Bauer, Matthias

Research Report

Building resilience? The cybersecurity, economic & trade impacts of cloud immunity requirements

ECIPE Policy Brief, No. 01/2023

Provided in Cooperation with:
European Centre for International Political Economy (ECIPE), Brussels

Suggested Citation: Bauer, Matthias (2023) : Building resilience? The cybersecurity, economic & trade impacts of cloud immunity requirements, ECIPE Policy Brief, No. 01/2023, European Centre for International Political Economy (ECIPE), Brussels

This Version is available at:
https://hdl.handle.net/10419/280811

ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

POLICY BRIEF – No. 01/2023

Building Resilience? The Cybersecurity, Economic & Trade Impacts of Cloud Immunity Requirements

by **Matthias Bauer,** *Director at ECIPE*

EXECUTIVE SUMMARY

- EU Member States should call on the EU's Cybersecurity Agency (ENISA) and the European Commission to abandon immunity requirements in the proposed EU Cloud Certification Scheme (EUCS).

- With immunity requirements in the EUCS, the EU risks opening a Pandora's box, paving the way for data localisation, foreign ownership restrictions, and local establishment requirements in digital industries globally leading to rising trade tensions. ENISA's current proposal could increase policymakers' appetite for data localisation in the EU. It would empower the European Commission and Member State authorities to exclude foreign businesses from domestic cloud services markets and set a dangerous precedent for any data-intensive sector. The list of "sectors of high criticality" could be logically extended to both existing services (e.g., financial services) and to new technologies and business models, such as IoT in the energy and healthcare sectors, and autonomous driving in the transport sector. Non-EU jurisdictions would be pressured to respond in kind.

- EUCS immunity requirements would increase cloud adopters' exposure to cybersecurity risks. Data localisation

often creates obstacles to an integrated management approach towards cybersecurity risks. Country of headquarter and foreign ownership restrictions in the proposed EUCS risk removing global frontier cybersecurity technologies from Member State markets. Excluding these and other EU and non-EU companies from EU Member States could result in a long-lasting security deficit of EU cloud adopters vis-à-vis organisations that are still able to use reliable and often best-practice cloud services offered by providers from outside EU Member States.

- Immunity requirements in the EUCS are discriminatory by design. They could provoke retaliatory measures by EU trading partners, either unilaterally or through WTO or bilateral FTA (e.g., UK-EU) Dispute Settlement. Local establishment requirements and foreign ownership restrictions would by design discriminate against foreign cloud providers. US-headquartered companies, which currently serve more than 75% of the EU market, would be most affected by EU immunity requirements. Depending on US preferences and the scope of the proposed EUCS, the EU could be subject to retaliatory tariffs of up to USD 12 billion worth of EU goods exports or equivalent restrictions for EU services exports to the US. Other governments could lodge complaints via the WTO as well (e.g., Singapore, Japan, Canada and others, where cloud development is advancing rapidly).

- EU suppliers are currently in no position to manage a broad-based transition to cloud, and thus such requirements would delay significant efficiency and security gains that current foreign suppliers could offer. A blanket exclusion of non-EU cloud vendors would also likely undermine Europe's objective to achieve a 75% cloud adoption rate for EU enterprises. Sensitive European businesses and public sector organisations would have to delay migration and make do with legacy systems for a very long time. Contrary to large countries, these negative impacts would be much more pronounced for smaller EU Member States, which lack the presence of large domestic incumbents and generally rely much more on an open international trading regime for digital services.

- ENISA's cloud certification scheme should be limited to technical and transparency requirements. Immunity requirements for non-personal data should be addressed in bilateral initiatives such as the EU-US Trade and Technology Council (TTC) or agreements requiring a company that sought to offer services of the highest level of sensitivity to be headquartered in a country granted adequacy with EU data protection rules, or a country that is an adherent to the OECD's Trusted Government Access principles, or (concerning the US) a participant in the upcoming Trans-Atlantic Data Privacy Framework. Excluding foreign companies from operating in the EU would have far-reaching consequences. If that is the intent, it should require a sound legal analysis and the decision should be taken through a formal legislative procedure at the EU level.

1. BACKGROUND: THE PROPOSED EU CLOUD CERTIFICATION SCHEME

The EU Agency for Network and Information Security (ENISA) is proposing a far-reaching Cybersecurity Certification Regime for Cloud Services (EUCS) to be established in the European Union. ENISA is following a request from the European Commission[1], which is considering mandatory cybersecurity certification in several EU policies targeting providers of ICT products and services in the EU. These include the EU Cybersecurity Act (CSA), the Network and Information Security (NIS2) Directive, the proposed Data Act, and the proposed Cyber Resilience Act (CRA).

ENISA's objective is, as originally stated in 2020, to *"further improve the Union's internal market conditions for cloud services by enhancing and streamlining the services' cybersecurity guarantees. The draft EUCS candidate scheme intends to harmonise the security of cloud services with EU regulations, international standards, industry best practices, as well as with existing certifications in EU Member States."* It is further stated that *"[a] single European cloud certification is critical for enabling the free flow of data across Europe, and is an important factor in fostering innovation and competitiveness in Europe."* [2]

ENISA's scheme is meant to establish an EU-wide certification regime for cloud services with three levels of assurance: "basic", "substantial", and "high". For high level assurance certification, the European Commission has asked ENISA to add immunity (sovereignty) requirements, with the political objective to ensure immunity from foreign jurisdictions.

According to the latest draft, the EUCS would by design prevent non-European vendors from providing high assurance level services in the EU. It would demand that a cloud service provider (CSP) be headquartered in an EU Member State. CSPs whose registered head office and global headquarters are not established in a Member State of the EU shall not, directly or indirectly, individually or jointly, hold effective control of the CSP applying for the certification of a cloud service. Together with other requirements for high assurance services this implies that

- certification eligibility is restricted only to cloud providers globally headquartered in the EU,
- EU established vendors for which a foreign-headquartered parent has a controlling share are excluded from the EU market,
- it is prohibited to store and process data outside the EU, and
- customer support capabilities are restricted to employees located in the EU.

Although the scheme itself is foreseen as voluntary, the high assurance level is expected to become mandatory for the essential and important services listed under the NIS2 Directive. And, even if

[1] According to Article 48.2 of the EU Cybersecurity Act. The proposed EUCS is a candidate scheme. It is a voluntary regime but could be validated under an EU implementing act based on Article 48.2 of the EU Cybersecurity Act. According to Article 48.2 of the Cybersecurity Act, "[t]he certification shall be voluntary, unless otherwise specified in Union law."

[2] ENISA (2021). Cloud Certification Scheme: Building Trusted Cloud Services Across Europe. Press release, 22 December 2020. Available at https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme.

it is technically voluntary, once it is included as a tender requirement by the customer, whether governmental or commercial, the requirement would, for that specific procurement, be mandatory. NIS2 allows EU governments and the European Commission to mandate certain cloud customers to only use a certified EUCS cloud service.[3] Governments and the European Commission have full discretion to mandate any assurance level in national laws or in a subsequent delegated act.

Beyond NIS2, the proposed Data Act could require cloud vendors to obtain an EUCS certification, as part of their legal obligations preceding transfers of non-personal data to non-EU jurisdictions.[4] Additional competences for Member States' enforcement bodies to require EUCS certification for services in the domestic market will likely result from the proposed CRA (Table 1).

TABLE 1: EUROPEAN COMMISSION AND MEMBER STATE COMPETENCES TO MAKE EUCS CERTIFICATION MANDATORY IN THE EU

EU Cybersecurity Act (CSA)	EU Network and Information Security 2 (NIS2)	EU Data Act (DA)	EU Cyber Resilience Act (CRA)
According to Articles 48.2 and 56.2 of the Cybersecurity Act, cybersecurity "certification shall be voluntary, unless otherwise specified in Union law." According to Article 56 of the Cybersecurity Act, "[t]he Commission shall regularly assess the efficiency and use of the adopted European cybersecurity certification schemes and whether a specific European cybersecurity certification scheme is to be made mandatory through relevant Union law to ensure an adequate level of cybersecurity of ICT products, ICT services and ICT processes in the Union and improve the functioning of the internal market."	According to Article 21.1 of NIS2, "Member States may require entities to use particular ICT products, services and processes, either developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes." According to Article 21.2 of NIS2, "[t]he Commission is empowered to adopt delegated acts […] by specifying which categories of essential or important entities shall be required to use certain certified ICT products, services and processes or obtain a certificate under a European cybersecurity certification scheme […]. Article 21.2 also states that "[b]efore adopting such delegated acts, the Commission shall carry out an impact assessment and shall consult stakeholders in accordance with Article 56 of Regulation (EU) 2019/881."	Article 27 compels cloud computing providers to take all reasonable technical, legal and organisational measures, including contractual arrangements to "prevent international transfer or governmental access to non-personal data held in the Union where such a transfer or access would create a conflict with Union law or the national law of the relevant Member State […]. Article 27.3 empowers the European Commission to develop guidelines, consistent with the recommendations of the European Data Innovation, for transfer risk assessments, which could rely on key EUCS cybersecurity requirements.	The proposed CRA aims to ensure a coherent cybersecurity framework and certain security properties of products with digital elements. Even though it is unclear how the CRA will interplay with the EU Cybersecurity Act and other digital policies, certification obligations might stem from CRA requirements for businesses to conduct third-party conformity assessment to demonstrate compliance with their higher regulatory obligations.

[3] Articles 21(1) and 21(2) NIS2 Directive allow Member States and the European Commission to require essential and important entities to use an EU certified ICT product, service, or process.

[4] ENISA explicitly states that EUCS Annex J provisions would align with Article 27 of the Commission proposal for an EU Data Act, which includes provisions about safeguards against such extra-territorial application of non-EU laws.

The thinking behind the immunity requirements of EUCS Annex J originated in France. ENISA explicitly states in its proposal that Annex J provisions of the EUCS follow the design of France's SecNumCloud, a cybersecurity scheme developed by the French National Cybersecurity Agency (ANSSI) for public authorities and Operators of Vital Importance (OVIs).[5] ANSSI already launched a SecNumCloud certification scheme in 2016. It was supposed to operate as a voluntary certification program, aimed at establishing certain minimum levels of security for French public entities procuring cloud services to host data and information systems. However, since then ANSSI has only certified seven services provided by five companies, all of which are headquartered in France.[6] And, as noted above, once this standard is specified on specific tenders, as has started occurring in France, the requirement becomes mandatory and foreign firms are ineligible to bid.

This stands in stark contrast to the US Federal Risk and Authorisation Program (FedRAMP), which also adopts a risk-based approach for certifying cloud services used by US federal government agencies. However, contrary to SecNumCloud and the proposed EUCS, FedRAMP certification requirements at the "High Risk Impact Level" do not include local majority ownership or establishment of headquarter requirements, or that CSPs' staff be US nationals or hold security clearances.[7] Indeed, several foreign-based firms, including Accenture (Ireland), Siemens (Germany), and Collabware (Canada), are currently authorised under "FedRAMP High".[8] Also, Germany's C5 cloud services' security standard does not discriminate against non-EU CSPs.[9]

A similar ability of EU companies to participate in the most sensitive sectors of US government procurement is evident in the strong EU participation in US defence procurement, in sectors ranging from air transport, weapons systems, avionics, and satellite transmission services.

Requirements under Annex J would not only affect foreign companies. EU businesses operating abroad are typically subject to foreign laws. Accordingly, irrespective of their size and the nature of their business activities, EUCS requirements could force EU businesses to decouple their global cloud operations from EU operations and vice versa. Referring to France's SecNumCloud, the proposed EUCS and the operations of globally operating businesses, one legal scholar from the US outlines that

"[i]t is a legally and factually complex question whether any cloud services company operating in the United States – American or European – can escape the reach of U.S. legal authorities. In the case of the CLOUD Act, the question may well turn on corporate structure and the choices of customers

---

[5] SecNumCloud mandates the CSP to be headquartered in the EU. EUCS' control requirements are also inspired by SecNumCloud, but ENISA replaced the numerical bounds defined by SecNumCloud by a broader definition of "effective control. The definition of "effective control" mentions the "possibility" to influence, not an actual instance.

[6] Oodrive provides three SecNumCloud certified Software-as-a-Service solutions. Cloud Temple, Outscale SAS, OVH and Worldline provide SecNumCloud certified Infrastructure-as-a-Service. See list of SecNumCloud certified cloud products and vendors on https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf, page 12. see also Propp, K. (2022). European Cybersecurity Regulation Takes a Sovereign Turn. European Law Blog, 12 September 2022. Available at https://europeanlawblog.eu/2022/09/12/european-cybersecurity-regulation-takes-a-sovereign-turn/.

[7] In some cases, the company managing the contract (which can be a subsidiary of the company owning the infrastructure) may have clearance/nationality requirement. However, the company can be fully foreign owned and controlled.

[8] See FedRAMP marketplace designations, as of 30 November 2022. Available at https://marketplace.fedramp.gov/#!/products?sort=productName. Note that in limited cases, federal agencies are required to keep national security-related data in the US.

[9] See Federal Office for Information Security (2023). Cloud computing C5 criteria catalogue. Available at https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5.html.

on the jurisdiction in which to store their data. The viability of an 'immunity' requirement in French or EU law thus ultimately will depend on how courts view company attempts to separate themselves from domestic jurisdictional reach. Because so many EU- based companies conduct at least some business in other countries, including through online services, an 'immunity' requirement in French or EU law thus could result in numerous disqualifications from cybersecurity certification."[10]

As will be further outlined below, immunity requirements in the proposed EUCS would open a Pandora's box because they:

- empower Member States and conformity assessment bodies to determine in isolation which operators of essential and important services – e.g., in healthcare, transport, energy, banking and financial market, manufacturing, digital infrastructure and water supply – must use cloud services with a high level of assurance. Cloud services which cannot be qualified with a high assurance level would be excluded from the market whenever such assurance level is required,
- empower Member States and conformity assessment bodies to determine in isolation where to delineate core services and ancillary services in sectors considered essential for the functioning of the economy and society,
- increase cybersecurity risks in the EU, for example, by affecting the speed with which organisations can identify vulnerabilities and deploy patches,
- increase regulatory fragmentation and legal uncertainty for CSPs operating in the EU and their customers,
- create uncertainty about the definition of "critical infrastructure" in EU law and potentially interfere with the sole competence of the Member States with respect to national security, defence, and military.
- serve as a template for other countries that are seeking mandatory data localisation, local establishment requirements, and foreign ownership restrictions,
- trigger a wave of trade disputes and retaliatory measures globally, and
- trigger potential competition and state aid infringements (and associated disputes), by creating a mechanism for discrimination and an uneven playing field via differing interpretations of "effective control".

Businesses or processing operations that currently are considered less sensitive could in the future also fall under the scope of Annex J requirements. Multiple cases involving cross-border data flows show that national authorities do not shy away from taking absolutist views on data flows, beyond the legislator's intentions and the letters of GDPR. In France and Germany, for example, national and sub-federal data protection authorities aim to ban Microsoft's Office 365 suite and Google Workspace[11] – solutions used by hundreds of millions of firms and individuals globally – from schools to public sector use based on disputed data privacy grounds. In Portugal, the Supervisory Authority

[10] See Propp, K. (2022). European Cybersecurity Regulation Takes a Sovereign Turn. European Law Blog, 12 September 2022. Available at https://europeanlawblog.eu/2022/09/12/european-cybersecurity-regulation-takes-a-sovereign-turn/.

[11] See, e.g., Brunoli, J. (2022). France bans Office 365 and Google Workspace in schools, 22 November 2022. Available at https://www.techzine.eu/news/privacy-compliance/95012/france-bans-office-365-and-google-workspace-in-schools/. Also see French Data Protection Authority letter regarding the use of US collaborative tools for higher education and research. Available at https://www.cnil.fr/fr/la-cnil-appelle-evolutions-dans-utilisation-outils-collaboratifs-etatsuniens-enseignement-superieur-recherche, and Ministry of Education of State of Baden-Wuerttemberg, Stellungnahme zur Nutzung von Microsoft 365, 26 April 2022. Available at https://km-bw.de/,Len/startseite/service/stellungnahme-nutzung-von-ms-365.

even argued that data cannot be processed by a non-EU entity even where there are no transfers involved.[12] Last but not least, the EDPB has expressed support for data localisation and overly discriminatory requirements against non-EU cloud vendors to facilitate compliance with GDPR, even though GDPR explicitly provides for international data transfer mechanisms.[13] Countries like the US, whose companies are hit by the EU's immunity requirements, would be pressured to respond in kind by imposing similarly restrictive measures targeted at EU data and, potentially, other industries (see below).

2. THE ECONOMIC IMPACTS OF FOREIGN OWNERSHIP RESTRICTIONS AND DATA LOCALISATION

Digital services are key enablers of the process of digitisation of business models. Modern cloud services also help governments upgrade and streamline public services and solve infrastructure issues, cost issues, and improve service delivery and transparency.[14] Big and small firms in the EU use data intensively: 98% of the EU's multinational corporations and 83% of EU SMEs report having at least one business use for data.[15] The use of internal cloud-based services ranges from email, videoconferencing, Internet protocol telephony, document sharing, shared workspaces, and project management. Many, if not most, of these services are currently provided by suppliers headquartered outside the EU.

Modern IT services are of utmost relevance for companies across all economic sectors and sizes. Cloud storage and processing services are revolutionising how businesses create value. At the same time, IT services themselves, including cloud computing services, undergo a constant process of upgrading and innovation, delivering faster, more secure, and more customised services to demanding clients and complex use cases. Importantly, by far the largest part of economic value-addition and savings in the process of supplying goods and services stems from the adoption of cloud services rather than its supply.

The immunity requirements in Annex J of the proposed EUCS would not allow globally operating CSPs to qualify for the highest assurance level of cybersecurity. This prevents EU customers in sectors that require the highest assurance level of cybersecurity certification from purchasing reliable customised solutions including the world's most advanced cloud services with reliable security profiles. Should the Annex J-like restrictions be extended to other areas in the future – which is not unlikely given some Member State authorities' inclination to favour domestic companies over foreign ones – the negative effects could be much greater. In the future "sectors of

---

[12] See, e.g., DisCo (2021). Portuguese Decision Another Foreboding Sign for Global Data Transfers, May 2021. Available at https://www.project-disco.org/european-union/050721-portuguese-decision-another-foreboding-sign-for-global-data-transfers/.

[13] See EDPB letter to ENISA regarding the European Cybersecurity Certification Scheme for Cloud Services (EUCS), 23 November 2021. Available at https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-enisa-regarding-european-cybersecurity_en.

[14] See, e.g., Abied et al. (2022). Adoption of Cloud Computing in E-Government: A Systematic Literature Review. Science & Technology 30 (1): 655 - 689 (2022). Also see Deloitte (2021). Digital Government: How the EU cannot miss the cloud opportunity, November 2021. Available at https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/public-sector/20211129-cloud-gps-eu.pdf.

[15] Kearney and ECIPE (2021). The economic costs of restricting the cross-border flow of data. Joint Kearney-ECIPE study. Available at https://www.kearney.com/documents/3677458/161343923/The+economic+costs+of+restricting+the+cross-border+flow+of+data.pdf/82370205-fa6b-b135-3f2b-b406c4d6159e?t=1625036783000.

high criticality", as stated in Annex 1 of the NIS2 Directive, could also include sensitive IoT industry use cases and autonomous driving. The extension of legal competences over time to sectors that currently are considered less sensitive would impact legal certainty and business operations in many EU industries, especially those that undergo a fast process of digitisation and those that increasingly rely on software-as-a-services solutions (SaaS) and intra-business cloud solutions that are spread across their global entities.

The literature is clear that law-imposed data storage and processing, and localisation would create a major misallocation of resources in the EU, which will reduce European firms' productivity and competitiveness. The free cross-border flow of data supports EU businesses' intra-EU as well as global supply chains and the cost-efficient management of international production processes.[16] Statistics demonstrate that data is especially important in the context of the Transatlantic economy: over the past 15 years, the balance of trade between the EU and the US has shifted to services, especially digital services.[17] In addition, international trade in goods, such as consumer products, agricultural commodities, and machinery equipment, is increasingly facilitated by data-intensive services such as, analytics, content management, tracking, maintenance, but also complex financial and logistics services. In that context, it should be noted that US providers currently provide more than three quarters of cloud computing services in the EU.[18]

A recent study conducted by Kearney and ECIPE estimates that a full ban on cross-border data flows of only personal data from the EU to the US could result in a 31% decline in digital services imports from the US to the EU – a substantial impact given that digital services account for 39% of the total US exports to the EU. It is highlighted that substitution of imports of some of the world's most advanced and most internationally competitive digital services from the US would be unlikely in the short- and medium-term, especially where there is a lack of established and globally competitive providers outside the US. Overall, it is estimated that company productivity will decline in the EU. On aggregate, the impact of a ban on cross-border data flows outside the EU could have a huge long-term impact, ranging from an estimated 1.9% to 3.0% of EU GDP.[19]

It should be noted that a ban on the cross-border transfer of non-personal data, which is often difficult to separate from personal data, has not been accounted for in the study conducted by Kearney and ECIPE. However, a related study by Frontier Economics on the economic impacts of restrictions to the cross-border flow of non-personal data arrives at similar conclusions. The study finds that new regulations, which require EU businesses to assess the laws and practices of non-EU countries they share non-personal, commercially sensitive data with/from, would cause 40% of surveyed businesses to stop their cross-border flows of such data. Large EU

---

[16] See, e.g., OECD (2020). Data localisation trends and challenges, December 2020. Available at https://www.oecd.org/sti/data-localisation-trends-and-challenges-7fbaed62-en.htm. See also ECIPE (2016). Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States, Policy Brief 03/2016. Available at https://ecipe.org/wp-content/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf.

[17] Digital services or digitally enabled services typically are telecommunications services, IT and other information services, financial and insurance services, professional and business services, and research and development related services incl. charges for the use of intellectual property.

[18] Synergy Research (2022). European Cloud Providers Continue to Grow but Still Lose Market Share, 27 September 2022. Available at https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share.

[19] Kearney and ECIPE (2021). The economic costs of restricting the cross-border flow of data. Joint Kearney-ECIPE study. Available at https://www.kearney.com/documents/3677458/161343923/The+economic+costs+of+restricting+the+cross-border+flow+of+data.pdf/82370205-fa6b-b135-3f2b-b406c4d6159e?t=1625036783000.

businesses and multinational EU corporations expect costs equivalent to on average 4% of their annual global revenues. The impact is expected to be larger for R&D-intensive companies that share data for innovation purposes. It is highlighted that such regulations would act as a tax on R&D, innovation and business scale-up in Europe as these costs are non-recuperable costs, diverting EU businesses' resources away from productive investments in future capacities and capabilities.[20]

Overall, Frontier estimates that the cost of new restrictions to the cross-border flow of non-personal data to MNEs and scaleups would be around EUR 79bn per year, of which 20bn would be from impact on scaleups and 60bn from impact on other MNEs. This is around 0.6% of EU GDP. It is highlighted that European SMEs account for a minority of the overall impact, around 40% (EUR 26bn). This is because large enterprises are more likely than SMEs to have an international presence and therefore to share data across borders.

While it may be premature at this time to conduct a similar impact analysis of the proposed EUCS given uncertainties on scoping, there are several important aspects that need to be taken into account by policymakers.[21]

a) The EU could open a Pandora's box by setting a big precedent on the basis of which other countries could impose similar measures across industries and business activities.

The proposed immunity requirements, regardless of the level of assurance with which they are advocated, are politically motivated. What has been pushed by the French government, following France's SecNumCloud template, will only decrease the availability of advanced and resilient cloud technologies for sensitive adopters in the EU Member States. The proposed immunity requirements will create very complex legal compliance procedures and, as outlined further below, reduce risk detection and effective cybersecurity management.

The European Commission and ENISA are considering bans on cloud vendors to do business in the EU if they already have operations abroad or are headquartered outside Europe. As outlined by many observers, Annex J immunity requirements are an attempt by some large EU governments, especially France, Italy and Spain, to impose industrial policy through the backdoor, by forcing EU adopters of cloud services to purchase local cloud products at the expense of quality and choice, and at the expense of the EU's commitment to open markets and global trade rules (see further below). On September 19, Germany noted that the matter had reached a political dimension. A joint letter by

[20] Frontier Economics (2022). Beyond Personal Data: The Cost of Data Flow Restrictions to EU Companies. 17 February 2022. Available at https://www.frontier-economics.com/media/5065/beyond-personal-data_the-cost-of-data-flow-restrictions-to-eu-companies.pdf.

[21] It is difficult to come up with an exact quantification of the impacts of the proposed EUCS and, in particular, the proposed Annex J requirements for CSPs. Unless Annex J obligations extend to less sensitive entities and use cases, the effect of EUCS might be more limited than those estimated for EU economy-wide restrictions to the free cross-border flow of personal and non-personal data (according to Frontier Economics, 2022, see preceding footnote). However, an analysis by IDC on the economic contribution of cloud services to the European economy estimates that the public cloud supply chain contributed almost USD 500 billion to European GDP - 2.7% of total European GDP. Given that some 90% of the European cloud market are served by foreign suppliers, restricting these suppliers would result in significant capacity shortages across digital services supply chains in Europe. See IDC (2021). Public Cloud and the Related Supply Chain Contributed Almost $500 Billion to European GDP in 2020. 10 December 2021. Available at https://www.idc.com/getdoc.jsp?containerId=prEUR148556621.

several German ministries called on the European Commission to consider a political discussion on the sovereignty requirements in the European cybersecurity cloud certification scheme.[22]

In contrast to taxes on digital services and to subsidy-related local content requirements in the US Inflation Reduction Act, the restrictions on headquarter and foreign ownership would by design, as a de jure matter, exclude businesses from the EU market on the basis of the nationality of the company or its investors.[23] By doing so, the EU could open a Pandora's box by setting a big precedent on the basis of which other countries could impose similar measures, not only in the area of digital services, but across industries and business activities. Indeed, it is hard to conceive of any good or service incorporating information technology, supplied by a foreign company, that would not be amenable to equivalent restrictions.

The associated risks are actually known to EU policymakers. EU trade policy for a very long time has been pushing trading partners to liberalise and abstain from local establishment obligations and restrictions on foreign ownership, particularly joint venture requirements in services and high technology industries. Considering the same trade and investment-restrictive measures, the EU is undermining its own credibility in global trade fora and its own trade negotiations. Take key elements of the EU-China Comprehensive Agreement on Investment as an outstanding example: it took EU trade negotiators many years to achieve new market access openings and commitments such as the elimination of quantitative restrictions, equity caps, or joint venture requirements in a number of sectors, including cloud computing. These are restrictions known to severely hamper the activities of EU companies in China and other countries.

b) Easy to implement and technologically advanced cloud services are key for cost competitiveness and innovation.

Excluding non-EU CSPs from Europe would reduce competition as European providers would not need to innovate or price as fiercely anymore in order to win business. Ultimately, European customers would lose out, compared to those in other countries where more innovative operators would need to compete strongly to win business.

Recent research into more than 700 industry cases across 20 industries demonstrates that businesses maximise the value of cloud adoption in three different ways: rejuvenation, innovation, and pioneering. It is estimated that by far the largest part of the value-added created by the adoption of cloud services is generated through the use of cloud services to foster multiple innovation activities (72%), while about one third (28%) of the value-added from cloud adoption is estimated to stem from increased production efficiencies and associated cost reductions, and reductions in operating costs (see Figure 1 and Table 2).[24] It should be noted that additional value-

[22] Joint letter sent by Germany's Ministry of the Interior, the Ministry of Economic Affairs, and the Ministry for Transport and Digital Policies, 19 September 2022. Also see Euractiv (2022). Germany calls for political discussion on EU's cloud certification scheme, 19 September 2022. Available at https://www.euractiv.com/section/cybersecurity/news/germany-calls-for-political-discussion-on-eus-cloud-certification-scheme/.

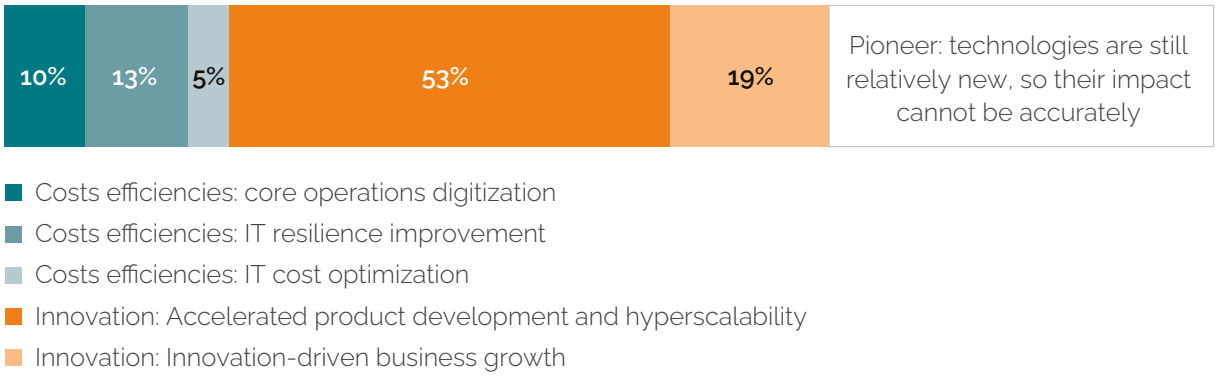
[23] See, e.g., McKinsey (2022). The Inflation Reduction Act: Here's what's in it, 24 October 2022. Available at https://www.mckinsey.com/industries/public-and-social-sector/our-insights/the-inflation-reduction-act-heres-whats-in-it.

[24] McKinsey (2022). Projecting the global value of cloud: $3 trillion is up for grabs for companies that go beyond adoption. McKinsey Digital, 28 November 2022. Available at https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/projecting-the-global-value-of-cloud-3-trillion-is-up-for-grabs-for-companies-that-go-beyond-adoption.

added originates from "pioneering activities", such as the early adoption of cloud activities and a wide range of associated future and transversal technologies such as quantum computing and blockchain solutions. The economic impacts of these activities are difficult to estimate ex-ante, but they can be expected to be enormous especially over the medium- to the long-term. Missing out on pioneering activities could advance the EU's profound productivity and technological gap vis-à-vis the US and other jurisdictions[25], at least for organisations whose choice will be limited to EU-only cloud solutions.

Accordingly, restricting EU cloud adopters' – public authorities' and commercial entities' – choice to fewer, less expedient, and potentially less safe and reliable cloud solutions could have a significant negative impact on their cost efficiency and the quality of services and goods provided to customers and citizens, such as modern e-government solutions and offerings of public utilities. While the impact on public sector entities is clear-cut, the mere possibility of a scheme being applied to as-yet-unspecified sectors is likely to have a chilling effect on cloud adoption, undermining the EU's goal of achieving 75% adoption by European enterprises. Transitioning workloads to the cloud is typically a major efficiency-enhancing investment for an enterprise, and the risk that a cloud partner would be ineligible to offer a service in the near future could be enough to delay that transition until all the details are finalised.

FIGURE 1: CLOUD SERVICES CONTRIBUTION DO ADOPTERS' VALUE-ADDED



Source: McKinsey, based on estimated cloud adoption value drivers in EBITDA value across the Forbes Global 2000 companies. See McKinsey (2022). Projecting the global value of cloud: $3 trillion is up for grabs for companies that go beyond adoption. McKinsey Digital, 28 November 2022.

[25] McKinsey (2022). Addressing Europe's corporate technology gap, 5 May 2022. Available at https://www.mckinsey.com/mgi/overview/in-the-news/addressing-europes-corporate-technology-gap.

TABLE 2: ORGANISATIONS' VALUE DRIVERS FROM CLOUD ADOPTION

Rejuvenation	Innovation	Pioneering
• Cost optimization of application development, IT maintenance, and infrastructure • Improved business resilience of the organisation • Implementation of latest technological/ digitization achievements in core operations	• Adopting advanced cloud-based technologies in analytics, IoT, and automation • Innovation-driven growth from new and enhanced use cases in analytics, IoT, and automation • Accelerated product development from ease of cloud configuration, and democratised access to computing power • Hyperscalability due to instant on-demand elasticity in compute and storage capacity to scale across customer segments, geographies, and channels	• Early adoption of cloud technology • Embracing culture of experimentation with low cost of failure and gaining experience in cloud technology, • Enabling of early adoption of future technologies such as quantum computing, virtual reality applications, blockchain, and 3-D/4-D printing

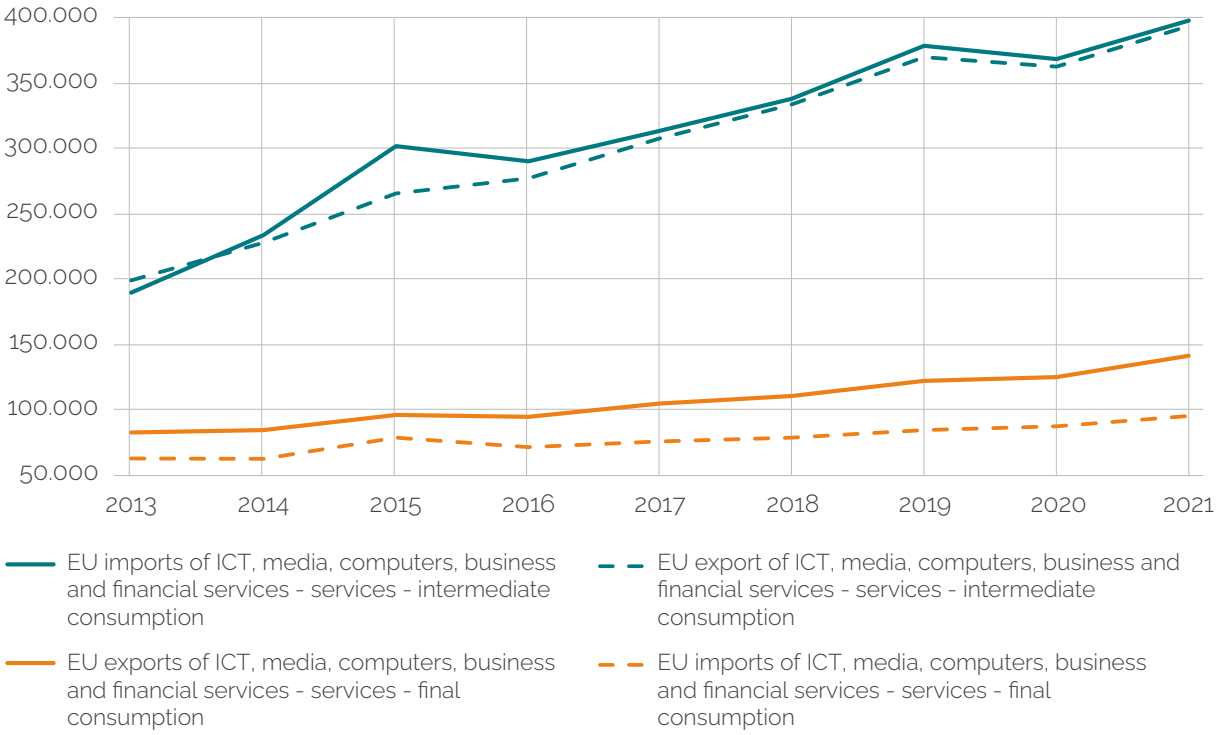
Source: McKinsey, based on estimated cloud adoption value drivers in EBITDA value across the Forbes Global 2000 companies. See McKinsey (2022). Projecting the global value of cloud: $3 trillion is up for grabs for companies that go beyond adoption. McKinsey Digital, 28 November 2022.

c) EU-only cloud providers may not have the capacity to meet surging demand for high assurance services.

EUCS-imposed data localisation requirements will effectively limit the choice of Europe's public sector and commercial entities by mandating exclusive use of EU-only offers for their cloud infrastructure. Depending on the speed of implementation and Member States' lists of essential and important services referred to under NIS2 Directive, European public authorities and commercial entities would face severe capacity shortages in the EU. The question should be posed, whether the same standards will be applied across the EU and whether in practice the same delimitations will exist across the EU with regard to "essential entities" or "important entities"

Trade data indicates that Europe's "native" cloud market simply does not have the capacity to meet surging demand. In 2021, EU imports of "ICT, media, computers, business, and financial services" for intermediate consumption – e.g., inputs by a process of production – from non-EU countries amounted to EUR 400 billion. Many of these services are provided cloud-based. Imports from outside the EU in this industry more than doubled over the past decade, indicating that EU capacities are either inadequate or insufficient to meet EU businesses' and public sector demand for high quality digital or digitally enabled services.

FIGURE 2: EU TRADE IN DIGITAL AND DIGITALLY ENABLED SERVICES FOR INTERMEDIATE CONSUMPTION AND FINAL CONSUMPTION, IN MILLION EUR



Source: Eurostat trade in services statistics.

Industry data also reveals that for a broad variety of Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) services, there are simply no satisfactory European alternatives that could result in cost reductions, improve resilience, and enhance innovation. Synergy Research states that Infrastructure-as-a-Service (Iaas) and Platform-as-a-Service (PasS) indeed are among the fastest growing services in the EU market, currently accounting for over 80% of the European cloud market. Data by Synergy Research also shows that while European cloud providers have seen their revenue increase by 167% over the 5 years, the collective share of cloud computing services provided by European CSPs has dropped from 27% to 13% in their home territory over the same period. In 2021 alone, their share has dropped by around two percentage points.[26] Assuming that shares in the narrow segment of high assurance services roughly correspond with overall shares of cloud services providers in the EU, "EU-only cloud providers" would have to meet a demand of about 90% of the market value, excluding future growth of the sector. Some of those European cloud providers will continue to grow, but they are unlikely to move the needle much in terms of overall European market share."[27]

[26] Fierce Telecom (2022). European cloud players losing share to AWS, Microsoft, Google, 3 October 2022. Available at https://www.fiercetelecom.com/cloud/european-cloud-players-losing-share-aws-microsoft-google.

[27] See, TechRepublic (2022). Response provided by John Dinsdale, a chief analyst at Synergy Research Group on why huge investment in the cloud has been a key factor in ensuring the U.S. cloud giants maintain the lion's share in the global cloud market. 29 September 2022. Available at https://www.techrepublic.com/article/european-vs-us-cloud-provider-market/.

EU public authorities and commercial entities may face difficulties when migrating complex datasets and associated user interfaces to alternative and less technologically advanced suppliers. Migrating IT services or an entire data centre involves the moving of data assets in an existing data centre – be it on-premise, software, or hardware – to a new location. It means moving operations, applications, and data from a legacy IT solution to something different, which is an extremely complex, human resource-intensive, highly skilled, and time-consuming process.

Due to lacking quality and capacity many EU-only providers would be forced to decline tenders or migration requests. In contrast to large countries, these negative impacts would be much more pronounced for smaller EU Member States, which lack the presence of large cloud providers and generally rely much more on an open international trading regime for digital services. By contrast, large countries, such as Germany, France, Italy, and Spain could count on their comparatively large national ICT incumbents which have already gained scale in their domestic markets. Also, legacy incumbents in larger EU countries, such as Germany's Deutsche Telekom and France's OVH, often have close ties to governmental institutions and may benefit from financial incentives if they prioritise national demand for cloud services. As a result, such an imbalance is likely to decrease intra-EU competition and reduce the level-playing field for EU CSPs and customers of cloud services.

Overall, obligations to migrate, store, and process data through EU-only solutions will not only be overly costly to European businesses and Europe's public sector; it will also lead to authorities and businesses not being able to select a cloud service that is best tailored to their specific needs, and this could in fact reduce their operational resilience and the overall performance of the organisation.

There is a real risk that European businesses and public sector organisations will have to delay migration and make do with legacy systems for a very long time. It is unclear how global operations of EU businesses could be maintained in the long term if the data needs to be localised in Europe, especially when obligations are enforced at the same time for financial services and banking, energy, healthcare, and public sector institutions. Needless to say, given that many, if not most, technological developments continue to take place mainly outside the EU, there is the risk that the EU will become a laggard in the adoption and use of the best available services globally.

To the extent that lack of capacity delays adoption of cloud services, cybersecurity risks for EU governments and critical industries are likely to increase: one of the key results of the US "cloud first" policy initiated in the Obama Administration was that it vastly reduced the number of data centres individual agencies maintained. This consolidation significantly reduced the "surface area" and number of "vectors of attack" that bad actors could exploit to breach sensitive systems. In addition, the very economies of scale that drive the efficiency of cloud computing also apply to cybersecurity, where best-in-class defences for a system can be most effectively deployed, in a manner legacy systems have difficulty matching.

d) EUCS sets out horizontal requirements that will also impact other regulated sectors leading to overlap or duplicative compliance obligations.

Experiences from Russia, China, India, and Vietnam show that data localisation policies are extremely complex and difficult to comply with.[28] Experts across industries agree that the proposed immunity requirements in the EUCS will be difficult to implement and enforce, and therefore will inevitably lead to higher compliance costs for CSPs in the EU (regardless of their country of origin) and many European companies could start considering leaving the EU internal market.[29] It would simply be too burdensome to deal with many separate laws and guidelines addressed to different entities and activities along with differences in discretion between Member State and European agencies and institutions over how to implement EU provisions at the national level.

Take financial services as an example. In November 2022, the EU Council adopted the Digital Operational Resilience Act (DORA), a regulatory framework intended to improve cybersecurity and network resilience in Europe's financial sector. DORA is a sector-specific regulation for banks and other companies which provide financial services in the EU. Contrary to the EUCS and NIS2, DORA formulates clear standards and ensures a "supervisory right of access" for financial service providers from non-EU countries without imposing immunity requirements. Also, DORA is a regulation adopted in ordinary legislative procedure. It is risk based and does not include any such sovereignty requirements. If the EUCS would be adopted with the sovereignty requirements, it would be an implementing act that is amending a secondary EU legislation. However, an implementing act cannot alter a regulation, such as DORA, and thus would contradict EU legal principles, including principles of subsidiarity and proportionality.

It remains unclear how the proposed EUCS regulations, especially Annex J requirements, relate to DORA and how they would impact value chains in the financial sector. The only impact that can already be foreseen is an increase in legal uncertainties: EUCS requirements with risk class "high" would impose two special conditions on the provision of cloud services: (a) cloud service providers (CSPs) would have to have their main office within the EU and (b) the direct provision of cloud services by CSPs would be prohibited if their corporate interests are controlled by non-EU countries. From a finance-sector perspective, this approach represents a clear departure from the basic principles of DORA as Articles 18 and 21 NIS2 provide for a possible obligation to use certification schemes such as the EUCS for "essential entities" and "important entities" including many financial services operators. It is not clear if a lex specialis clause would address concerns with potential conflicts.

---

[28] See, e.g, Karpukhin, A. E. and Sivkova, D.A. (2017). How to comply with the Russian requirements on localisation of personal data. Article of November 2017. Available at https://www.financierworldwide.com/how-to-comply-with-the-russian-requirements-on-localisation-of-personal-data#.Y7-1Hy8w1eg. Also see FPF (2022). Report on demystifying data localization in China. 21 February 2022. Available at https://fpf.org/blog/new-fpf-report-demystifying-data-localization-in-china-a-practical-guide/.

[29] See, e.g. Digital Europe (2022). Joint letter on 'sovereignty requirements' in candidate European Cybersecurity Certification Scheme for Cloud Services. 16 June 2022. Available at https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2022/06/DIGITALEUROPE_Joint-letter-on-'sovereignty-requirements-in-candidate-EUCS.pdf. Also see BDI (2022). European Cybersecurity Certification Scheme for Cloud Services (EUCS): German Industry's 7 key recommendations, 17 June 2022. Available at https://english.bdi.eu/publication/news/european-cybersecurity-certification-scheme-for-cloud-services-eucs/.

Depending on how Member State authorities interpret these terms, the EUCS rules would severely limit the freedom of the EU financial market to work with suppliers of their choice. A key problem, which is not limited to the financial sectors, is that it is still unclear which data, business models, and value chain ingredients will fall under which safety standards/levels within the proposed EUCS / NIS2 framework and how this process of classification would be specifically designed. It is only clear that the inclusion of such requirements would mean that certain CSPs would not be able to obtain high security level certification.[30]

European financial services clearinghouses note that they often outsource certain workflows to cloud services providers to increase their operational resilience. Cloud service providers *"can offer solutions with higher operational resilience by providing robust IT infrastructure, allowing geographical diversity of data centres, through enhanced disaster recovery and by mitigating legacy technology risks, such as single-points- of-failure. By outsourcing to CSPs, CCPs benefit from increased operational resilience, improved efficiency and scalability, and higher flexibility and innovation capabilities. The use of CSPs allows for more efficient and timely workstreams and increases the flexibility to boost cloud capacities when necessary."* For cybersecurity risks, it is highlighted that European clearinghouses *"are core to the financial stability of the EU, and because of this operational resilience is increasingly central to ensuring well-functioning EU financial markets. Over the recent years, financial markets are facing a rise in the number and sophistication of cyber-attacks. As such, ensuring cybersecurity and operational resilience is at the heart of CCP operations."*[31] Localisation barriers, it is concluded, could:

- force European financial services providers to exit longstanding contracts with existing non-EU based CSPs without suitable alternatives,
- make it more difficult for European companies to operate and compete globally,
- reduce EU companies' operational and cyber resilience,
- deter innovation and weaken security by hindering the exchange of information, and
- provoke localisation rules from other jurisdictions, which could severely impact EU service provision globally and should be avoided.

The potential for EUCS to be applied to cloud computing services offered to financial services (if they are deemed critical infrastructure) underscores the reductio ad absurdum consequences implicit in the very concept of immunity: whether or not a foreign financial service supplier migrates workloads to the cloud or not, that very same data, by virtue of being controlled by a foreign company, raises the very same issues of immunity, the solution to which can only mean banning foreign suppliers of financial services.

A cross-industry perspective is provided by Germany's Confederation of Industry (BDI), which calls for profound changes in the proposed EUCS framework. It is highlighted that, in principle, *"companies should have the choice whether they certify their cloud services against the EUCS or*

[30] See, e.g. Bitkom (2022). Stellungnahme zur Bedeutung des Zusammenspiels von EUCS / NIS / DORA für den Finanzmarkt, 29 November 2022. Available at https://www.bitkom.org/Bitkom/Publikationen/Stellungnahme-Bedeutung-Zusammenspiel-EUCS-NIS-DORA-Finanzmarkt.

[31] European Association of CCP Clearing Houses (2022). EACH Letter – EACH members considerations and recommendations on EU Cybersecurity Certification Scheme for Cloud Services, August 2022. Available at https://eachccp.eu/wp-content/uploads/2022/08/EACH-Letter-Cybersecurity-Certification-Scheme-for-Cloud-Services-August-2022-2.pdf.

other relevant standards (for example European harmonised standards).” Making EUCS mandatory should only be an option if voluntary approaches turn out to be ineffective. BDI argues that the proposed EUCS and the NIS2 Directive would actually increase regulatory fragmentation in the EU as individual Member States would be encouraged to *“make a certification based on the EUCS mandatory for private entities falling within the scope of NIS2 and national laws implementing NIS2.”* Immunity requirements *“would have far-reaching consequences for industry and the European cloud market”*, resulting *“in increasing operational costs with effects on the competitiveness of the companies concerned.”* BDI also cautions the lack of advanced cloud services provider in the EU: *“certain CSPs will no longer be able to provide services in this segment. This would mean that at least in the short- to medium-term, European industry would be confronted with fewer options in this market segment.”*[32]

Importantly, BDI highlights that data localisation for “high assurance services” could become a cross-industry standard: *”Even though it is not possible at this stage to predict exactly for what percentage of cloud services this certification level will be relevant, it is not unlikely that the assurance level ‘high’ will rather emerge as the de-facto-standard for cloud security, as legal and regulatory requirements in different sectors as well as customers’ expectations might make certifications according to the assurance level ‘high’ in practice indispensable.“*

3. CYBERSECURITY IMPLICATIONS

EUCS immunity requirements increase cloud adopters’ exposure to cybersecurity risks. EUCS provisions, thus, fail the proportionality test (see further below).

Rather than protecting cybersecurity, data localisation often creates obstacles to an integrated management approach for cybersecurity risks. Mandatory data localisation “pervasively limits provision of cybersecurity-related services by third parties, a global market of roughly USD 200 billion currently. Notably, data localisation laws supported in the name of cybersecurity often severely undermine cybersecurity – purchasers in the locality are deprived of best-in-breed cybersecurity services, thereby making them systematically easier targets for attackers.”[33]

In view of “defensive cybersecurity”, which is a key objective of ENISA and the proposed EUCS, mandatory data localisation reduces the effectiveness of purchasing globally available cybersecurity-related services and systematically disrupts information sharing. For example, with mandatory localisation of non-personal data, business auditing activities could become unlawful, intrusion monitoring would become more difficult, and the effectiveness of organisation-wide approaches for reducing cybersecurity risks would be reduced.[34]

---

[32] BDI (2022). European Cybersecurity Certification Scheme for Cloud Services (EUCS): German Industry’s 7 key recommendations, 17 June 2022. Available at https://english.bdi.eu/publication/news/european-cybersecurity-certification-scheme-for-cloud-services-eucs/.

[33] See Swire, P. and Kennedy-Mayo, D. (2022). “The Effects of Data Localisation on Cybersecurity, 12 September 2022. Georgia Tech Scheller College of Business Research Paper No. 4030905. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4030905.

[34] See Swire, P. and Kennedy-Mayo, D. (2022).

Country of headquarters and foreign ownership restrictions in the proposed EUCS risk removing global frontier cybersecurity technologies from Member State markets. Many internationally operating CSPs are leading providers of cybersecurity solutions to public sector users and critical industries globally. Excluding these and other EU and non-EU companies from EU Member States could result in a long-lasting security deficit of EU cloud adopters vis-à-vis organisations that are still able to use reliable and often best-practice cloud services offered by providers from outside EU Member States. Due to lacking EU capacities in advanced cloud services, immunity provisions in the EUCS would require a significant overhaul of existing cloud and network infrastructure, hindering affected organisations in the Member States from attaining state of the art cybersecurity. Given that the overall scope of EUCS' high risk assurance certification is unclear and difficult to project, EUCS provisions put at risk the cybersecurity and resilience of a large number of essential entities unless implementation is extended to many years, if not decades.

EUCS data localisation requirements would prevent the sharing of security data between security operations centres in EU Member States and those in non-EU countries. This would severely inhibit threat detection by creating loopholes that malicious hackers and foreign espionage agencies could exploit.

Rigorous data localisation would deprive local adopters and cloud operators of key data resilience strategies, e.g., setting-up data storage and processing capacities in locations immune to natural disasters or shielded in case of armed conflicts. It would also prevent cloud operators from "sharding", a common cybersecurity practice of dividing data into pieces of independently useless data and scattering these pieces across secluded storage locations.

Finally, given the profound lack of ICT professionals in the EU, the requirement to have local customer support would likely negatively impact the resilience of EUCS-certified services.[35] For these professionals – of which many are the most high-paying engineering jobs – European companies already compete with other regions of the world. It is unrealistic to assume that an EUCS on its own will attract highly qualified engineers to Europe. On the contrary, realistic and responsible politics should strive to create the conditions for cybersecurity to be provided effectively by the most capable companies and employees irrespective of their country of headquarter and origin respectively.

[35] See, e.g. Euractiv (2022). Looming talent shortage will limit cybersecurity efforts in Europe, French agency warns. 8 June 2022. Available at https://www.euractiv.com/section/cybersecurity/news/looming-talent-shortage-will-limit-cybersecurity-efforts-in-europe-french-agency-warns/.

4. DISCRIMINATION BY DESIGN AND THE TRADE POLICY IMPLICATIONS

Key EUCS Annex J provisions are discriminatory by design. The nature of effective foreign control, local establishment, and data localisation in the proposed EUCS corresponds to policies imposed by several authoritarian regimes such as China, Russia, Vietnam, and Saudi Arabia. By contrast, the world's most economically developed countries – typically mature democracies – abstain from imposing far-reaching bans and restrictions on the free cross-border flow of non-personal data.

It should be noted that WTO law and trade agreements recognise the right to regulate in the interest of "national security". However, it is striking that in the area of cross-border data flows the very countries that rely on this exception are those that restrict civil liberties, freedom of expression, freedom of the press, and basic economic freedoms the most (see Table 3).

TABLE 3: QUALITY OF POLITICAL AND ECONOMIC INSTITUTIONS OF COUNTRIES WITH/ WITHOUT HAVING IN PLACE FAR-REACHING BANS TO TRANSFER DATA AND LOCAL PROCESSING REQUIREMENTS

Countries WITH far-reaching ban to transfer and local processing requirement in place									
	Ecoomic freedom	Regula-tory trade barriers	Non-tariff trade barriers	Quality of legal sys-tem and property rights	Corrup-tion in the public sector	Rule of law	Internet censor-ship	Freedom of expres-sion	Media self-censor-ship
Vietnam	6,42	5,32	4,88	5,14	3,9	4,6	5,82	2,25	2,5
Saudi-Arabia	6,78	6,8	6,18	6,81	5,3	5,45	4,6	1,75	1,07
Russia	6,62	6,06	5,19	5,13	2,9	3,97	6,8	4,5	3,31
China	6,27	7,22	5,81	5,12	4,5	4,45	2,2	2,25	1,33
Countries WITHOUT far-reaching ban to transfer and local processing requirement in place									
	Ecoomic freedom	Regula-tory trade barriers	Non-tariff trade barriers	Quality of legal sys-tem and property rights	Corrup-tion in the public sector	Rule of law	Internet censor-ship	Freedom of expres-sion	Media self-censor-ship
United States	7,97	8,16	6,52	7,56	6,7	6,75	9,68	10	8,22
United Kingdom	7,71	7,97	6,62	7,75	7,8	7,51	9,8	10	8,69
Sweden	7,56	8,48	7,03	7,93	8,5	8,61	9,94	10	8,86
Nether-lands	7,75	8,56	7,15	8,35	8,2	8,23	9,91	10	81,7
Germany	7,65	7,87	6,56	7,75	8	8,32	9,33	10	8,96
France	7,33	8	6,01	7,19	7,1	6,84	9,86	7,5	9,69

Sources: Digital Trade Integration Project, Fraser Institute Human Freedom Index, Fraser Institute Index of

Economic Freedom in the World, Amnesty International Corruption Perception Index. Scale: 0 indicating worst performance – 10 indicating best performance. Ranking in Corruption Perception Index divided by 10 to match scale.

In practice, assessing when data transfers may be made to third countries and which data localisation requirements apply is extremely complex, with many separate laws and guidelines targeting different entities and activities. China's Cybersecurity Law, for example, requires that personal information of Chinese citizens and important data collected by critical information infrastructure operators (CIIOs) must be stored within mainland China. Additionally, guidance issued by China's Cyberspace Administration for data transfers outbound from China expands this requirement to all "network operators", covering most, if not all, cloud service providers. Many more measures were imposed by separate legal acts on financial data, telecommunications data, online gaming data, healthcare data, and transport data.

EU policymakers are aware of the political ramifications and economic consequences of data localisation policies. It is a stated ambition of the EU to champion its trade interests using core principles of the rules-based international trading system.[36] Recognising the economic importance of the data economy and the potential interference of data policies with political ambitions for international trade commitments and principles, particularly non-discrimination, the least trade-restrictive policy option and proportionality, the EU itself is a strong promoter of the free flow of non-personal data. While in its recent FTAs (e.g. with Japan and the UK) the EU has carefully negotiated broad discretion with respect to measures it can take to protect privacy, it has taken on binding commitments to curtail that discretion with respect to non-personal data. As prominently stated in the EU's "Regulation on the free flow of non-personal data in the European Union", the EU wants to ensure free flow of data in the EU, allowing companies and public administrations to store and process non-personal data wherever they choose."[37] It is explicitly stated that

"Data value chains are built on different data activities: data creation and collection; data aggregation and organisation; data processing; data analysis, marketing and distribution; use and re-use of data. The effective and efficient functioning of data processing is a fundamental building block in any data value chain. However, the effective and efficient functioning of data processing, and the development of the data economy in the Union, are hampered, in particular, by two types of obstacles to data mobility and to the internal market: data localisation requirements put in place by Member States' authorities and vendor lock-in practices in the private sector." (recital 2 of Regulation (EU) 2018/1807)

"The freedom of establishment and the freedom to provide services under the Treaty on the Functioning of the European Union ('TFEU') apply to data processing services. However, the provision of those services is hampered or sometimes prevented by certain national, regional or local requirements to locate data in a specific territory." (recital 3 of Regulation (EU) 2018/1807)

---

[36] See, e.g., European Commission (2021). Trade Policy Review – An Open, Sustainable and Assertive Trade Policy. 18 February 2021. Available at https://trade.ec.europa.eu/doclib/docs/2021/february/tradoc_159438.pdf.

[37] See Regulation (EU) 2018/1807.

The EU's Regulation on the free flow of non-personal data establishes the same principle of free movement within the EU for non-personal data except when a restriction or a prohibition is justified by public security reasons. Accordingly, based on Articles 4 and 52 of the Treaty on the Functioning of the European Union (TFEU), national security is the sole responsibility of each Member State and covers the investigation, detection, and prosecution of criminal offences as well as the functioning of institutions and essential public services. However, in compliance with the principle of proportionality enshrined in Article 5 TFEU, data localisation requirements that are justified on grounds of public security must be suitable for attaining the objective pursued and should not go beyond what is necessary to attain that objective.[38]

Similar limitations apply for key WTO agreements: the General Agreement on Trade in Services (GATS) and the Agreement on Government Procurement (GPA), and the currently negotiated WTO E-Commerce Agreement, where the EU is a known opponent to national restrictions to the free cross-border flow of non-personal data in the recent past (Table 4).[39]

TABLE 4: RELEVANT COMMITMENTS IN WTO LAW

WTO E-Commerce Agreement (under negotiation)	WTO GATS	WTO GPA
"Cross-border data flows shall not be restricted by: (a) requiring the use of computing facilities or network elements in the Member's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Member; (b) requiring the localisation of data in the Member's territory for storage or processing; (c) prohibiting storage or processing in the territory of other Members; (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Member's territory or upon localisation requirements in the Member's territory".	GATS requires any Member shall to services and service suppliers of any other Member treatment no less favourable than that it accords to like services and service suppliers of any other country. GATS contains a right to market access in sectors including computer and related services. The EU has committed to national treatment and most-favoured nations obligations, notably in its GATS schedule of commitments and FTAs services schedules of commitments notably under "computer related services".	GPA requires that any state party treat foreign companies supplying cloud services on a cross-border basis to government entities no less favourably than locally established suppliers. For the EU, GPA Annex 5 explicitly covers computer and related services covered by the GPA.*

* See WTO GPA coverage schedules. Available at https://www.wto.org/english/tratop_e/gproc_e/gp_app_agree_e.htm.

Both, GATS (which applies to commercial services, e.g., "critical industries" for which the EU has made commitment) and GPA (which applies to government procurement, for which the EU and

[38] See, e.g. recital 19 of Regulation (EU) 2018/1807.

[39] Regarding the EU's position in WTO E-Commerce Agreement negotiations, see EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, 26 April 2019. Available at https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/22.pdf&Open=True. Also see European Parliamentary Research Service (2020). WTO e-commerce negotiations, October 2020. Available at https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/659263/EPRS_ATA(2020)659263_EN.pdf: "The EU proposal seeks to balance the free flow of data for business purposes with a commitment to personal privacy, which it considers a fundamental right. Enterprises should not be restricted by requirements to localise data or computer facilities in a given member's territory."

Member States have full cloud computing commitments), are agreements that allow exceptions to specified public policy objectives including national security. GATS, in addition, offers broader exceptions, including privacy, and other public policy interests, whereas GPA exceptions are a narrower, closed list. While there is no WTO jurisprudence in applying the GPA and GATS to cloud services, the outcome of any potential dispute settlement proceeding would critically rely on EUCS provisions' compliance with key international trade commitments and principles, such as non-discrimination, the least trade-restrictive policy option and, related proportionality (i.e., the key aspects of national treatment and MFN).

Regarding the principle of non-discrimination, key EUCS provisions are discriminatory by design: Annex J requirements do not allow globally operating cloud service providers to qualify for the highest assurance level of cybersecurity certification. Only majority EU-owned providers would qualify under the current approach.

Regarding the principle of proportionality, control and ownership restrictions for cloud services providers and the blanket obligation to localise data within EU borders and restrict international trade seem to be out of any reasonable proportion. The trade-restricting measures proposed in the EUCS framework are significantly greater than those of alternative measures to achieve EU cybersecurity objectives and immunity from non-EU laws and jurisdictions.

EUCS provisions also fail the proportionality test for immunity provisions: there are alternative ways to better protect EU cloud adopters from being exposed to the law of foreign jurisdictions.

Protecting cloud providers and adopters from law enforcement in non-EU jurisdictions is an important political objective. However, dealing with this problem in the proposed EUCS, which is intended to serve as a voluntary scheme, is in several respects not the right approach. Excluding all foreign companies from operating in the EU requires a sound legal and economic impact analysis and should be decided through a formal legislative procedure at the EU level. By contrast, ENISA's EUCS certification should be limited to technical and transparency issues and remain consistent with the Cybersecurity Act.

Foreign ownership restrictions and local establishment requirements would exclude many foreign and local cloud services providers from the possibility of making offerings in a large market segment of advanced digital services in the EU. Considering the adverse implications for cybersecurity, business activities, innovation, and trade ramifications, ENISA and the European Commission should consider a complete removal of Annex J requirements. Removing Annex J requirements would still allow the EU to enforce a harmonised cybersecurity certification across the EU Member States on the basis of all three assurance levels.

Immunity requirements for non-personal data should generally be addressed in bilateral initiatives or agreements requiring a company that sought to offer services of the highest level of sensitivity to be headquartered in a country granted adequacy.[40] To the extent that EUCS aims to provide

[40] See European Commission (2023). Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection. Available at https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

a shield against authoritarian and non-rule-of-law countries like China, whose ability to disrupt governmental industries is a credible concern, the measure is unnecessary, since no such countries are part of the GPA and thus the EU is within its rights, under the GPA, to deny access to companies based in such jurisdictions.

As concerns the Transatlantic relationship, immunity requirements for non-personal data should be addressed in bilateral talks such as the EU-US Trade and Technology Council (TTC) and, the Commission's recent (draft) adequacy decision based on the US' "Enhancing Safeguards for United States Signals Intelligence Activities Executive Order".[41] Another avenue could be an EU-US Cloud Act agreement, which would set legal clarity for European and US law enforcement on data access for both in each other's jurisdiction. In any case, ENISA and the European Commission should postpone EUCS negotiations until Annex J immunity requirements have undergone comprehensive legal and economic impact assessments, followed by adequate political and legislative proceedings.

Failure to allow US-headquartered CSPs to continue to serve customers across the EU could result in significant retaliatory action, based either on WTO dispute settlement or measures determined unilaterally based on an investigation pursued under Section 301 of the Trade Act of 1972. Under U.S. statute, the US Trade Representative can "impose duties or other import restrictions on the goods of, and, notwithstanding any other provision of law, fees or restrictions on the services of, such foreign country for such time as the Trade Representative determines appropriate" to "eliminate an act, policy, or practice" that discriminates against US-based companies

Section 301 can be a powerful tool, assuming a political willingness to use it.[42] The previous US Administration announced retaliatory tariffs against four EU countries that implemented discriminatory taxes on digital services provided by US technology companies. Retaliatory tariffs would have covered approx. USD 3 billion worth of traded goods annually (see Table 5).[43]

---

41 See European Commission (2022). Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US. 13 December 2022. Available at https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631. Also see The White House (2022). President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework, 7 October 2022. Available at https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/.

42 The motivation behind creating and strengthening mechanisms for potential retaliation had been primarily to expand US export opportunities and to induce other nations to reduce trade barriers – not to punish or inflict economic harm on trading partners. There have been 130 cases under section 301 since its enactment in the Trade Act of 1974, of which 35 have been initiated since the WTO's establishment in 1995. Historically, section 301 cases have targeted primarily the EU, which accounts for about 30% of all cases – concerning mostly agricultural trade.

43 Austria, France, Italy and Spain, and the UK, which has left the EU. On October 21, 2021, the US announced it will terminate tariffs it had threatened against Austria, France, Italy, Spain, and the United Kingdom in exchange for removing digital services taxes imposed on large US technology firms. See USTR (2021). USTR Announces, and Immediately Suspends, Tariffs in Section 301 Digital Services Taxes Investigations, 2 June 2021. Available at https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/june/ustr-announces-and-immediately-suspends-tariffs-section-301-digital-services-taxes-investigations.

TABLE 5: US RETALIATORY TARIFFS TO DIGITAL SERVICES TAXES (DSTs) IMPOSED BY EU COUNTRIES

	US retaliatory Tariffs to Digital Services Taxes imposed by EU(28) countries				Share in EU-US services trade	
Country	**Affected items**	**Value of Affected U.S. Imports (2019)**	**Tariff Rate**	**Tarif cost burden**	**Share in EU28 services exports to US**	**Share in EU28 services imports from US**
Austria	classware, binocu-lars, refrigerators ect.	65,207,231	25%	16,301,808	0.70%	0.80%
France	cosmetics, handbags etc.	1,296,969,068	25%	324,242,267	9.70%	8.60%
Italy	textiles anf footwear etc.	385,757,538	25%	96,439,385	3.30%	3.80%
Spain	sea food, tetiles, footware etc.	323,435,820	25%	80,858,955	3.10%	2.10%
UK	textiles, footwear, furniture etc.	886,553,092	25%	221,638,273	30.60%	17.90%
Total		**2,957,922,749**		**739,480,687**	**47.40%**	**33.20%**

Source: USTR announcements on Section 301 – Digital Services Taxes, available at https://ustr.gov/issue-areas/enforcement/section-301-investigations/section-301-digital-services-taxes. Trade data from Eurostat.

It is difficult to estimate the value of EU cloud services imports from the US that would in turn determine the level of Section 301 retaliation against EUCS provisions. However, it is clear that local establishment requirements and foreign ownership restrictions would by design discriminate against US cloud providers that currently serve more than three quarters of the EU market.

Strict local establishment obligations and rigorous foreign ownership limitations could have farther reaching effects than, for example, taxes on digital services. US retaliation could, therefore, substantially exceed the value of covered trade determined for retaliatory tariffs against EU taxes on digital services. Assuming an EU cloud market size of USD 40 billion annually[44] and a share of high assurance services of 10%, an EUCS immunity provision would effectively ban services from the three largest suppliers worth USD 2.9 billion. Depending on US preferences, a 25% retaliatory tariff could be imposed on at least about USD 12 billion worth of goods (or equivalent restrictions for EU services exports to the US). Assuming a share of high assurance services of 20%, the value of trade covered by US retaliation would double. It should be noted that the list of "sectors of high criticality" allows for a high level of discretion regarding activities and services considered critical by Member State authorities. In addition, the growth and emergence of new technologies and business models, such as IoT in the energy and healthcare sectors and autonomous driving in the transport sector, could in the future lead to an expansion of the list of critical sectors.

[44] Recent data from Synergy Research Group shows that the European cloud market is now over five times as big as it was in early 2017, reaching EUR 10.4 billion (US$10.9 billion) in the second quarter of 2022. See Synergy Research (2022). European Cloud Providers Continue to Grow but Still Lose Market Share, 27 September 2022. Available at https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share.

5. CONCLUSION

EU Member States should call on the EU's ENISA and the European Commission to abandon immunity requirements in the proposed EU Cloud Certification Scheme.

With immunity requirements in the EUCS, the EU risks opening a Pandora's box, paving the way for data localisation, foreign ownership restrictions, and local establishment requirements in digital markets and industries globally and rising trade tensions. ENISA's current proposal could increase policymakers' appetite for data localisation in the EU. It would empower the European Commission and Member State authorities to exclude foreign businesses from domestic cloud services markets and set a dangerous precedent for any data-intensive sector.

EUCS immunity requirements would increase cloud adopters' exposure to cybersecurity risks. Country of headquarters and foreign ownership restrictions in the proposed EUCS risks removing global frontier cybersecurity technologies from Member State markets. EUCS data localisation requirements would prevent the sharing of security data between security operations centres in EU Member States and those in non-EU countries. This would severely inhibit threat detection by creating loopholes that malicious hackers and foreign espionage agencies could exploit. Moreover, rigorous data localisation would deprive local adopters and cloud operators of key data resilience strategies, e.g., setting-up data storage and processing capacities in locations immune to natural disasters or shielded in case of armed conflicts.

Key EUCS Annex J provisions are politically motivated and discriminatory by design. They could provoke retaliatory measures by EU trading partners, either unilaterally or through WTO Dispute Settlement. ENISA's cloud certification scheme should be limited to technical and transparency requirements. Immunity requirements for non-personal data should be addressed in bilateral initiatives or agreements requiring a company that has sought to offer services for the highest level of sensitivity to be headquartered in a country granted adequacy, or (for the US) is participating in the upcoming Trans-Atlantic Data Privacy Framework.

EU suppliers are currently in no position to manage a broad-based transition to cloud, and thus such requirements would delay significant efficiency and security gains that current foreign suppliers could offer. In contrast to large countries, these negative impacts would likely be more pronounced for smaller EU Member States, which lack the presence of large cloud providers and generally rely much more on an open international trading regime for advanced digital services.

As reiterated in a recent policy statement, several EU Member States have concerns about the vagueness, mandatory nature, lack of flexibility, legal challenges, and lack of consistency with other certification schemes.[45] They are, thus, calling on the European Commission to properly assess the economic impacts of sovereignty requirements and to what extent they would be incompatible with trade law.

Excluding foreign companies from operating in the EU would have far-reaching consequences. If that is the intent, it should require a sound legal analysis and be decided through a formal legislative procedure at the EU level.

Disclaimer

This is an independent report commissioned by the Computer & Communications Industry Association (CCIA Europe). The opinions offered herein are purely those of the author. They do not necessarily represent the views of CCIA Europe.

[45] See, e.g. Euractiv (2023). EU countries seek way out of impasse on sovereignty requirements for cloud services. Article from 30 January 2023. Available at https://www.euractiv.com/section/cybersecurity/news/eu-countries-seek-way-out-of-impasse-on-sovereignty-requirements-for-cloud-services/. Reference is made to a "Joint Paper on alternative solutions regarding the issue of Independence to non-EU law in the context of EUCS, dated 23 January". The non-paper outlines six potential scenarios which can be broadly divided in two categories: the first category of scenarios suggests keeping the immunity requirements in the EUCS framework, through additional assurance or evaluation levels within "High" and "Substantial" assurance levels. These create two outstanding problems: first, creating more than three assurance levels seems incompatible with the Cybersecurity Act, which EUCS derives its existence from. Second, when and to whom those immunity requirements would apply would remain largely unpredictable, with vast discrepancies across the EU single market. Another category of scenarios suggest moving this discussion to the political level, either through a new regulation or a directive, an existing proposal, or through the establishment of a so-called trustworthiness evaluation mechanism whereby non-EU vendors would be screened against a set of criteria, defined at EU level, before they can enter or remain in the market. Whether the EU is legally competent to deliver an instrument for governments to use in the name of their own national security, for instance, is questionable. Compliance with EU's trade commitments, and the reduction of cloud offering for European customers are also recurring concerns among all those scenarios.