

A report for BT Group

The UK's Digital Sovereignty Opportunity



About Assembly

Assembly provides independent research on regulatory, policy, and legislative developments in communications markets and the digital economy.

For more information visit assemblyresearch.co.uk

About this study

BT asked Assembly to research the potential benefits of digital sovereignty to the UK and the policy levers that the Government could use to realise them. We outline policy actions that could encourage the business adoption of digital sovereignty, in support of the Government's growth agenda.

Contents

Executive summary	3
Introduction	7
Understanding what is meant by digital sovereignty	8
The benefits of sovereignty for UK organisations	12
The economic benefits of sovereignty for the UK	14
How the UK Government can seize the opportunity of digital sovereignty	17

Executive summary

Digital sovereignty is now a priority for businesses in the UK, driven by internal security and resilience priorities and external factors, such as geopolitics and regulatory pressures. Policymakers too are focused on how to navigate the issue given concerns around the over-reliance on foreign firms, particularly for technology. Though few governments have formalised approaches, there are expectations that many could move to impose sovereignty-related obligations over the coming years.

It is widely seen as an opportunity to create value for organisations, sectors and the economy at large. The advantages of sovereignty to domestic businesses and vital public services could be manifold, including strengthening data privacy and resilience by enhancing control over the digital services they employ, encouraging investment into critical digital infrastructure in the UK, and more. We estimate that many of these benefits are likely to translate into significant benefits for the UK economy. For example, the adoption of digital sovereignty could better protect businesses' data, encouraging them to adopt AI, which we estimate could support the UK to fully realise £18bn per year of the emerging technology's total projected economic impact. Without such adoption, the UK risks missing out on the full extent of AI's economic benefits in the coming years, which the UK Government has estimated to amount to £47bn each year over the course of the next decade.

Recent geopolitical events have exemplified why sovereignty has risen up commercial and policy agendas. Within a concentrated global public cloud market, for instance, dependencies during periods of service disruption have led to significant downtime costs for UK businesses. Such major incidents have also cost the UK economy through the loss of data, intellectual property (IP) and other digital assets, with estimates quoting that this cost could have been as much as £8.5bn in 2024 alone.¹ While strengthening digital sovereignty cannot eradicate these costs altogether, it can be part of the toolkit to reduce some security and resilience risks in the current climate, helping them to limit any potential impacts on their services, customers and revenues, with our estimates showing that this cost of data, IP and asset loss could be reduced by up to £632m.

The UK Government is increasingly alive to both the benefits and the risks; however, the risk of inaction is significant, given the potentially lucrative

economic benefits of a wider adoption of digital sovereignty. Our research highlights the different risks of Government inaction on this issue, but also outlines the potential benefits of intervention. There are policy levers it could use to support demand for domestically-developed digital solutions, from outlining a framework that builds consensus as to the importance of sovereignty to identifying the specific sectors where it might be most valuable. The Government could also make use of its natural convening powers to bring suppliers and customers together, while encouraging changes in procurement to support companies in the UK that could help promote a virtuous cycle of investment and national competitiveness.

As the political focus on digital sovereignty has started to develop in the UK and further afield, commercial approaches to the issue have emerged too. Telecoms operators have been quick to utilise their experience in the management of critical digital infrastructure and services to offer new sovereign solutions for businesses. Given this experience, we perceive that the telecoms sector will play a crucial role in the delivery and adoption of digital sovereignty.

Quantifying the economic impact of sovereignty and the risk of inaction



£18bn

Stronger data sovereignty could enable the UK economy to realise £18bn per year by giving businesses more confidence to adopt AI.



+£15bn

Sovereignty-led investment in data centres could have an economic impact of nearly £15bn by 2030.



£1bn

With data sovereignty, businesses in the UK's digital sector could avoid the risk of incurring GDPR fines totalling £1bn.



+£14bn

Growth in the sovereign cloud market in the UK over the next five years presents a £14bn commercial opportunity.



£630m+

The adoption of operational or technical sovereignty could reduce the annual costs to the UK economy of data, IP and asset loss by more than £630m.

Key messages

1. Few policymakers have so far formalised interpretations of digital sovereignty, but a general consensus around the three differing layers of sovereignty (data, operational, technical) has emerged in Germany and at an EU level. These early adoptions of definitions or frameworks for sovereignty have guided initial commercial approaches to the issue, with telecoms operators well-positioned to play a crucial role in ensuring sovereignty.
2. The adoption of the data, operational or technical layers of sovereignty will strengthen the resilience and data privacy of UK businesses in CNI and public sectors by increasing their control and visibility over sensitive data and key digital services. For each of these layers of sovereignty, solutions for businesses should align with their varying needs – for example, in the public sector, more sensitive digital operations may require complete operational control.
3. Our estimates show that the adoption of digital sovereignty could unlock significant economic benefits for the UK by enabling businesses to realise AI's full potential, encouraging investment into local data centres, protecting against regulatory fines, growing a domestic sovereign cloud market, and limiting the economic costs of data, IP and asset loss.
4. There are four actions the UK Government could take to support the adoption of secure and reliable UK-based digital services: i) outline a framework for sovereignty; ii) highlight sectoral requirements for sovereignty; iii) use natural convening powers to connect the supply and demand sides of the market; and iv) revise procurement rules and practices.

Introduction

Recent major cloud service outages and cyber attacks alongside current geopolitical tensions have raised concerns about over-reliance on a select few digital service providers. To combat this reliance, sovereign control over critical digital services has increasingly been hailed as a more resilient alternative for the future.

Digital sovereignty has quickly become a priority talking point among policymakers and businesses within the digital ecosystem around the world. So far, just a few jurisdictions have formalised their own understandings of what digital sovereignty means in practice, whether that be processing and storing data locally to increase privacy, full domestic supply chain control or some combination of these and other measures. The political desire for this has guided early commercial approaches too – in telecoms, operators recognise the importance of domestic network infrastructure and reliability to ensure sovereign control over digital services, and in some cases have started offering sovereign services to customers.

A range of sectors stand to benefit from the adoption of sovereign services, with solutions varying depending on the required levels of control. For example, a high criticality department of government will need a stronger degree of sovereign control over its digital services than a business operating in non-critical sectors, such as retail. These less critical sectors will still benefit from sovereign services, but may only require sovereign control and visibility over one element of their digital operations, e.g. data.

Understanding what is meant by digital sovereignty

Although existing frameworks differ, there is a general understanding that there are layers of digital sovereignty, such as data sovereignty, mid-level sovereignty that provide businesses with more control over their digital services, and a more full-control layer similar to the EC's 'full digital sovereignty', all of which can strengthen resilience. The mid-layer of sovereignty is often referred to as 'operational sovereignty', which the EC's Cloud Sovereignty Framework defines as, "the practical ability of EU actors to run, support, and evolve a technology independently of foreign control".² BT's own sovereign platform offering opts for this terminology and refers to its full sovereignty offering as 'digital sovereignty'.³ To assess the potential benefits of the adoption of digitally sovereign services for UK businesses, it is important to split these layers out, identifying where each would be most applicable in the UK.

Although these different layers of digital sovereignty are likely to benefit the UK's economy while strengthening the resilience and security of businesses in CNIs sectors, it is important to note that there may be some drawbacks of adopting more digitally sovereign services. Most notably, sovereign services are likely to come at a higher price than a non-sovereign alternative due to the increased costs associated with ensuring digital operations or data flows remain securely in the UK. Despite the potential benefits of these sovereign services to UK businesses, many may opt to continue to use non-sovereign services to keep their costs from rising.

The importance of telecoms operators to digital sovereignty

Amid geopolitical risks and compliance pressures, incumbent telecoms operators – as critical national assets – are well placed to offer the capabilities and infrastructure to help deliver digital sovereignty that is aligned with domestic interests and policy. As sovereignty does not require a 'one-size-fits-all' approach, at each layer identified (see *Figure 1*), operators seek to offer customers tailored solutions and controls that suit their needs, while still ensuring compliance with national legislation and sector-specific regulation:

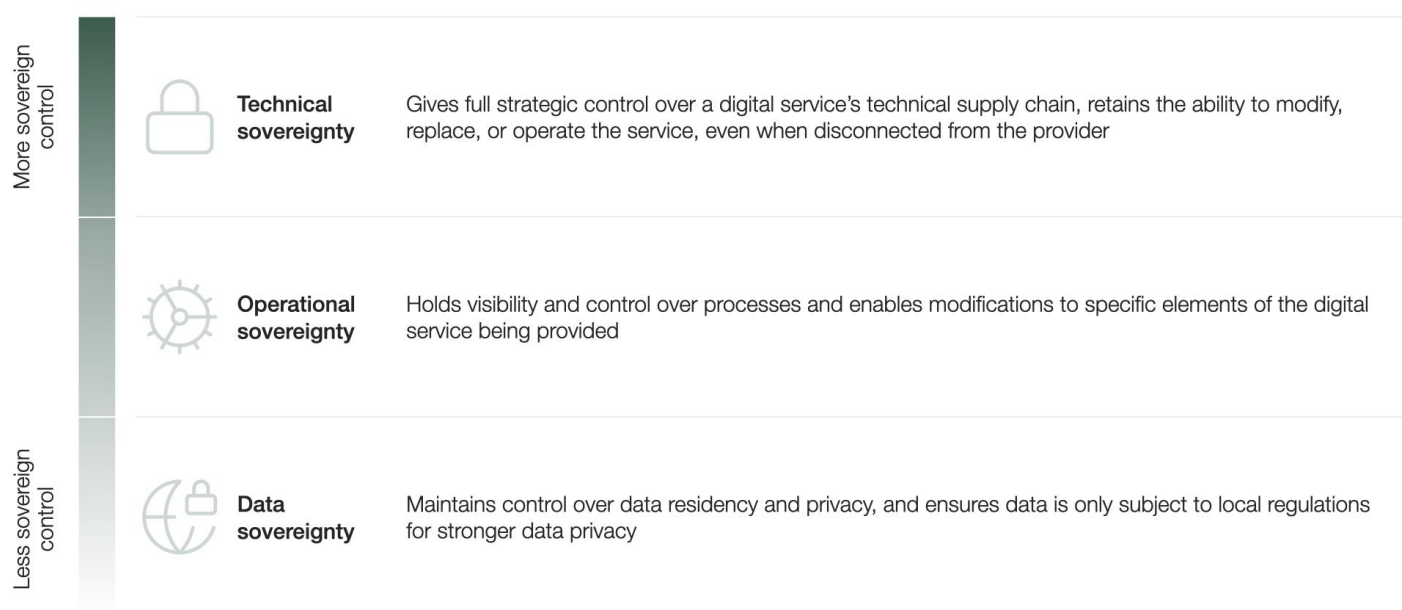
- **Data:** Critical and personal data needs to be strictly controlled, whether for practical, performance or regulatory reasons, such as compliance with the GDPR. Here, operators have experience in managing sensitive and

complex customer data requirements, including protecting patient records, financial transactions or government information;

- **Operational:** Beyond where data resides in the cloud, digital sovereignty means an organisation having domestic control, governance and accountability across its technical assets and resources. Operators aim to provide customers the freedom to choose the level of sovereignty they need, while helping them build resilience to external risks; and
- **Technical:** Full digital sovereignty also reflects the ability of an organisation to control and manage their full IT estate as a whole within national borders. Operators' portfolio of solutions, including cloud, AI, connectivity and security, can meet demands for sovereign services for critical public sector use cases.

Figure 1

The layers of sovereign control over digital services



Source: Assembly, BT, EC

The few, different interpretations of sovereignty by policymakers so far have guided some early commercial approaches

Only a select few jurisdictions have established an official definition or understanding of digital sovereignty so far. While definitions vary, there has been a common focus on establishing a framework that recognises varying degrees or layers of digital sovereignty. The issue has also attracted commercial attention from those looking to meet the increasing need for sovereign services, which mostly relates to cloud services, due to concerns over the security and privacy of how providers store and process data. Telecoms operators (such as BT in the UK, Deutsche Telekom in Germany and Swisscom in Switzerland) have been quick to offer new sovereign services via their network infrastructure, which are already critical sovereign assets that

underpin the digital economy. In doing so, operators have begun to demonstrate their own understandings of digital sovereignty.

This increasing political focus on digital sovereignty has encouraged commercial attention on the issue, particularly in the telecoms sector. Given the critical role of telecoms infrastructure in enabling the digital economy, operators are quickly becoming a necessary element of digital sovereignty. Operators have started to offer sovereign services, picking up on the increasing demand for these, especially from the public sector.

In Germany, Deutsche Telekom is building an 'AI gigafactory' to provide sovereign AI services to European manufacturers and is hoping to do so with the support of public funding from the EU. This follows the EC's commitment to funding a number of these 'AI gigafactories' in order to encourage digitally sovereign AI development.

Operators have so far tended to partner with foreign hyperscalers, to offer or develop new sovereign capabilities. For example, Deutsche Telekom, Swisscom and Telenor (Norway) have all launched projects with NVIDIA to deploy data centres with the ultimate goal of holding sovereign compute capacity to offer AI services to domestic businesses. While NVIDIA's hardware or software plays a key role in each of these developments, adding a non-sovereign actor into these operations, the operators still own the relevant infrastructure, adding at least some level of digital sovereignty, such as ensuring customer data is stored and processed locally, rather than with a foreign cloud provider per se. Recently, in February 2026, Deutsche Telekom launched its sovereign Industrial AI Cloud in partnership with NVIDIA, which is set to expand German compute capacity by 50%.^{4, 5} This additional capacity is aimed at providing companies, research institutions and the public sector in both Germany and Europe as a whole with sovereign compute for AI.

In South Korea, SK Group has become similarly invested in offering digitally sovereign services, but has done so slightly differently. SK Group, via SK Telecom and SK Broadband, is building a data centre for AWS. The project has seen significant funding committed from both sides, with investment in the data centre totalling to approximately SK₩9tn (£4.7bn). The data centre will be owned by AWS, rather than SK Group, differing from the aforementioned European examples in which the telecoms operator has owned the infrastructure element of such projects. The data centre is set to provide sovereign compute capacity to South Korean citizens and businesses, despite being owned by AWS, a non-sovereign platform.

The EU's approach to digital sovereignty



The EU's focus on sovereignty has been driven by the EC's geopolitical concerns around relying on foreign (particularly US, but also Chinese) digital platforms, services and hardware. In September 2024, the Draghi Report stressed the need for a strengthening of sovereignty in cloud and AI on competition grounds.⁶ Draghi argued that while the EU could not seek to develop significant challengers to major US cloud providers such as Amazon Web Services (AWS), Google and Microsoft, it could develop more competitive domestic markets to meet the demand for digitally sovereign solutions. In January 2026, Henna Virkkunen (EVP for Tech Sovereignty, Security and Democracy, EC) further stressed the EC's focus on digital sovereignty, arguing that the EU could not afford to be dependent on one foreign country or company for critical technologies, fearing that such dependencies could be "weaponised" against the bloc.⁷

In the upcoming proposal for a Cloud and AI Development Act (CAIDA), the EC is set to outline its understanding of digital sovereignty. It is understood the EC is considering including a benchmark of effective European control for cloud and AI providers, which it would be responsible for scrutinising. One of the main pillars of the proposed act will focus on highly critical sectors and use cases where stronger sovereign solutions are needed.⁸ It will explain that in defence programmes, public sector work and critical infrastructure, operations should be kept secure by using sovereign, EU-based cloud capacity. The EC has recognised that there are differing levels of sovereignty required for different purposes here, and has set out a framework for these that includes jurisdictional, data, and full digital sovereignty.

Germany's approach to digital sovereignty



In January 2021, the Federal IT Cooperation (FITKO) published a strategy for strengthening digital sovereignty in the public sector, which adopted a definition of digital sovereignty for the Federal Government.⁹ The strategy defines digital sovereignty as "the capabilities and possibilities of individuals and institutions to perform their roles in the digital world autonomously, confidently and safely". This definition relates to the public sector, where sovereign solutions are in higher demand for security reasons, especially in critical use cases. The strategy also establishes a number of objectives for public sector procurement of IT systems, such as having the capability to design its own IT systems, or at least participate in this design process with the provider. More recently, in March 2025, the German Government launched its own secure cloud service.¹⁰

Switzerland's approach to digital sovereignty



In November 2025, the Swiss Federal Council published a report on digital sovereignty, which has been a focus of its Digital Switzerland Strategy since 2023.¹¹ The report includes a definition of the term, an assessment of the state of digital sovereignty in Switzerland and a strategy for the Government's future approach to it. According to the Federal Council, "digital sovereignty means that a state has the necessary control and ability to act in the digital space to ensure the fulfilment of its state responsibilities".¹² The report promotes the use of open-source software to reduce vendor lock-in, launches a hybrid cloud strategy to better protect sensitive data, and announces an expected new provision in the Telecommunications Act to restrict so-called 'high-risk' equipment from telecoms networks, as is being proposed in the EU.¹³ Unlike in Germany and at the EU-level, the Swiss approach does not reference the differing levels of sovereignty that may be required in different use cases.

The benefits of sovereignty for UK organisations

A faster adoption of sovereign services will strengthen resilience and data privacy for UK businesses and the public sector

Data sovereignty can ensure stronger data privacy for the UK economy's critical sectors

Businesses operating in digital markets may have concerns over the privacy of their company or customer data when using a foreign-owned, public cloud service. As these public cloud networks are owned by foreign providers, the hosted data may be subject to legislation originating from the country these companies are based in. For example, the US' 2018 CLOUD Act, gives authorities the ability to request data held by major US cloud providers.¹⁴ Businesses may be interested in a more private cloud solution that is only subject to domestic regulation, increasing their control, visibility and certainty around the privacy of their data. Businesses without this control over their data are more likely to violate the UK's General Data Protection Regulation (GDPR), potentially incurring significant fines. For example, in Ireland, Meta was fined €1.2bn (£1bn) in 2023 over the flow of data from Facebook to the US that was in violation of the GDPR.¹⁵

When using a data sovereignty solution, businesses would have far better assurances that their data would only be subject to the laws of the jurisdiction it is located in, strengthening privacy and simplifying compliance, reducing costs for businesses. Businesses that are better able to offer a higher standard of data privacy will be a more attractive option for customers, especially against the backdrop of increasing geopolitical tensions and recent major cloud service outages. Businesses should consider the potential consequences of their dependencies on foreign digital providers, particularly in cloud services.

The adoption of services that ensure data sovereignty can support the UK economy via increased consumer confidence

Providing these more secure services can improve consumer confidence in how businesses handle data, especially if that involves their personal information. Currently, only 20% of UK adults say they feel confident about the privacy of their data and personal information.¹⁶ The UK Government has previously recognised this, explaining that to maximise the potential economic benefits of data, the public needs to be more confident about the security of their personal data and how it is being handled by UK businesses.¹⁷

CNI sectors and the retail industry would benefit most from the adoption of data sovereignty

While the adoption of data sovereignty would benefit a range of industries, it is most important in the UK's CNI sectors such as communications, emergency services, energy, finance, health, transport or water. The critical operations of businesses within these sectors require increased protection from the threat of outages, cyber incidents and any resulting data breaches. Other non-critical sectors such as retail should also look to adopt data sovereignty to better protect customer data in the event of major outages.

Operational sovereignty provides CNI sector businesses and public sector bodies with increased control over their digital services

Operational, or mid-level, sovereignty can strengthen resilience for those that need more visibility or control over the operation of their digital services. While some of the demand for operational sovereignty may come from CNI sectors in more sensitive use cases, more demand may come from the public sector, although in less critical areas. The public sector's digital operations and systems require stronger resilience and security compared to most businesses due to their own more sensitive data, the personal data of citizens they may hold and the criticality of the services they provide. Although most public sector bodies are unlikely to need the same level of security and control as specific high-sensitivity use cases such as in defence or the NHS, they are likely to need better visibility or even control over their digital services than just data sovereignty could provide. This added control is especially important in the event of a major outage or cyber incident that may impact customer services or see a surge in reliance on government digital services.

Technical sovereignty will ensure high-sensitivity government operations remain secure and detached from any external actors or services

Technical, or high-level, sovereignty is only required in very select cases such as defence, health or other highly sensitive, critical operations that involve national security in some way. In these instances, customers need full technical control of the service being provided and the ability to operate autonomously when disconnected from their service provider. The FITKO digital sovereignty strategy in Germany considered this approach a necessity for public sector use cases, requiring that public sector bodies be able to either design their own systems or at least significantly influence how a provider designs them.

The economic benefits of sovereignty for the UK

- Stronger data sovereignty could enable the UK economy to realise £18bn per year of AI's projected economic impact by giving businesses more confidence to adopt the technology;
- Sovereignty-led investment in data centres could have an economic impact of nearly £15bn by 2030;
- With data sovereignty, businesses in the UK's digital sector could avoid the risk of GDPR fines totalling £1bn;
- Growth in the sovereign cloud market in the UK over the next five years presents a £14bn commercial opportunity; and
- The adoption of operational or technical sovereignty could reduce the annual costs to the UK economy of data, IP and asset loss by £632m.

Stronger data sovereignty could enable the UK economy to realise £18bn per year of AI's projected economic impact

The UK Government has made clear, particularly through its AI Opportunities Action Plan, that it is highly optimistic about the economic growth potential of AI. When announcing this plan, Prime Minister Keir Starmer said that the productivity gains brought about by AI could be worth up to an average of £47bn per year for the next decade.¹⁸

However, despite this potential benefit, many businesses are yet to adopt AI at a significant scale, or in many cases, at all. One of the key reasons for this is due to their fears over the security, ownership, control and visibility of their data, with estimates varying between 31% and 68% of UK businesses refraining from adopting AI as a result.^{19, 20}

The adoption of stronger data sovereignty solutions could support businesses here by ensuring they have more control and visibility over their data, potentially resulting in a more widespread adoption of AI. Until such measures are adopted by businesses, we estimate that the UK economy will miss out on approximately £18bn of the UK Government's predicted yearly £47bn AI productivity benefit, restricting the UK economy from making the most of the rapidly developing AI opportunity.²¹

Sovereignty-led investment in data centres could have an economic impact of nearly £15bn by 2030

The announcements of major corporations such as Google, Microsoft and NVIDIA reflect the surging investment in data centres and associated infrastructure in the UK. The Government itself, through its AI Growth Zones initiative, underlined that “onshore data centre capability is essential for protecting sensitive data, maximising AI adoption benefits, and ensuring resilience from global shocks”.²²

In light of current projections, annual data centre investment in the UK could reach close to £12bn by the end of the decade.²³ With the prioritisation of operational sovereignty likely to drive demand for localised AI and cloud compute capabilities and physical infrastructure, we consider that this could encourage some additional investment into data centres between 2025-2030. Based on a conservative multiplier effect, we estimate that this additional investment could therefore lead to a total economic impact worth £14.6bn by the end of the period.²⁴

With data sovereignty, businesses in the UK’s digital sector could avoid the risk of GDPR fines totalling £1bn

Data sovereignty’s primary function is to ensure data remains within the country of its origin, therefore only being subject to the laws of that jurisdiction. Under the UK’s GDPR, there are strict rules around the international transfer of data to certain countries that do not have data protection regimes that are considered strong enough. Across the EU, infringements of this rule have seen some of the most significant GDPR fines such as the Irish Data Protection Commission’s fines of €1.2bn (£1bn) on Meta and €530m (£450.4m) on TikTok in 2023 and 2025, respectively.^{25, 26}

The adoption of data sovereignty solutions can better protect businesses against the risk of incurring such fines under the GDPR. Currently, estimates show that only 35% of UK businesses have full visibility into where their data is stored, processed and governed.²⁷ Of the approximately 65% of businesses without this visibility, we estimate that a notable proportion of these could be at risk of breaching the GDPR’s rules around the transfer of international data.

We estimate that in the UK’s digital sector alone, if even 10% of these at-risk businesses were deemed in breach of the GDPR by the Information Commissioner’s Office (ICO), the collective fines could accumulate to approximately £1bn based on the ICO’s methodology for calculating such penalties.²⁸

Growth in the sovereign cloud market in the UK over the next five years presents a £14bn commercial opportunity

The global sovereign cloud market is projected to expand at pace during the course of the decade, with security, privacy and compliance needs all supporting growing momentum. Demand for cloud services that offer data sovereignty, for example by ensuring data is managed according to local legislation and not transferred across borders without consent, is expected to be particularly strong, with 44% of technology leaders currently wary of using the public cloud over concerns around data security.²⁹

The adoption of operational or technical sovereignty could reduce the annual costs to the UK economy of data, IP and asset loss by £632m

According to our estimates, the sovereign cloud market in the UK – which accounts for a meaningful share of the wider European market – could see growth of more than 230% over the 2025-2030 period.³⁰ For data sovereignty specifically, this expansion presents providers with a potential commercial opportunity worth over £13.6bn.³¹

Major cloud outages and cyber incidents can cause significant costs to businesses in a variety of areas including the cost of losing data, IP or other digital assets. A study commissioned by the UK Government estimates that in 2024, with a higher-end estimate, these losses cost the UK approximately £8.5bn, or £1bn with a lower-end estimate.³²

With stronger digital sovereignty, businesses would likely be able to better protect their data, IP and digital assets, potentially reducing this cost. Studies show that businesses can reduce the costs of such losses by implementing stronger controls that enable better visibility over each component of their digital architecture, potentially by as much as 20.5%.^{33, 34}

When adopting data sovereignty solutions, businesses would be able to benefit from some of this cost reduction, but not all of it, as this level of sovereignty only provides added control and visibility over data, rather than control over a business' full set of digital services and/or systems. We estimate that the adoption of data sovereignty could reduce the annual economic cost of data losses following outages and cyber incidents by approximately £316m (based on 2024 figures).

However, with the use of operational or technical sovereignty solutions, we predict that businesses would be more likely to benefit from the full potential cost reduction. Operational and technical sovereignty provide businesses with the ability to control and modify the processes within their digital services and/or systems. In the case of technical sovereignty, businesses would even be able to continue operating these systems in the event of a wider outage. In these instances, we estimate that the annual economic cost of data, IP and asset losses could be reduced by up to £632m.³⁵

How the UK Government can seize the opportunity of digital sovereignty

While the Government has established a Sovereign AI Fund of £500m, it has not yet set out a policy-based approach to digital sovereignty.³⁶ For example, the Government has not defined a set of requirements or recommendations relating to digital sovereignty at an enterprise level that could be used to drive demand for sovereign digital services.

Of the few jurisdictions that have established understandings or definitions of digital sovereignty, most have recognised that there can be different levels or layers of sovereignty. For example, the EC's five tiers of different digital sovereignty layers highlight the differing degrees of sovereign control that can be held over digital services. By doing so, businesses are given a clear signal about the importance of the issue, but also a framework for where there is likely to be demand for sovereign services, as have begun to be offered by operators. The UK Government should look to establish its own clear framework and understanding of digital sovereignty to provide a better picture of the issue to businesses. Without such an intervention, the UK risks missing out on a host of economic benefits that could be driven by increased demand for sovereign digital services.

This is also an area in which the UK Government could align with the EU in some areas (as has become a policy target of the UK Government recently³⁷), while also diverging from it in other areas. For example, the UK could look to align with the EC's aforementioned plans to detail which critical national infrastructure (CNI) sectors may benefit from adopting sovereign services for resilience and security-related reasons. However, the EC's current framework will be modified by the CAIDA, which is expected to establish a stricter approach to digital sovereignty that risks reducing the continent's access to some of the best tech and digital services that are provided by foreign firms, often those from the US. This is where the UK could diverge slightly, adopting a less stringent framework that encourages businesses to use more sovereign digital services and details where it may be beneficial to do so, while still maintaining a more positive and open relationship with major foreign hyperscalers that can make significant contributions to the UK's economic growth.

The Government's limited focus on the policy side of digital sovereignty risks leaving businesses without an adequate understanding of how current

geopolitical tensions may impact cloud services that are essential for large parts of the UK economy. Inaction from the Government creates uncertainty, potentially limiting investment and harming business confidence. The Government also risks failing to benefit from the development of a new market for sovereign services, which we estimate could be worth almost £14bn by 2030, potentially boosting the UK's economic growth. Without intervention or clarity on the issue, demand for sovereign services will be limited. The creation of a framework for understanding the issue, and where businesses may need to take it into consideration could open up a new avenue for economic growth.

Four government policy interventions could encourage the adoption of sovereign services

There are four actions the Government should consider taking in parallel to support demand for secure and reliable domestic digital services:

1. Outline a framework for sovereignty;
2. Highlight sectoral requirements for digital sovereignty;
3. Make use of natural convening powers; and
4. Revise procurement rules and practices.

The UK Government's focus on sovereignty is beginning to intensify, considering how it can be implemented across the economy to ensure sufficient control over crucial elements of supply chains, as well as how the country can capture the benefits (e.g. investment) of frontier technologies, such as AI. However, the Government has so far not been as forthcoming as its EU counterparts in seeking to reach a view on requirements for an enterprise level of sovereignty and where it is needed, and how policymakers can facilitate it. While a hard and fast definition may be unnecessarily prescriptive, **a framework for digital sovereignty** in the UK could help build general consensus around its importance and application.

Building on that framework, and recognising that not every organisation will require the 'highest grade' of digitally sovereign solutions, it may be instructive for the market that the Government nevertheless identifies **critical sectors** – or layers or processes within them – where such digitally sovereign services could be needed most. Doing so would help to ensure that appropriate steps were taken in different sectors to maintain security and resilience, as well as helping to inform market needs for those looking to invest in new sovereign products.

The Government may also have a role to play in supporting the commercialisation of homegrown sovereign services by using its **natural convening powers**. The UK has traditionally operated as an open economy and domestic organisations should not be expected to forego foreign suppliers whose products may best fit their needs (and/or budget). However, the Government is well positioned to connect the supply side of the market to relevant customers on the demand side, with the effect of creating opportunities to scale the UK tech sector. The UK Sovereign AI Industry Forum,

Assembly

is a first step in this regard, bringing together leading UK businesses to develop and deploy the technology across the country.

A possible complementary policy lever could then relate to the revision of certain **procurement rules and practices**. The UK is unlikely to go as far as the EU might in regulating for sovereignty, or follow the lead of certain Member States (e.g., France and Germany) that have over the past decade enacted sovereign cloud requirements. However, regulation and policy could be influential in driving demand for sovereign offerings. For instance, a voluntary sovereign procurement framework could be established. This would not explicitly limit options for UK businesses, but may act as a signal for them to invest more in sovereign services. Stimulating this demand could boost growth in the UK's digital services sector, supporting the Government's overarching national growth mission.

Endnotes

1. Economic Impact of Intellectual Property and Knowledge Assets Theft from Cyber Attacks in the UK, Alma Economics, 2025
2. Cloud Sovereignty Framework, EC, 2025
3. Turn compliance into competitive advantage with digital sovereignty, BT, 2026
4. Industrial AI Cloud, Deutsche Telekom, 2026
5. Germany's first AI factory for industry officially goes into operation in Munich, Deutsche Telekom, 2026
6. The future of European competitiveness, Mario Draghi, 2024
7. EU tech chief sounds alarm over dependence on foreign tech, POLITICO, 2026
8. Cloud and AI development act briefing, European Parliament, 2025
9. Strategy for strengthening the digital sovereignty of public administration IT, FITKO, 2021
10. Germany launches government cloud, BMI, 2025
11. Federal Council adopts report on Switzerland's digital sovereignty, The Swiss Federal Council, 2025
12. The Swiss approach to digital sovereignty, Assembly Research, 2025
13. Revising the EU's Cybersecurity Act, Assembly Research, 2026
14. CLOUD Act, US Congress, 2018
15. Data Protection Commission announces conclusion of inquiry into Meta Ireland, Irish Data Protection Commission, 2023
16. Public Attitudes on Information Rights Survey 2025, ICO, 2025
17. Unlocking the power of data in the UK economy and improving public confidence in its use, DSIT, 2023
18. Prime Minister sets out blueprint to turbocharge AI, UK Government, 2026
19. The digital sovereignty revolution: What UK businesses need to know, Civo, 2025
20. AI Readiness Report, ANS, 2025
21. The missed benefit is based on the estimated number of businesses refraining from adopting AI due to data security concerns and on the UK Government's estimate of

AI's potential economic benefit, adjusted according to the private sector's contribution to the UK's annual GVA.

22. Delivering AI Growth Zones, DSIT, 2025

23. The total level of investment in 2030 is based on external projections of data centre investment between 2025-2029, with the average growth rate over this period then applied for one further year.

24. The economic impact is based on applying a multiplier effect of 1.7 to an elevated level of data centre investment over the period out to 2030.

25. Data Protection Commission announces conclusion of inquiry into Meta Ireland, Irish Data Protection Commission, 2023

26. Irish Data Protection Commission fines TikTok €530 million, Irish Data Protection Commission, 2025

27. The digital sovereignty revolution: What UK businesses need to know, Civo, 2025

28. Data Protection Fining Guidance, ICO, 2024

29. Accelerating Europe's AI adoption: The role of sovereign AI, McKinsey, 2025

30. The growth rate is based on the assumption that the UK continues to account for the same share of the European sovereign cloud market in 2030 as it is estimated to represent in 2025.

31. The potential opportunity is based on external projections of the growth of the overall global and European sovereign cloud markets, subsequently rationalised downwards to reflect the share of that opportunity expected to be relevant to data sovereignty specifically.

32. Economic Impact of Intellectual Property and Knowledge Assets Theft from Cyber Attacks in the UK, Alma Economics, 2025

33. IBM Cost of a Data Breach 2022 – Highlights for Cloud Security Professionals, Cloud Security Alliance, 2022

34. Zero Trust, National Cyber Security Centre, 2026

35. Our estimates for the reduction in IP, data or asset loss costs are based on external estimates for the cost reduction when using 'zero trust' cybersecurity architecture, of which we assume would be equivalent to implementing operational or technical sovereignty. For data sovereignty, we assumed that only half of this cost reduction would be realised due to the more limited control offered.

36. Sovereign AI, UK Government, 2026

37. Chancellor's growth plan sets key principles for UK-EU alignment, UK Government

Important notice

By accepting this research, the recipient agrees to be bound by the following terms of use. This research has been prepared by Assembly Research Limited and published solely for guidance and general informational purposes. It may contain the personal opinions of analysts based on research undertaken. Assembly Research Limited gives no undertaking to provide the recipient with access to any additional information or to update or keep current any information or opinions contained herein. The information and any opinions contained herein are based on sources believed to be reliable but the information relied on has not been independently verified. Assembly Research Limited, its officers, employees and agents make no warranties or representations, express or implied, as to the accuracy or completeness of information and opinions contained herein and exclude all liability to the fullest extent permitted by law for any direct or indirect loss or damage or any other costs or expenses of any kind which may arise directly or indirectly out of the use of this research, including but not limited to anything caused by any viruses or any failures in computer transmission. The recipient hereby indemnifies Assembly Research Limited, its officers, employees and agents and any entity which directly or indirectly controls, is controlled by, or is under direct or indirect common control with Assembly Research Limited from time to time, against any direct or indirect loss or damage or any other costs or expenses of any kind which they may incur directly or indirectly as a result of the recipient's use of this research.

© 2026 Assembly Research Limited. All rights reserved. No part of this research may be reproduced or distributed in any manner including, but not limited to, via the internet, without the prior permission of Assembly Research Limited. If you have not received this research directly from Assembly Research Limited, your receipt is unauthorised.

Assembly

36 Spital Square
London
E1 6DY
United Kingdom

+44 20 3026 2700
info@assemblyresearch.co.uk