techUK
FOR WHAT COMES NEXT



Protecting Sovereignty Through Partnership

November 2026

Executive Summary: CADA, Sovereignty at What Expense?

After decades of increasingly free trade, stresses to the international trading system, combined with the COVID-19 pandemic and Russia's war of aggression in Ukraine, have caused governments around the world to place a greater emphasis on sovereignty, security, and resilience. In response to this changing landscape, many governments are seeking to reduce their interdependency risks, restrict international technology flows, and develop their own domestic innovation and technology capability.[1]

In response to these domestic desires and external pressures, the EU has developed its own Technological Sovereignty Package – comprised of two legislative proposals, the *Chips Act 2.0* and the *Cloud and AI Development Act (CADA)*.[2] While the package as a whole is commendable in its attempt to address technological dependency risks, the means it proposes risk wider, unintended damage. This includes imposing significant costs on the digital economies of essential global partners like the UK, disrupting EU supply chains, and inhibiting the productive capacity of critical institutions.

The protectionist policies found throughout the EU's proposed Technological Sovereignty Package are perhaps most evident in CADA – the central pillar of the package. CADA is designed with the legitimate and important goal of reducing the EU's dependence on foreign cloud and AI services and infrastructure, while promoting innovation and strengthening the domestic cloud and AI service industry. However, to achieve these ends, CADA effectively closes off key parts of the public sector, an important facet of the European cloud services market, to foreign competition, including from essential digital and security partners like the UK.

This paper examines the potential impact that CADA might have on the UK economy – modelling two scenarios: a low and a high-impact scenario. We find that CADA would cost the UK between **£19.55 billion** and **£22.34 billion** over the next five years. This is the estimated equivalent of between **41% and 47% of projected UK GDP growth** over the 5-year period. However, these estimates likely understate the true costs of CADA to the UK as they do not account for the significant compliance costs many UK businesses will face when attempting to meet the standards of CADA's lower assurance levels.

The sheer scale of this damage to the UK's digital economy will also harm the EU. Excluding the UK will not strengthen the EU's technology sovereignty and the EU's digital sector will not capture the UK's losses as gains. This is because the UK remains a central pillar of Europe's innovation and technology ecosystem. Decades of cooperation have created dense business networks and digital supply chains that criss-cross the English Channel. Many EU companies have critical operations in the UK and many UK firms provide essential services within the EU, offering a rare alternative to less dependable international partners.

1 "OECD Science, Technology and Innovation Outlook 2023," OECD, 2023, https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/03/oecd-science-technology-and-innovation-outlook-2023_fb6e6c20/0b55736e-en.pdf

2 "Commission proposes tech sovereignty package to strengthen Europe's digital autonomy and resilience," *European Commission*, 2026-06-02, https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1187

The interdependence between the UK and the EU reflects CADA's fundamental misstep. Complex global value chains have rendered it not only extremely difficult but also harmful to attempt to isolate and build supply chains based on national boundaries. Attempting to do so will not only force critical EU public functions to rely on subpar technology solutions, but may also impact the productive capacity of EU digital firms.

It is essential that the EU acts to prevent this damage to the interconnected and interdependent UK-EU digital and technology sector. To do this, techUK recommends that:

- **The EU designates the UK as a recognised third-country provider and a trusted partner from Day One.** There should be no doubt about the importance of the UK to the EU's technological future and the entire continent's security. Policy should be built from the ground up around the importance of protecting and deepening the mutual value that comes from this irreplaceable economic and security relationship.
- More broadly, the **EU should focus on technical security assurances to protect sovereignty**. Measures such as customer-exclusive keys, zero-retention policies, data portability requirements, and service continuity planning do more to practically protect security and resilience than attempts at national control.
- Likewise, the **EU should remove blanket citizenship requirements for technology workers**. These are unrealistic given the nature of the technology workforce, and duplicate preexisting EU and member state rules where citizenship requirements already exist for dealing with classified information and data. If these rules are not already in place for the services covered by CADA, the personnel screening to agreed standards should be sufficient protection.



Cloud and AI Development Act (CADA): A Protectionist Approach to Sovereignty

It is no surprise that strengthening Europe's sovereignty, security, and resilience have each become higher priorities for leaders in the EU and in the UK. Strained international relationships, global security threats, and increased economic and technological interdependence have created a fundamentally changed landscape to that of only a decade ago. As Prime Minister Andy Burnham has argued, we now live in a "darker world" that requires new approaches.[3]

The Technological Sovereignty Package, proposed by President von der Leyen in June 2026, is a central plank of the European Commission's attempt to strengthen the EU's position. The package is comprised of two legislative proposals, the *Chips Act 2.0* and the *Cloud and AI Development Act (CADA)*, as well as an *Open Source Strategy* and a *Strategic Roadmap for Digitalisation and AI in Energy*.[4] Combined, these measures seek to secure critical supply chains, and then "reinforce a 'European way' to technological sovereignty." [5]

However, while the package is aimed at addressing very real dependency risks, the means it proposes go far beyond strengthening the EU vis-à-vis undependable partners. As currently written, it will impose significant costs on the UK's digital sector, which is tightly integrated with the EU. This relationship means harm to one partner risks undermining the EU and UK's shared security.

The package as a whole takes what Bruegel Senior Fellow Mario Mariniello calls a "protectionist turn."[6] This is most apparent in CADA, the central pillar of the package. It is designed with the legitimate and important goal of reducing the EU's dependence on foreign technology, particularly cloud and AI services and infrastructure, while promoting innovation and strengthening the domestic cloud and AI service industry. However, to achieve these ends, CADA closes off critical components of the European cloud services markets – namely the public sector – to essential foreign firms like those in the UK.

3 Andy Burnham, "We must rebuild Britain's hard power to face a darker world," *The Times*, 2026-07-08, https://www.thetimes.com/uk/politics/article/andy-burnham-defence-nato-investment-rebuild-bc7rnr5l5

4 "Commission proposes tech sovereignty package to strengthen Europe's digital autonomy and resilience," *European Commission,* 2026-06-02, https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1187

5 "Shifting away from dependency: The EU's Tech Sovereignty Package," *Freshfields*, 2026-06-30, https://www.freshfields.com/en/our-thinking/blogs/technology-quotient/shifting-away-from-dependency-the-eus-tech-sovereignty-package-102n7kn

6 Mario Mariniello, "To achieve tech sovereignty, Europe must not mimic its rivals," *Bruegel*, 2026-06-11, https://www.bruegel.org/first-glance/achieve-tech-sovereignty-europe-must-not-mimic-its-rivals

CADA's Risk-Based Sovereignty Framework

CADA's proposed risk-based "cloud computing sovereignty framework" is made up of **four assurance levels** [Box 1] that outline the level of sovereignty required for cloud and AI service providers to do business with EU public entities. The higher the level, the more demanding and restrictive the cumulative sovereignty, security, and control requirements. The higher assurance tiers for cloud service providers are intended to apply to more sensitive activities and domains, such as national security, border management, defence, justice, and law enforcement. In the Commission's estimate, only 1% of public procurement use cases will require Assurance Level 4 and 9% will fall under Level 3. The vast majority would fall under Level 1.[7]

UK cloud-computing firms, and firms in the wider cloud services supply chain, may qualify for EU public contracts under Levels 1 and 2 with certain safeguards in place – bearing significant compliance costs given the amount of audit evidence required. Level 3 contracts will be very difficult, if not impossible, for UK firms to qualify for, and Level 4 contracts are virtually off the table. Many UK digital firms already face EU-ownership eligibility rules through programs like the Digital Europe Program as well as various EU public tenders. CADA risks entrenching and even extending existing restrictions, which will harm both the UK and the EU.

Box 1: EU Cloud Sovereignty Assurance Levels

	Description	Examples
Assurance Level 1	Data is processed and stored in infrastructure in the EU	Provider and relevant subcontractors that are subject to the control of a third country which guarantees no existing laws and practices that require the cloud computing service provider to report information on software vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited.
Assurance Level 2	Providers demonstrate independence from third countries and transparency over software supply chain	Provider and relevant subcontractors that are subject to the control of a third country demonstrate strong safeguards (e.g. no third-country ability to restrain or restrict service delivery).
Assurance Level 3	Providers owned and controlled from the EU and meet additional criteria (e.g. personnel citizenship)	Provider and relevant subcontractors are not subject to the control of a third country or a legal entity established in a third country (exceptions apply to EU "associated" third countries).
Assurance Level 4	Providers have full transparency and control over their software supply chain and no interference from a third country	Provider and relevant subcontractors are not subject to the control of a third country or a legal entity established in a third country (no exceptions apply).

7 "Impact Assessment Report," *European Commission*, 2026-06-03, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52026SC0502



However, under Article 18 of CADA, the Commission may determine that third countries whose regimes are seen as compatible with Level 3 could qualify for Level 3 assurance levels. Even without this determination, a very small subset of UK firms might still be able to qualify for level 3 assurance levels.[8]

Bolstering EU Data Centre Capacity

A secondary element of CADA is focused on building out the EU's compute infrastructure. The Commission has determined that the EU's limited data centre capacity poses a significant threat to their domestic technology industries given the need for most EU firms to route critical workloads through foreign hyperscaler infrastructure. In their estimates, demand is going to continue to significantly outstrip supply by 2036, with a 20 GW gap in their baseline scenario. This will make the region less competitive than those with abundant, low-cost compute resources.

The Commission aims to **triple** the EU's data centre capacity by 2030, with the goal to close the compute capacity gap by 2035. Through CADA, it seeks to simplify and accelerate the approval and deployment processes for data centres and to improve access to key resources such as energy, land, water, and financing.[9]

8 "Impact Assessment Report," *European Commission*, 2026-06-03, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX-:52026SC0502

9 "Impact Assessment Report," *European Commission*, 2026-06-03, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX-:52026SC0502

CADA's Potential Impact on the UK Digital Economy

Exclusion from CADA would have far-reaching impacts on the UK's digital sector and broader economy, and by extension the EU. As techUK's recent report, *Towards a UK-EU Partnership for a New Age*, argued, the UK and EU are inextricably bound together when it comes to their digital economies and broader technology and innovation ecosystems.[10] Their bilateral trade in digitally deliverable services was worth over £274 billion in 2024, and the UK is one of the continent's most innovative digital partners and an irreplaceable security partner.

In 2025, the UK exported an estimated £149 billion in digitally delivered services to the EU alone.[11] Roughly £100 billion of that is either delivered via cloud services, includes AI elements, or has cloud or AI components in their supply chain. Given their long history of collaboration and shared strategic threats, the UK and the EU have together described how they "share a responsibility for the security of Europe" and their security and prosperity are "closely interconnected and interdependent."[12]

The European Commission frames the level of exclusion under CADA assurance levels 3 and 4 as minimally impactful for external trading partners like the UK. However, in practice exclusion will have wide-reaching impacts given the integration between the UK and the EU digital sectors, combined with the prominent role public procurement plays across the EU economy and the breadth of CADA's assurance levels. They apply to "cloud computing services" as defined in the Network and Information Security (NIS2) Directive. This encompasses: "a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations."[13] As well as direct hyperscaler offerings, the result is that SaaS, IaaS, and PaaS are also broadly included under "cloud computing services."[14]

Therefore, taking the European Commission's estimate that 10% of EU public procurement will be covered by Levels 3 and 4, given the scale of UK digital exports to the EU, and the fact that public procurement constitutes an estimated 15% of EU GDP, the potential impacts of CADA's restrictions on the UK are significant.[15]

10 "Towards a UK–EU Partnership for a New Age," *techUK*, 2026-09-10, https://www.techuk.org/insights/reports/techuk-report-towards-a-uk-eu-partnership-for-a-new-age

11 Orbit Policy calculations, "Digitally delivered services trade dataset," *WTO*, 2026-07, https://www.wto.org/english/res_e/statis_e/gstdh_digital_services_e.htm

12 "Security and defence partnership between the European Union and the United Kingdom of Great Britain and Northern Ireland," *UK Government*, 2025-05-19, https://www.gov.uk/government/publications/uk-eu-security-and-defence-partnership/security-and-defence-partnership-between-the-european-union-and-the-united-kingdom-of-great-britain-and-northern-ireland

13 "DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," *EUR-Lex*, 2022-12-14, https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

14 "Cloud computing service," *Precursor*, 2026-09-15, https://cybersecurityandresiliencebill.com/glossary/cloud-computing-service

15 "Commission publishes evaluation of EU Public Procurement Directives," *European Commission*, 2025-10-14, https://single-market-economy.ec.europa.eu/news/commission-publishes-evaluation-eu-public-procurement-directives-2025-10-14_en

However, the European Commission likely underestimates the magnitude of CADA's potential impacts over time. The incentive structures inherent in CADA make it likely that EU incumbents will push for more protected market access for public contracts. Over time, UK firms will be pushed out of a greater proportion of EU public contracts as more activities fall under the higher sovereignty assurance level buckets.[16] The EU Commission also anticipates that the sovereignty measures and assurance levels outlined in CADA will be mirrored to some extent by the private sector, in particular in highly regulated sectors.[17] Combined, these factors significantly exacerbate the potential risks and impacts of CADA on the UK.

Furthermore, the total cost to the UK extends well beyond lost contracts. It also requires an examination of the significant compliance costs UK firms would face to meet the standards of even the lower levels of CADA's risk assurance framework. UK firms seeking to do business with many EU public and private organisations would be required to conduct complex annual audits of international supply chains and shareholders, as well as undertake potentially costly reorganisations of global value chains. This process will result in higher costs, significant delays in contract decisions, and will likely deter many UK firms, particularly SMEs, from seeking qualification under the framework. It also fosters an uneven competitive environment between UK and EU firms by adding additional complexities for UK firms.

Finally, CADA's efforts to significantly bolster EU data centre capacity – with the goal of tripling data centre capacity over 5 to 7 years – have the potential to crowd out foreign direct investments across the UK. With an announced pipeline of £36.4bn in UK data centre investments from 2025 to 2028, diversion of data centre investments of any magnitude could have sizable economic consequences.[18]

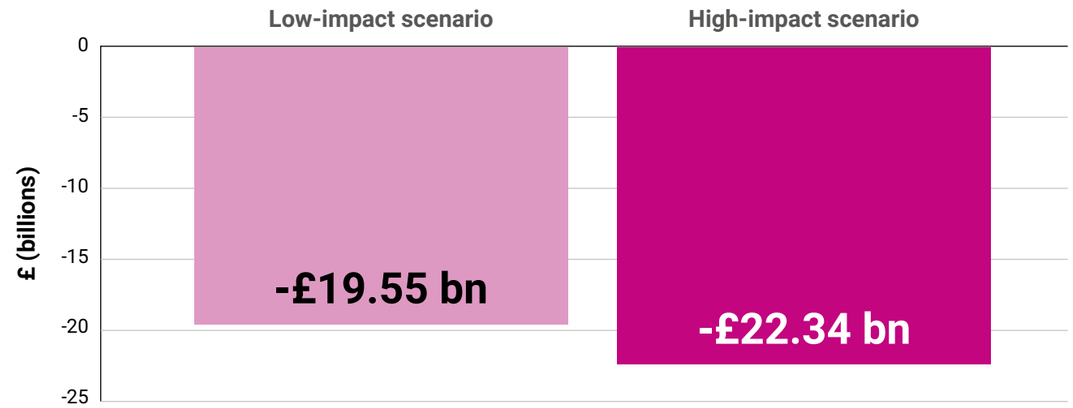
Estimated Impacts of CADA on the UK

In our illustrative model, we attempt to isolate the significant, far-reaching impact that CADA may have on the UK economy by outlining potential scenarios and highlighting their potential economic impacts. This model is not meant to be prescriptive, but rather to be used as a tool to help understand the interdependencies of the digital economy and outline the potential impacts CADA may have on the UK.

While initially CADA may have a relatively small impact on the UK economy, its effects will compound over time. We outline two five-year scenarios and highlight the cumulative impact on the UK's economy. In the **low-impact scenario** [Box 2], CADA has the potential to cost the UK economy **£19.55 billion** over 5 years. In a **high-impact scenario**, CADA has the potential to cost the UK economy **£22.34 billion** over 5 years. These losses represent between an estimated **41% and 47% of UK GDP growth** over a five-year period, assuming a conservative average annual GDP growth of 1.3% over the period.

It is important to note that this model is meant only to be illustrative and is likely an **underestimation of the total cost of CADA on the UK**. We applied relatively conservative assumptions as inputs into the model to avoid significant overestimation [see Appendix A for a more detailed methodology], and critically the model does not take into account the significant compliance costs to UK businesses associated with annual audits and potential supply chain reorientation to meet lower assurance levels.

UK 5-Year Compound GDP Loss, CADA



Box 2: Model Scenarios

	Description	5-year compound impact
Low-tier scenario	In the first year 10% of EU public sector cloud and AI contracts fall under the highest assurance levels – with an estimated contract loss of 90% at assurance level 3 and 100% at level 4 – combined with an estimated 10% of the UK's data centre foreign direct investment at risk of being diverted to the EU. By the second year, EU incumbent pressures result in a higher proportion of public AI and cloud contracts falling under the highest assurance levels; ultimately 15% of EU public cloud and AI contracts require assurance levels 3 and 4. This proportion remains constant for the rest of the five-year period, however, by years 3 and 4, the private sector adopts just 5% of CADA's restrictions. This increases to 10% by year 5.	**-£19.55 billion** over 5 years
High-tier scenario	In the first year 10% of EU public sector cloud and AI contracts fall under the highest assurance levels – with an estimated contract loss of 90% at assurance level 3 and 100% at level 4 – combined with an estimated 10% of the UK's data centre foreign direct investment at risk of being diverted to the EU. By the second year, EU incumbent pressures result in a higher proportion of public AI and cloud contracts falling under the highest assurance levels; ultimately 15% of EU public cloud and AI contracts require assurance levels 3 and 4. The private sector adopts 5% of CADA's restrictions. In years 3 and 4, public sector contract loss increases to 20% of year 0 and the private sector continues adopting 5% of CADA's restrictions. By year 5, this increases to 10%.	**-£22.34 billion** over 5 years

16 Mikołaj Barczentewicz, "Europe's Sovereignty Stack: CADA, Compute, and the Limits of Autarky," *International Center for Law & Economics*, 2026-06-15, https://laweconcenter.org/resources/europes-sovereignty-stack-cada-compute-and-the-limits-of-autarky/

17 Mikołaj Barczentewicz, "Europe's Sovereignty Stack: CADA, Compute, and the Limits of Autarky," *International Center for Law & Economics*, 2026-06-15, https://laweconcenter.org/resources/europes-sovereignty-stack-cada-compute-and-the-limits-of-autarky/

18 "Data Centre Programme - What we achieved in 2025," *techUK*, 2026-01-21, https://www.techuk.org/insights/news/data-centre-programme-what-we-achieved-in-2025

CADA: Missing the Mark and Harming the EU in the Process

In addition to its impacts on essential partners like the UK, CADA will also fail to have its intended impact and likely harm EU firms and public authorities in the process. This is due to two interrelated factors: the reality of complex advanced technology global value chains and the conflation of nationality with security.

While European countries hold many advantages, they also occupy a particularly weak position in the global value chains of advanced technologies such as semiconductors and AI. Many of the major breakthroughs in these technologies were pioneered by Europeans, and Europe is home to globally leading companies, such as ARM in the UK and ASML in the Netherlands. However, European countries are laggards when it comes to production, and as of 2022, were dependent on foreign countries for 80% of their digital products, services, infrastructure, and intellectual property.[19]

The AI value chain is dominated by the US and China, with both countries outpacing Europe and the rest of the world when it comes to talent, IP, capital, energy, data, and critically, compute.[20] The compute gap is particularly stark. By one estimate, as of May 2025, the US alone was home to almost 75% of global GPU cluster performance, followed by China with 14%. Despite accounting for 18% of the global economy, the EU makes up just 4.8% of the world's global GPU performance.[21] Europe's low relative share of global compute drastically understates European dependence on foreign states for the resources to train and deploy AI. Three non-EU hyperscalers control over 70% of the European cloud market, with the market share for EU providers declining from 2017 to 2022 despite significant growth in the overall market.[22]

However, this picture is even more complex. The companies operating within these value chains are never solely nationally bounded. Where a company is headquartered is often unrelated to ultimate ownership – even EU headquartered and owned firms often have critical operations outside the EU. Furthermore, leadership, researchers, and operational staff are made up of multiple nationalities, while R&D and production often take place across numerous countries.

This is where CADA's higher-tier requirements, namely that companies must be based within the EU, fully control their supply chains, and all personnel must be EU nationals, are particularly problematic. It is a central flaw of CADA's approach that it mistakes nationality for security.

Take, for example, ASML, which is headquartered in the Netherlands and is one of Europe's few globally essential tech companies. However, ASML's two largest shareholders are US asset managers and key parts of its extreme-ultraviolet lithography (EUV) machines are made in San Diego, California, and other critical operations take place in Wilton, Connecticut.[23] Even more critically, ASML's EU headquarters did not prevent the USA imposing sweeping export controls on the company that banned sales of EUVs to China.[24] ASML's equipment incorporates US technology, bringing it under the jurisdiction of the Foreign Direct Product Rule – an instrument that is also being used along with others to restrict access to AI models.[25] Nationality alone offers little security in these circumstances.

A similar dynamic plays out when looking at talent. The nationality of personnel is a poor proxy for trust, and one that is likely impossible for any firm to deliver. This is even more true in cutting-edge areas like AI. Recent analysis highlights how only 9% of top AI researchers were educated in the EU, while far fewer remained in the EU after their studies.[26] These findings are replicated even beyond the elite workforce. Other research has emphasised that "European countries are experiencing a significant loss of both national AI talent and the international talent they nurture."[27] European countries are heavily dependent on foreign nationals and the EU's tech sector could not function or be internationally competitive without international talent.

A focus on nationality is further complicated when examining the deeply integrated UK-EU technology and digital relationship. London alone is one of the largest tech talent and startup hubs in the world – the value of London's tech ecosystem being more than the next four European ecosystems combined. Many companies have shared UK and EU ownership, and significant operations across both [See Box 3 overleaf]. The UK is also central hub for European technology talent and has become a magnet for attracting leading AI researchers around the world.[28] Forcibly severing those ties would be profoundly counterproductive.

Ultimately, any attempts to separate EU companies from the global value chain and onshore all operations into the EU will ultimately hurt innovation and productivity within the EU digital sector. Economic research has long highlighted how protectionist measures reduce innovation and harm long-term competitiveness.[29] Furthermore, limiting EU public sector entities in some of the most sensitive and important areas to only EU providers raises real risks of EU entities being required to use inferior technology options, and having less secure ongoing defences from threats as a result.

Interdependence between trusted partners such as the UK and EU is essential to supporting security and resilience. It is very different conceptually and practically from one-sided dependence that creates leverage and vulnerability. As constructed CADA attempts to address the latter while devastating the former. It will leave the EU and the UK worse off and less secure as a result.

19 Paul Timmers, "Digital Industrial Policy for Europe," *Centre on Regulation in Europe*, 2022-10, https://cerre.eu/wp-content/uploads/2022/12/Digital-Industrial-Policy-for-Europe.pdf

20 Nikolaus Lang et al., "The Great Divide: How the US and China Are Splitting the AI World," *BCG*, 2026-06-30, https://www.bcg.com/publications/2026/us-and-china-ai-strategy-causing-global-ai-divide

21 "Strengthening the single market in a new geoeconomic context," *European Council*, 2026-08-19, https://www.consilium.europa.eu/en/european-council/president/strengthening-the-single-market-in-a-new-geoeconomic-context/; Konstantin F. Pilz et al., "The US hosts the majority of GPU cluster performance, followed by China," *Epoch AI*, 2025-06-05, https://epoch.ai/data-insights/ai-supercomputers-performance-share-by-country

22 "COM(2026) 502 final," *European Commission*, 2026-06-03, https://eur-lex.europa.eu/resource.html?uri=cellar:6e73e2db-5f40-11f1-aa6d-01aa75ed71a1.0001.02/DOC_1&format=PDF

23 Mikołaj Barczentewicz, "Europe's Sovereignty Stack: CADA, Compute, and the Limits of Autarky," *International Center for Law & Economics*, 2026-06-15, https://laweconcenter.org/resources/europes-sovereignty-stack-cada-compute-and-the-limits-of-autarky/

24 Kai Nicol-Schwarz, "U.S.-China AI feud sees ASML walk tightrope between sales and geopolitics," *CNBC*, 2026-07-17, https://www.cnbc.com/2026/07/17/us-china-ai-feud-asml-tightrope-sales-geopolitics.html

25 Gregory C. Allen and Issac Goldston, "Understanding U.S. Allies' Current Legal Authority to Implement AI and Semiconductor Export Controls," *Center for Strategic & International Studies*, 2025-03-14, https://www.csis.org/analysis/understanding-us-allies-current-legal-authority-implement-ai-and-semiconductor-export

26 "The Global AI Talent Tracker," *MacroPolo Archive*, https://archivemacropolo.org/interactive/digital-projects/the-global-ai-talent-tracker

27 Siddhi Pal, "Where is Europe's AI workforce coming from?," *Interface*, 2024-07-31, https://www.interface-eu.org/publications/where-is-europes-ai-workforce-coming-from

28 "Global Tech Talent Guidebook 2025," *CBRE*, 2025, https://www.cbre.com/insights/books/global-tech-talent-guidebook-2025/labor-supply; Kelly Wolfgang, "Europe's 2026 Comeback: Funding, AI, DefenseTech Frontier," *Startup Genome*, 2026-06-30, https://startupgenome.com/insights/europe-s-2026-comeback-funding-ai-defensetech-frontier

29 See for example, Ufuk Akcigit, Sina T. Ates & Giammario Impullitti, "Innovation and Trade Policy in a Globalized World," *NBER Working Papers*, 24543, 2018-04, https://www.nber.org/papers/w24543; David Lindequist, "Tipping into protectionism: Tariff shocks and the fragility of free trade," *Economics Letters*, 2026-06, https://doi.org/10.1016/j.econlet.2026.112983



Box 3: Interconnected and Interdependent

While headquartered in only one country, it is virtually impossible to distinguish many techUK members by nationality.

For example, Entrust are US headquartered, but are fully EU owned. Furthermore, they have deep roots in the UK. Their identity verification business was built in London and cryptographic hardware engineered in Cambridge. In addition, they have an operational presence across the EU, particularly in France and Spain.

A similar dynamic plays out in Darktrace, a company that provides services in multiple EU countries that would fall under Level 3 or 4 assurance levels. While it is headquartered in the UK, Darktrace's products are developed in the Netherlands as well as in the UK and it has staff across 12 EU member states.

These are by no means isolated examples. Companies from small startups, through to large multinationals, have taken advantage of the interconnected and interdependent UK-EU digital and technology ecosystems, becoming hybrid organisations that do not fit into any simple nationality box.

Crucial parts of their software supply chains, such as ongoing cyber defences, are also fundamentally international by nature. The UK and EU already rely on shared cyber threat intelligence, vulnerability coordination and cooperation between national authorities, making the idea that UK headquartered firms are less secure by virtue of their nationality clearly flawed.

For techUK members, "everything the levels are meant to assure – where data sits, who can access it, how the service is run and secured, its resilience – can be written as verifiable, auditable requirements that UK companies can meet. An ownership test adds exclusion without adding assurance."

Cultivating Trusted Interdependence: Recommendations

Sovereignty does not require isolation. Indeed, it can easily be weakened by it. Protecting Europe's security and resilience depends on effective cooperation between the UK and EU rather than each looking to isolate their own technology ecosystems from one another and the world. As the EU itself recognised in the UK-EU Security and Defence Partnership, the UK's and EU's "positions on foreign and security policy are closely aligned" and are underpinned by shared values. Both share a responsibility for the security of Europe and the prosperity and security of each are closely interconnected and interdependent.[30]

The fact then that CADA is projected to have deep economic impacts on the UK, in the exact critical technology areas where cooperation is so crucial, highlights the folly of relying on a national test. A loss for the UK in this field is not a gain for the EU given the interdependence between the two when it comes to technology. Instead, leaving the UK out of CADA's assurance framework will also harm the EU profoundly.

Fortunately, there is time to prevent damage to the integrated UK-EU technology sector, if several key actions are taken before CADA is passed.

First, **it is critical that the EU designates the UK as recognised third-country provider and a trusted partner**. There should be no doubt about the importance of the UK to the EU's technological future and the entire continent's security. Policy should be built from the ground up around the importance of protecting and deepening the mutual value that comes from this irreplaceable economic and security relationship. As the analysis above demonstrates, designating the UK as a recognised third-country provider from Day One under the assurance framework would go a long way to limit the economic impact.

However, even that would not fully mitigate CADA's broader impact. Fundamentally, it is necessary to revisit the approach taken in CADA and move away from a model that emphasises nationality as a means to achieve security and sovereignty. Instead, the **EU should focus on technical security assurances to protect sovereignty**. Measures such as customer-exclusive keys, zero-retention policies, data portability requirements, and service continuity planning do more to practically protect security and resilience than national control.

Likewise, the **EU should remove blanket citizenship requirements**. These are unrealistic given the nature of the technology workforce, and duplicate preexisting EU and member state rules where citizenship requirements already exist for dealing with classified information and data. If these rules are not already in place for the services covered by CADA, the personnel screening to agreed standards should be a sufficient protection.

The UK and EU are truly essential partners. There is no replacing the role the UK plays within the EU's broader digital economy or its security, and an attempt to do this will ultimately leave Europe as a whole more vulnerable to malicious actors. Neither is **dependent** on the other in a way that brings with it economic or security risks. Instead, both are **interdependent**. The prosperity and security of both are only strengthened when each leans into this essential interdependence.

30 "Security and defence partnership between the European Union and the United Kingdom of Great Britain and Northern Ireland," *UK Government*, 2025-05-19, https://www.gov.uk/government/publications/uk-eu-security-and-defence-partnership/security-and-defence-partnership-between-the-european-union-and-the-united-kingdom-of-great-britain-and-northern-ireland

Appendix A: Model Inputs and Assumptions

To estimate the potential impact of CADA on the UK, we constructed a model using publicly available data, multipliers, and a number of assumptions. The model is meant to be illustrative and is not intended to function as an entirely accurate representation of the complexity of economic activity between the UK and the EU.

We began with the level of digitally delivered service (DDS) exports from the UK, totalling roughly £412.8 bn in 2025 [WTO, 2026]. However, despite their ubiquity, not all these exports have cloud and AI components. While there is no exact data specifically identifying the cloud and AI composition of DDS, we estimate that roughly 67% of DDS are either delivered via cloud, include AI, or have cloud and AI components in their business model and/or supply chain – roughly £276.6 bn in exports. This estimation was arrived at by removing the finance and insurance components from DDS exports.

We then had to calculate the proportion of the total DDS cloud and AI exports that went to the EU. In 2021, roughly 36% of UK exports went to the EU [OECD, 2024]. Assuming this figure holds, we estimate that the UK exports roughly £99.6bn in cloud and AI DDS to the EU annually.

To identify the magnitude of DDS procured by EU public institutions, we first began by constructing custom queries of the TED database [TED, European Public Procurement, 2026]. However, since TED is not representative of all public procurement across the EU, the data produced were always underestimates. Instead, we relied on a broader macroeconomic picture of the EU, where estimates show that public procurement constitutes 15% of EU GDP [European Commission, 2025]. To estimate the proportion of cloud and AI DDS exports from the UK destined for EU institutions, we restrict this figure to 10% to ensure we are not overestimating. This results in a value of roughly £10.0bn in UK cloud and AI DDS exports purchased by EU institutions annually. From there, we can determine that the EU's private sector procures an estimated £89.6bn in cloud and AI DDS from the UK annually.

Next, we examined the proportion of UK contracts to the EU that fall under CADA Levels 3 and 4, based on three scenarios. In the baseline scenario, outlined by the European Commission, 9% of contracts fall under level 3 and 1% fall under level 4 [European Commission, 2026]. In the mid-tier scenario, due to inflationary incentives, 13% of contracts fall under level 3, and 2% level 4. Finally in the high-tier scenario, 17% of contracts fall under level 3 and 3% level 4. We also assume that not all UK vendors would be excluded from contracts under level 3 assurance levels. We used a conservative threshold of 90% exclusion from level 3 contracts. We assume 100% exclusion from level 4 contracts.

When it comes to the impact of data centre (DC) foreign direct investment, we relied on the UK announced DC FDI pipeline (2025–28) of £36.4 bn (£9.1 bn annually averaged over 4 years) [techUK, 2026]. Our model assumes that CADA's efforts to triple EU DC capacity in five years would divert 10% of foreign direct investment into the UK.

Our model also employed a trade type II multiplier using the UK's System of National Accounts, ONS IOAT tables for information service activities [ONS, 2025], while also relying on other external macroeconomic assessments of the economic contributions of data centres to develop an investment-to-GDP multiplier for data centre activities [PwC, 2026].

About techUK

techUK is the membership body for the tech industry. We support collaboration between the tech industry, the public and private sectors, regulators and government to build a better future for people, society, the economy and the planet.

We champion technology's role in empowering the UK for what comes next.

www.techuk.org

techUK
FOR WHAT COMES NEXT


linkedin.com/company/techuk


www.x.com/techUK


youtube.com/user/techUKViews


membership@techuk.org

If you have any questions about this report please email Sabina Ciofu (sabina.ciofu@techUK.org)

Image credits: Shutterstock.com