The digital sovereignty revolution:

What UK businesses need to know

WHITE PAPER

2025

Table of contents

Foreword

Amid rising scrutiny of US tech dominance and growing awareness of the need for digital autonomy, UK organisations are beginning to confront the long-term risks of outsourcing the UK's digital infrastructure to global cloud providers.

The sovereignty debate has reached a boiling point. Tariffs and increasing geopolitical instability have turned digital policy and decision making into a headline issue, forcing organisations in the UK and the EU to ask the question: *how much more control are we willing to cede?*

© Sportsfile / Sam Barnes

Speaking at an event on digital sovereignty, French Digital Minister, Clara Chappaz declared:

"In a world dominated by predators... Europe must work as a pack... and retaliate against the idiotic trade war."[1]

Her message cut through the usual diplomatic tone. It captured the growing European impatience with what Chappaz called "*sovereignty washing*", where US cloud providers strike surface-level partnerships with EU firms to claim local legitimacy.[2] At the heart of her warning was a harsh reality: US companies now control as much as 80% of the European cloud market.

In the EU, there are multiple initiatives underway in a bid to claim back EU's digital sovereignty, including EuroStack, which aims to "create resilience, protect our autonomy and sovereignty in a volatile world, and empower the people and businesses of Europe"[3].

As questions around digital autonomy and sovereignty move from the fringes to the centre of strategic planning, businesses and governments are beginning to diversify their cloud vendors, explore more locally governed services, and weigh sovereignty as a key factor in digital investment.

In March 2025 the Dutch Parliament asked the Dutch government to come up with a strategy to wean itself off the US cloud providers[4] and realise a Dutch sovereign cloud. Digital sovereignty plays a major role in Germany's cyber-security strategy[5]. EU cloud providers are seeing a significant up-tick in new business as European businesses and nations actively seek alternatives to US hyper-scale cloud[6].

We've seen global players respond to this shift by expanding their "sovereign" cloud offerings. Sovereignty is no longer a "nice to have", it's becoming a strategic imperative and the market is at a critical inflection point. These moves signal just how seriously vendors and buyers alike are treating the digital sovereignty conversation.

Civo examined how more than 1,000 UK IT decision-makers are thinking about digital sovereignty: what's driving concerns, what practical steps are being taken, and how attitudes toward US-based providers are evolving. This research also looked at the drivers behind multi-vendor strategies and the appetite for more local control.

We set out to understand how the growing focus on digital sovereignty is influencing infrastructure decisions, reshaping cloud partnerships, and emerging as both a strategic and political issue for UK businesses as they navigate global uncertainty.

M. Boost.

Mark Boost
CEO & Co-founder of Civo

Methodology

This report is based on research completed in April 2025 and conducted by Civo, through a third-party survey partner, surveying 1,006 UK IT decision-makers across a wide range of industries and organisation sizes. Respondents were selected to provide a representative view of organisations that rely on digital infrastructure to support critical business operations.

The survey explored attitudes toward:

- Data sovereignty and jurisdictional control
- Eroding trust in global hyperscalers and Big Tech
- The impact of geopolitical risks on cloud strategies
- Emerging multi-cloud, hybrid, and repatriation strategies
- Regulatory compliance pressures

The findings presented throughout this report offer a snapshot of how sovereignty is reshaping IT decision-making at a critical moment for the UK's tech sector and wider economy.

Key findings

84% of UK IT leaders are concerned that geopolitical developments could threaten their ability to access and control their data.

61% of organisations say sovereignty is now a strategic priority.

68% will only use AI services where they have complete certainty over data ownership.

60% of organisations are no longer reliant on a single cloud provider.

60% of UK IT leaders say the Government should stop buying US cloud in the wake of tariffs.

71% prioritise sovereignty in some way when choosing tech or infrastructure partners.

82% would consider switching from Big Tech to gain more control over data location and governance.

35% of organisations have full visibility into where their data is stored, processed, and governed.

24% say their organisation is not strategically or technologically prepared for new data protection or data sovereignty guidelines.

68% say stronger UK/EU compliance would make them more likely to choose a non-US or locally governed provider.

Trust in Big Tech is fracturing

For years, US tech giants have enjoyed near-unquestioned dominance over the global cloud market. Trust in their infrastructure and services has been largely an unspoken norm, sustained by assumptions of stability, neutrality, and shared economic interests. But today, that foundation is cracking.

In the first half of 2025 alone, we've seen escalating tariff threats aimed at the EU, growing geopolitical friction, and a US administration taking an increasingly isolationist approach to global tech policy. All of this is making compliance with international data protection rules increasingly complex and harder to navigate for businesses operating across borders. The old model of open international cooperation is being replaced by something far more unpredictable. And UK businesses are taking note. Nearly half (45%) of UK IT leaders are actively considering repatriating data from US platforms.

43% of UK IT leaders explicitly say they do not trust Big Tech with their data.

Political risk is now becoming a digital risk. Civo's research found that 84% of UK IT leaders are concerned that geopolitical developments could threaten their ability to access and control their data. This reflects a growing recognition that digital infrastructure choices are now deeply entangled with geopolitics.

Even after Brexit, the UK retained GDPR as transposed into the Data Protection Act 2018. That post-Brexit continuity is part of what's driving UK organisations to question the logic of handing over sensitive workloads to platforms governed by increasingly divergent legal systems.

This growing unease is being reflected in policy preferences. 62% of UK IT leaders believe the UK government should stop buying cloud services from US companies in retaliation against potential trade tariffs, suggesting a growing appetite for digital autonomy in the UK tech sector. It shows that a majority of UK businesses not only view digital sovereignty as a strategic concern but are also willing to see it enforced through procurement decisions.

37% of UK IT leaders worry that the US government could sequester their data, a concern that rises even higher in sectors with strict regulatory obligations.

Digital sovereignty, once dismissed as a niche technical concern, is now climbing the strategic agenda. Businesses now want complete transparency on where their data is stored and who ultimately controls it.

Digital sovereignty takes its seat at the strategy table

Few sectors are talking about sovereignty more than tech. As organisations race to modernise with AI, they are also becoming acutely aware that this shift cannot come at the expense of customer trust. In a time of extreme geopolitical volatility, we're seeing an increasing number of businesses wanting their data closer to home. 61% of respondents agree that digital sovereignty is a strategic priority for their organisation.

77% of UK IT leaders agree that the most accurate definition of digital sovereignty means maintaining authority and control of data within the jurisdictional boundaries of one nation.

But the motivations behind this trend reveal an even deeper recalibration of business risk:

- **60% cite data access guarantees** as a key motivation. This means ensuring they can retain unbroken access to critical information amid geopolitical uncertainty.
- **54% prioritise compliance with jurisdiction-specific rules,** recognising the growing complexity and consequences of regulatory obligations.
- **53% are motivated by concerns over third-party control.** There's a growing awareness that even the most advanced technologies offer little protection if governance lies outside their influence.

As one respondent put it:

"Data sovereignty is a strategic concern for our organisation because we handle sensitive client information, including personal data shared through interpreting and translation services. If data is stored or processed outside the UK without proper controls, it could expose us to legal risks around GDPR compliance and undermine the trust we have with service users and partner agencies like the NHS and local councils."

Trust, once assumed, now has to be earned. Big Tech's recent track record has only deepened scepticism. High-profile antitrust cases and regulatory investigations have exposed patterns of market dominance, data misuse, and opaque practices that undermine confidence. In the United States, the Federal Trade Commission (FTC) has launched major cases against several tech giants, alleging abuses of monopoly power and anti-competitive behaviour.[7] [8]

Similar efforts are underway in the UK and the EU. In January 2025, the UK's Competition Markets Authority (CMA) released its provisional findings from an ongoing investigation into Microsoft and Amazon's dominance in the cloud computing industry. Citing evidence of intentional barriers to switching providers and restrictive software licensing practices, the CMA provisionally concluded that Microsoft's conduct is "harming competition in cloud services."[9] Meanwhile, the European Commission continues to scrutinise and regulate tech platforms under its Digital Markets Act, the Data Act, and the European Parliament has recently adopted a call to open new investigations into the cloud sector to ensure competition and innovation.

Globally, regulators are increasingly scrutinising the role these companies play not only in shaping markets, but in influencing the flow and control of sensitive information.

Against this backdrop, many UK organisations are starting to feel uneasy about outsourcing their most critical data to providers whose priorities and jurisdictions often don't align with their own. The introduction of the UK Cyber Security and Resilience Bill has added another layer of complexity.[10] For businesses working with critical infrastructure, the bill introduces tougher reporting rules and puts more pressure on businesses to understand and secure their supply chains. In practice, that means companies will need to think more carefully about where their data lives, who has access to it, and whether their current setup can meet these new expectations.

Across the Atlantic, the US CLOUD Act has intensified concerns around privacy and control, giving US authorities the power to access data held by US companies, even if that data is stored outside the United States. For UK businesses, this raises the risk that sensitive information could be subject to foreign government access, undermining local data protection laws and ultimately eroding customer trust.

In July 2024, it was revealed that Police Scotland's data, hosted on Microsoft Azure, could potentially be moved to the US.[11] Microsoft admitted that, under certain conditions, it couldn't guarantee that sensitive UK policing data would remain within national borders. This incident, where UK data protection regulation was knowingly breached, cast a spotlight on the risks of hosting data with overseas providers that provide processing and support services from overseas. For organisations navigating strict regulatory environments, this disconnect between data policy and jurisdiction can quietly but seriously undermine trust.

As one respondent put it bluntly:

"Big Tech has misused data in the past, and therefore has proved it cannot be fully trusted."

AI digital sovereignty

This growing mistrust is being felt in decisions around AI adoption.

68%

68% of respondents say they will only use AI services where they have complete certainty over data ownership.

While AI offers enormous potential, organisations are rightfully asking tough questions: Who owns the data being fed into these models? Where is it processed? Can we ensure that sensitive information stays protected, both legally and practically? These concerns are no longer hypothetical.

Recent trade tensions have only intensified these anxieties. In an unprecedented move, Microsoft recently pledged to protect its EU cloud operations from potential political interference, with Brad Smith, Vice President and Chair, writing: "In a time of geopolitical volatility, we are committed to providing digital stability".[12] As part of this commitment, the company will add binding clauses to its contracts with EU governments and institutions, reserving the right to challenge any US mandate in court that seeks to suspend or disrupt services in Europe.

But while the gesture is significant, it is far from a guarantee. The US CLOUD Act remains firmly in place, granting US authorities the right to access data held by US companies, regardless of where it resides. While the CLOUD Act remains in force, enterprises and governments simply cannot trust US hyperscaler firms to keep their data fully private, regardless of the physical location of their infrastructure.

In that context, Microsoft's pledge is a hollow attempt to reassure an EU market increasingly wary of geopolitical overreach. With the prospect of more assertive US measures, this kind of commitment does little to resolve the structural vulnerability at the heart of the transatlantic cloud and AI infrastructure. For businesses navigating this shift, solutions like relaxAI, Civo's open-source sovereign AI assistant, offer a way to harness the power of generative models without handing over sensitive data to third-party platforms.[13] Built with transparency and control in mind, it aligns with the growing demand for AI tools that put security and data ownership first.

Multi-cloud migration is getting political

As digital sovereignty moves to the forefront of strategic planning, infrastructure strategies are being rewritten. Organisations are no longer building around a single trusted partner, they are looking to diversify for the sake of control, flexibility, and resilience.

40% of UK IT decision-makers would consider switching away from Big Tech to gain greater control over their infrastructure, and **78% already weigh sovereignty as a key factor in partner decisions.** This tells us that the traditional dominance of global hyperscalers is eroding as businesses reassess their long-term dependencies.

Today, 60% of organisations are no longer reliant on a single provider. Instead, they are adopting more diversified approaches:

- **29% are pursuing multi-cloud strategies,** spreading workloads across several providers.
- **31% are embracing hybrid models,** blending public and private infrastructure to regain flexibility.

Motivations vary:

- **65% want to enhance resilience and flexibility,** ensuring they can adapt to future regulatory, political, or operational shocks.
- **58% aim to reduce reliance on any single provider,** minimising the risk of vendor lock-in or foreign jurisdictional control.
- **46% are seeking to lower costs** through competitive sourcing.
- **41% are working to meet increasingly complex regulatory obligations** that demand clearer lines of data governance and accountability.

For many, cost pressures are beginning to reshape the digital sovereignty conversation. Recent US tariff threats have cast new doubt on the affordability of US cloud services. As import taxes on infrastructure components rise, there's growing concern that hyperscalers will pass these costs onto EU customers, hitting startups and leaner businesses hardest. With Microsoft, AWS, and Google controlling over 70% of Europe's cloud market, a price surge could stall growth, delay profitability, and deepen margin pressures for early-stage companies.[14]

At the same time, as concerns over control and geopolitical risk grow louder, businesses are rethinking the very foundations of their digital operations. Infrastructure decisions, once driven purely by cost and performance, are now entangled with questions of sovereignty, resilience, and national interest.

For many UK organisations, choosing a cloud provider is no longer just a commercial decision. It's becoming a political one too. Solutions like Civo's FlexCore are emerging to meet this need, offering flexible, on-premises cloud-native infrastructure that allows organisations to scale quickly while maintaining full digital sovereignty and regulatory alignment.[15]

Awareness has yet to translate into action

While concerns around control and resilience come to the forefront, structural changes have been slow to materialise. Despite the growing risks, many UK and EU businesses remain exposed, tied to critical infrastructure they don't fully control. Few have taken steps to migrate data or diversify their provider base, leaving operations vulnerable to external pressures and an increasingly volatile political landscape.

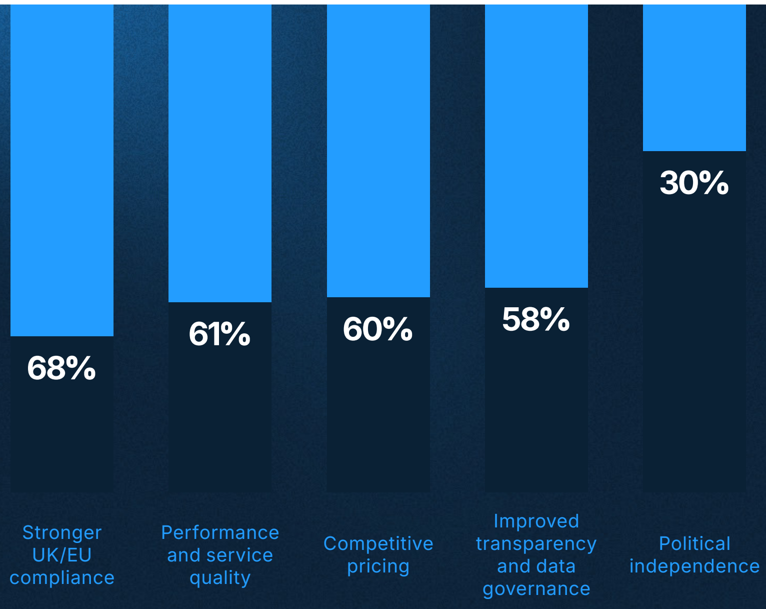
The gap between intention and execution:

- **Only 35% of organisations have full visibility into the jurisdictions where their data is stored and governed** - a dangerous blind spot in an era of regulatory complexity and geopolitical tension.
- While **76% say they are strategically prepared for new sovereignty guidelines,** just **15% have launched a significant data migration in the past year.**

This inertia reveals a dangerous disconnect: organisations recognise the strategic importance of sovereignty but are struggling to operationalise that understanding into their infrastructure decisions.

What customers say they want and what they're acting on

When asked what would encourage a shift away from Big Tech, respondents emphasised five key priorities:



Sovereignty is clearly playing a big role in decision-making: regulatory alignment, transparency, and local governance are among the top factors UK IT leaders say would encourage a shift away from Big Tech. But a closer look reveals that these concerns are still filtered through traditional enterprise priorities. Performance and price remain just as important, and in some cases, more actionable, than abstract ideals like political or legal independence.

Organisations want the benefits of digital sovereignty, but not at the expense of convenience or cost. The good news is that a new wave of sovereign providers is rising to meet that challenge, companies like Civo who are blending local control with enterprise-grade capability. As these offerings mature, the longstanding trade-off between sovereignty and competitiveness is starting to fade as cloud and AI consumers are given genuine choices.

As the political and regulatory landscape continues to evolve, the window for proactive action is narrowing. Those who delay risk finding themselves trapped in architectures that no longer meet the demands of digital sovereignty, compliance, or customer trust.

Conclusion

The sovereignty debate marks a fundamental shift in how UK organisations view digital infrastructure. No longer seen merely as a technical utility, sovereignty has moved into the public consciousness as a strategic imperative, central to questions of control, resilience, and future growth.

Our research shows that UK businesses are beginning to move beyond cloud strategies driven solely by convenience. Visibility, control, and jurisdictional certainty are becoming essential markers of resilience in a landscape where digital risk is now as much political as it is technical.

Sovereignty is no longer seen as a barrier to innovation. It is becoming a precondition for sustainable growth and long-term competitiveness amid shifting regulatory and political landscapes. Businesses that recognise this early and take tangible steps to re-architect their strategies will be better positioned to navigate the next phase of digital transformation with confidence.

As we look ahead, we see an opportunity to rebuild trust and create a cloud ecosystem that is more open, more accountable, and more aligned with the values businesses and customers increasingly expect. It's an opportunity to build a truly resilient and innovative British tech industry.

To achieve this, we recommend that UK and EU businesses take the following steps:

Recognise sovereignty as a strategic imperative:

Digital sovereignty is no longer a niche technical concern but has moved to the centre of strategic planning.

Prioritise sovereignty in infrastructure decisions:

Businesses should actively weigh sovereignty as a key factor when choosing cloud providers and tech partners.

Diversify cloud strategies:

Organisations should reduce their reliance on a single cloud provider and adopt multi-cloud strategies or hybrid models.

Gain visibility and control over data:

Businesses should strive to have complete visibility and control over their data, including where it is stored, processed, and governed.

Align with jurisdictional compliance:

Businesses should prioritise aligning their data location and governance with UK/EU compliance frameworks.

Address geopolitical risks:

Businesses should recognise that geopolitical developments could threaten their ability to access and control their data.

By taking these steps, UK and EU businesses can ensure they are well-positioned to navigate the complexities of digital sovereignty and achieve sustainable growth and long-term competitiveness.

About Civo

Civo is a global cloud provider 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 CLOUD

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

CIVO PRIVATE CLOUD

- 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] Euractiv. (2025, April 15). 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/

[2] Euractiv. (2025, April 15). 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] Euro-Stack. (n.d.). Euro-Stack.
https://euro-stack.eu/

[4] Desmarais, A. (2025, March 20). 'A threat to autonomy': Dutch parliament urges government to move away from US cloud services. Euronews.
https://www.euronews.com/next/2025/03/20/a-threat-to-autonomy-dutch-parliament-urges-government-to-move-away-from-us-cloud-services

[5] International Trade Administration. (2025, April 10). Germany – Digital economy.
https://www.trade.gov/country-commercial-guides/germany-digital-economy

[6] Nicol-Schwarz, K., Partington, M., & Sraders, A. (2025, April 29). Trump tariffs threaten cloud price hike for European startups. Sifted.
https://www.technewsday.com/2025/03/26/europe-seeks-alternatives-to-u-s-cloud-providers-amid-sovereignty-concerns/

[7] Federal Trade Commission. (2023, September 26). FTC sues Amazon for illegally maintaining monopoly power.
https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-sues-amazon-illegally-maintaining-monopoly-power

[8] Reuters. (2025, March 12). Trump's FTC moves ahead with broad antitrust probe of Microsoft.
https://www.reuters.com/technology/trumps-ftc-moves-ahead-with-broad-antitrust-probe-microsoft-bloomberg-news-2025-03-12/

[9] Competition and Markets Authority. (2025, January 28). Cloud services market investigation: Provisional findings.
https://www.gov.uk/guidance/cloud-services-market-investigation-provisional-findings

[10] UK Government. (2025, January 28). Cyber Security and Resilience Bill.
https://www.gov.uk/government/collections/cyber-security-and-resilience-bill

[11] Computer Weekly. (2025, April 28). Microsoft admits no guarantee of sovereignty for UK policing data.
https://www.computerweekly.com/news/366589152/Microsoft-admits-no-guarantee-of-sovereignty-for-UK-policing-data

[12] Smith, B. (2025, April 30). European digital commitments. Microsoft On the Issues.
https://blogs.microsoft.com/on-the-issues/2025/04/30/european-digital-commitments/

[13] Civo. (n.d.). relaxAI.
https://www.civo.com/ai/relaxai

[14] Sifted. (2025, April 29). Trump tariffs threaten cloud price hike for European startups.
https://sifted.eu/articles/trump-tariffs-cloud-price-hike

[15] Civo. (n.d.). FlexCore.
https://www.civo.com/flexcore