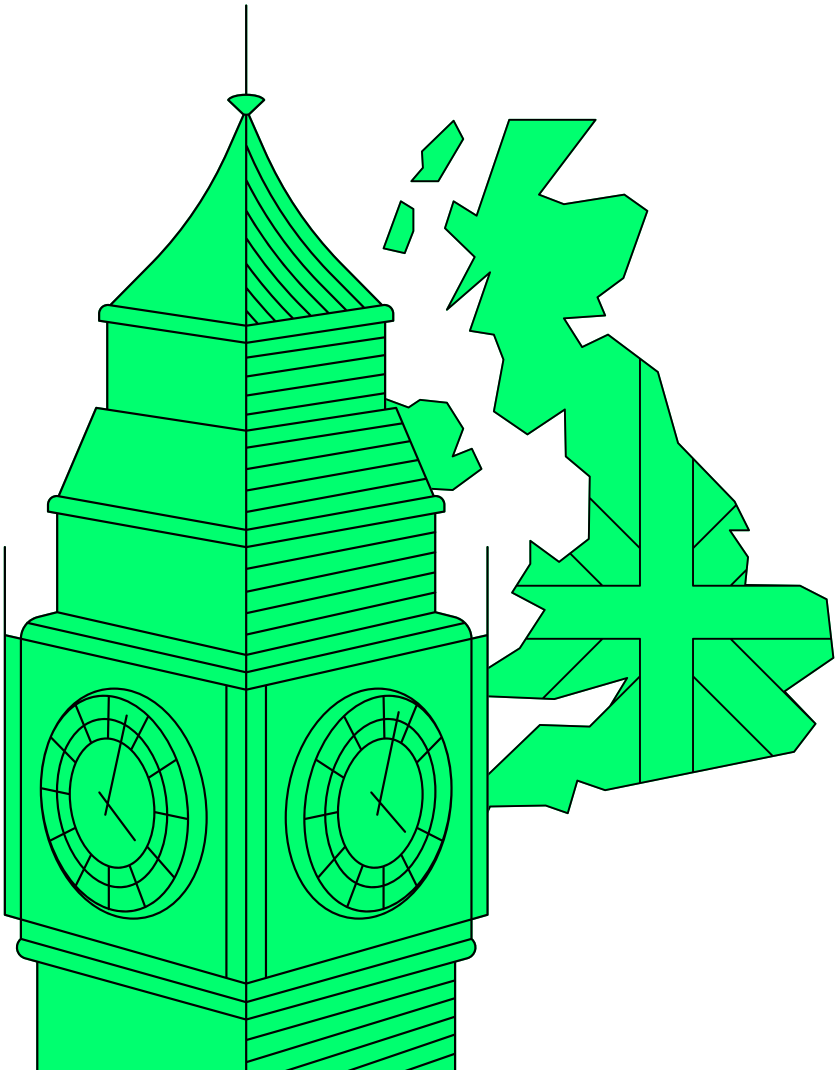


# UK tech demands action over policy statements

**While Parliament has adopted a stronger stance on data sovereignty, the UK tech sector demands more than standalone policy statements.**

A substantial shift in attitudes has been tracked across the industry over the past 12 months: 90% of IT leaders now believe the government must take a more proactive approach to supporting homegrown tech, up sharply from 60% last year.

The geopolitical risk is choking growth, too. Forty-two per cent of leaders affected said international instability in the last year meant they've delayed critical strategy at work, and simply 'avoiding suppliers from abroad' is not proactive enough. At this stage, the industry needs an unequivocal and proactive commitment from political leaders to work closely with the private sector on building credible domestic alternatives and a future-proofed UK technology ecosystem.



# Stuck in the vendor lock-in trap

The evidence is clear: while strategy is better understood and more organisations begin to treat sovereignty as a boardroom-level issue, the architectural changes required to implement this shift are relatively slow to manifest. Usage of US-based providers isn't declining at the rate expected. In fact, the opposite is true: the percentage of organisations intending to deepen their US ties has doubled. This highlights an ever-greater gap in confidence between stated strategy and actual execution.

While strategic roadmaps often preach diversification, execution tells a different story—one deeply rooted in vendor lock-in and interoperability challenges. Organisations frequently buy more hyperscaler services not out of strategic preference, but because they are already stuck there. The friction of moving data and the lack of seamless cross-platform interoperability create a gravitational pull, effectively forcing companies to double down on their incumbent US providers rather than transitioning away. These restrictions turn potential interoperability through open source into a closed environment.

Only one in four leaders truly believes they could exit a major US provider, and a significant minority admit they can't exit at all. In practice, an ever-tightening web of technical and contractual lock-in is conspiring against the objective of increased local control. There is also a significant disconnect: while a majority (66%) are willing to switch providers to regain control, vendor lock-in has stalled the successful migration of usage to a more domestic alternative at just 15%.

# Open source and the road to UK sovereignty

Open source has been recognised as a critical factor in achieving sovereignty today and described by Hugging Face as a “cornerstone” of Sovereignty. It is indeed critical to today’s infrastructure and has the potential to enable trust.

> **We will “make the UK the home of open source talent.”** - ***Kanishka Narayan, MP, Minister for AI and Online Safety***

Today’s cloud environment is dependent on open source software for its infrastructure. Hyperscalers and domestic providers alike depend on it. Its use enables the build out of globally collaborative infrastructure by local businesses in competition to the hyperscalers.

"Open source is at the heart of today’s digital infrastructure. From K8s to Open Stack and of course AI, without these we could not hope to build the innovative environments that enable a sovereign approach to cloud and infrastructure. Re-using that globally collaborative and freely available technology enables new market entrants and opens up competition. That’s the only route to sovereignty today."

*- Amanda Brock, CEO, OpenUK*

Open source is not a peripheral consideration in the sovereignty debate. It is foundational to it. Without the freely available, globally collaborative infrastructure that open source provides, the domestic alternatives that UK organisations need could not exist at competitive scale.

It levels the playing field, allowing British providers to build on the same technological foundations as the hyperscalers, without the dependency or the lock-in that follows. Crucially, it also enables the interoperability that makes switching providers a realistic prospect rather than a distant ambition. The UK cannot close the gap between sovereign intent and sovereign action without treating open source as a strategic national asset. It underpins competition, fuels innovation, and makes genuine digital independence possible.

# Conclusion

The debate surrounding digital sovereignty represents a fundamental paradigm shift in how UK organisations approach critical digital infrastructure. Far from a legacy IT consideration, sovereignty has emerged as a frontline strategic imperative—central to national resilience, customer trust, and long-term economic security. This shift was catalysed by high-profile legal admissions proving that contractual promises cannot fully override extraterritorial laws, laying bare the structural vulnerabilities at the heart of global cloud architectures. In an era where political friction and tariff threats directly manifest as operational volatility, structural passivity poses a severe threat to corporate governance. Organisations that fail to proactively re-architect their infrastructure risk finding themselves trapped in legacy ecosystems that can no longer meet modern compliance, privacy, or sovereign data standards.

True resilience demands immediate action to bridge the gap between strategic intention and operational execution. To systematically turn these vulnerabilities into a sustainable competitive advantage, UK enterprises and public sector bodies must immediately execute a definitive sovereign framework built upon five core pillars:

**Establish a sovereign risk framework:** Elevate digital sovereignty to a frontline item on the corporate risk register, embedding a quantifiable Sovereignty Tax directly into all long-term financial and operational forecasts.

**Mandate complete data visibility:** Eliminate dangerous administrative blind spots by conducting comprehensive audits to achieve full visibility into the exact physical jurisdictions where corporate and client data is stored, processed, and governed.

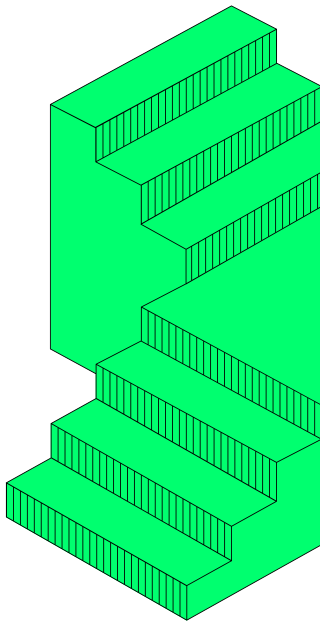
**De-risk through infrastructure diversification:** Mitigate single-vendor lock-in and foreign jurisdictional exposure by actively transitioning workloads toward robust hybrid architectures or multi-cloud strategies.

**Prioritise local compliance alignment:** Base all infrastructure procurement decisions on strict alignment with UK data protection frameworks, ensuring sensitive operational workloads remain completely insulated from foreign legal overreach.

**Scale domestic alternatives:** Move past abstract architectural designs and actively recognise, procure from, and scale viable, high-performance domestic technology providers capable of competing effectively on a global stage.

By systematically embedding these pillars into core business strategies, UK organisations can effectively navigate the complexities of shifting regulatory and geopolitical landscapes. Moving away from infrastructure decisions driven solely by short-term convenience allows the tech sector to rebuild foundational trust with consumers and partner agencies alike. Ultimately, transforming technological sovereignty from a restrictive compliance burden into a baseline requirement for innovation will ensure sustainable growth, secure data integrity, and foster a truly resilient and independent digital economy.

# About Civo



Civo is the Sovereign Cloud and AI platform built for more, delivering fast, reliable, and scalable infrastructure with simplicity at its core. Offering both public and private cloud solutions, Civo ensures organisations have full control over their data while maintaining flexibility and compliance. Designed to challenge traditional cloud models, Civo prioritises fairness, data sovereignty, and transparent pricing, enabling businesses to scale without hidden costs.

**Trusted by DevOps teams and enterprises worldwide, Civo provides:**

## civo public

- Superfast managed Kubernetes
- High performance compute
- Powerful managed databases

## civo private

- CivoStack Enterprise
- Civo FlexCore
- Edge Computing

## civo ai

- High Performance GPUs
- relaxAI: A privacy-first AI assistant
- Climate-friendly AI services

## Contact our sales team

Explore how our cloud services can empower your digital future.

Scan the QR code to learn more

# Resources


[1.] **Commons Library. (2026, March 6). Digital sovereignty (CBP-10547). UK Parliament.**
https://commonslibrary.parliament.uk/research-briefings/cbp-10547/

[2.] **Euractiv. (2025, April). Against US digital 'predators,' France digital minister calls for a European 'pack hunt.'**
https://www.euractiv.com/section/tech/news/against-us-digital-predators-france-digital-minister-calls-for-a-european-pack-hunt/

[3.] **Sénat français. (2025, June 10). Commande publique: audition de Microsoft [Public procurement: Microsoft hearing].**
https://www.senat.fr/actualite/commande-publique-audition-de-microsoft-5344.html

[4.] **Congress.gov. (2018). H.R.4943, 115th Congress (2017-2018): CLOUD Act. Library of Congress.**
https://www.congress.gov/bill/115th-congress/house-bill/4943

[5.] **UK Parliament. (2026, March 10). Technology sovereignty. Hansard, House of Commons.**
https://hansard.parliament.uk/commons/2026-03-10/debates/A91DF2A1-6231-4A38-AF17-56B742D06E95/TechnologySovereignty

[6.] **Competition and Markets Authority. (2025, July 31). Cloud services market investigation. GOV.UK.**
https://www.gov.uk/cma-cases/cloud-services-market-investigation

[7.] **European Commission. (2025, November 18). Commission launches market investigations on cloud computing services under the Digital Markets Act.**
https://digital-markets-act.ec.europa.eu/commission-launches-market-investigations-cloud-computing-services-under-digital-markets-act-2025-11-18_en

[8.] **Computerworld. (2024, November 27). FTC opens antitrust investigation into Microsoft's cloud, AI, and cybersecurity practices.**
https://www.computerworld.com/article/3614495/ftc-opens-antitrust-investigation-into-microsofts-cloud-ai-and-cybersecurity-practices.html

[9.] **Computer Weekly. (2024). Microsoft hides key data flow information in plain sight.**
https://www.computerweekly.com/news/366632040/Microsoft-hides-key-data-flow-information-in-plain-sight

[10.] **Department for Science, Innovation and Technology, and Kendall, L. (2026, April 28). Britain must secure greater control and leverage over AI to protect our national security in fractured world. GOV.UK.**
https://www.gov.uk/government/news/britain-must-secure-greater-control-and-leverage-over-ai-to-protect-our-national-security-in-fractured-world

[11.] **Kaffee, L. A. (2025, June 11). Open Source AI: A Cornerstone of Digital Sovereignty. Hugging Face Blog.**
https://huggingface.co/blog/frimelle/sovereignty-and-open-source

[12.] **The Stack. (2026, May 7). UK open-source contributions tick upward, but...**
https://www.thestack.technology/uk-open-source-contributions-tick-upward-but/

[13.] **UK Parliament. (2026, February 3). Cyber Security and Resilience (Network and Information Systems) Bill: Written evidence (CSRB04).**
https://publications.parliament.uk/pa/cm5901/cmpublic/CyberSecurityResilience/memo/CSRB04.htm

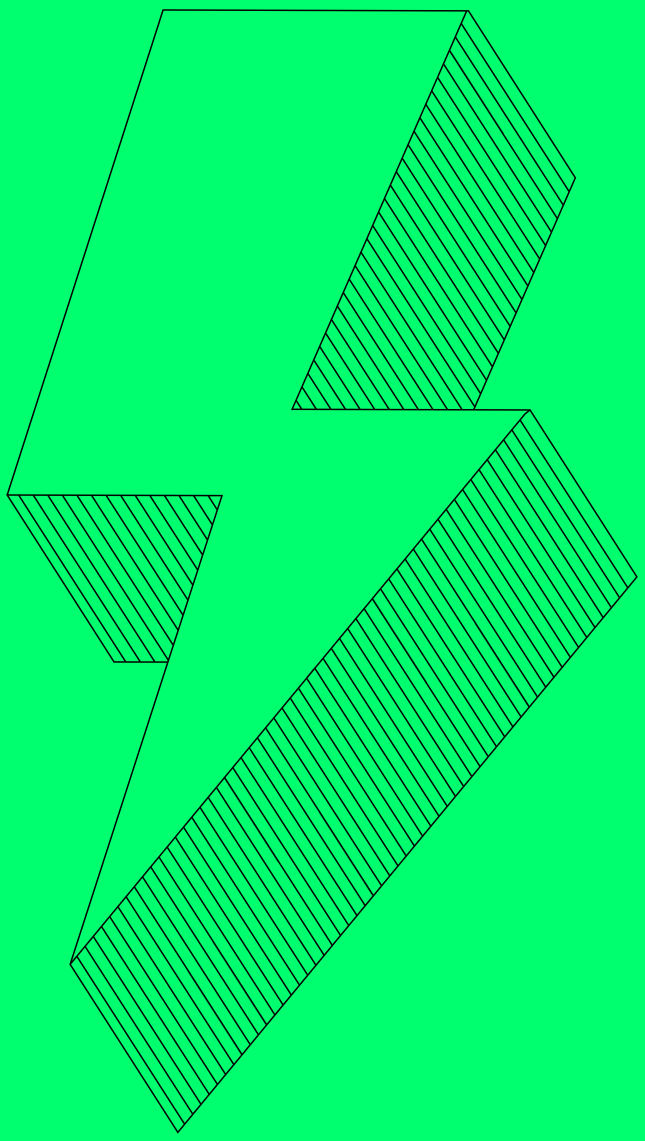
[14.] **Ravindran Pillai, P. (2026, April 1). The architect's dilemma: Balancing global software standards with regional sovereignty mandates in the age of geopatriation. SSRN.**
https://ssrn.com/abstract=6598278

[15.] **EuroStack. (n.d.). EuroStack: Building Europe's digital future.**
https://eurostack.eu/

[16.] **Civo. (2025). The digital sovereignty revolution: What UK businesses need to know.**
https://www.civo.com/digital-sovereignty-revolution-report-2025

The Digital Sovereignty Revolution

civo



# Built for more

Civo Ltd
www.civo.com
sales@civo.com

32-37 Cowper St,
London EC2A 4AW
United Kingdom