ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

OCCASIONAL PAPER – No. 04/2023

The Economic Impacts of the Proposed EUCS Exclusionary Requirements

Estimates for EU Member States

By **Dr Matthias Bauer** *and* **Dr Philipp Lamprecht**, *Directors at ECIPE*

EXECUTIVE SUMMARY

The EU Agency for Network and Information Security (ENISA) is proposing a far-reaching "European Cybersecurity Certification Scheme for Cloud Services" (EUCS) to be established in the European Union (EU). According to the latest draft of August 2023, leaked by Politico in September 2023, the proposed EUCS would by design prevent non-European vendors from providing "high assurance level" cloud services in the EU. In this study, we show that the proposed "immunity" requirements, i.e., foreign ownership and headquarter restrictions, local staff requirements, and data localisation would lead to significant losses in Member States' aggregate economic activity and drive a big wedge between economic growth in the EU and the growth of non-EU economies. The projected losses in annual EU GDP will vary from EUR 610 billion to EUR 29 billion within approx. two years of implementation, contingent upon the specific sectoral coverage of high-assurance use cases under the cloud service evaluation level CS-EL4. The results fit into the overall picture of EU digital policy, which has weakened rather than strengthened the competitiveness of EU industries in the past. Our findings align with the broader impacts of EU digital policy, which runs the risk of exacerbating the growth gap and technology disparity between the EU and other advanced economies.

Cloud services have become increasingly popular and integral to Europe's economy. Cloud services are granting businesses of all sizes equal access to global data and resources, stimulating collaboration, and bolstering competitiveness. Advanced cloud services are levelling the playing field in domestic commerce and international trade. Smaller enterprises can harness advanced IT capabilities, particularly cloud-based supply chain management, to streamline their operations. Cloud computing solutions are also playing a crucial role in modernising public services, offering transformative potential for government administrations and service quality.

Cloud services adoption is expected to grow substantially in the years ahead, driven by data analytics, AI applications as well as quantum and edge commuting solutions. The global cloud computing market is on a rapid growth trajectory and is expected to reach some EUR 2,080 billion by 2030. Industry forecasts indicate that cloud services and transversal cloud-based technologies like AI applications, quantum, and edge computing will experience consistent growth in innovation and are increasingly finding broader applications across various industries. Overall, the global market for IT services is highly competitive and dynamic, with global cloud service providers competing against a broad range of IT service providers of varying scale, including on-premises hardware vendors, private and co-located data centre providers and software providers.

Despite showing a trade deficit in international cloud services trade, trade in ICT and digitally enabled services is not a one-way-street for the EU. Recent trade data reveals that the total value of EU exports in digital and digitally enabled services to the rest of the world is roughly equivalent to the total value of EU imports from the rest of the world. This balance in trade is also observed in EU digital trade with the US, where EU exports of ICT services to the US nearly match US exports of digital services to the EU.

The proposed EUCS exclusionary requirements entail various negative consequences. As recognised by the European Commission's latest progress report on digitisation in the EU, European companies have yet to reach the "Digital Decade" targets, especially when it comes to embracing cloud-supported technologies such as AI and big data, as the adoption of digital technologies remains significantly below these objectives.[1] Exclusionary requirements would create operational inefficiencies and increased production costs for cloud services providers and cloud adopters. They would undermine investments in the domestic economy, resulting in reduced international trade, competition, and innovation. The imposition of exclusionary requirements by the EU could create a domino effect of restrictions caused by retaliation and protectionism.

Data localisation and nationality requirements stifle innovation and competition, particularly in data-driven industries. The creation of redundant capacities in the EU would have adverse environmental impacts, including increased energy consumption, land use, and electronic waste. Immunity requirements would increase rather than mitigate cybersecurity risks, creating a security deficit for EU cloud adopters that lose access to proven global risk detection and prevention solutions.

This study provides estimates of potential GDP and industry output effects from the implementation of exclusionary requirements under the proposed EUCS framework.[2] It is shown that the strict "immunity" requirements in the EUCS cybersecurity certification framework would severely limit European customers' access to advanced technologies, innovation and global ICT industry growth trends. The study's findings highlight the significant economic consequences of potential restrictions on access to global cloud services across three scenarios of different sectoral coverage. It is shown that even in the least restrictive scenario, where "immunity" requirements would only be applied to a narrow spectrum of sectors and highly critical use cases, the reduction in the EU's annual GDP could be substantial.

In scenario 1 (broad critical sector coverage), reflecting political demands of the current French government, the EU's annual GDP is projected to decrease by 3.9% when accounting for lost cloud capacities and forgone cloud capacity and productivity growth, within 2 years of implementation. For scenario 2 (medium critical sector coverage) and scenario 3 (narrow critical sector coverage), the estimated annual losses in GDP amount to -2% and -0.2%, respectively. In terms of current EU GDP, annual losses would amount to EUR 610 billion, EUR 317 billion, and EUR 29 billion, respectively, underscoring the significant magnitude of the potential impacts.

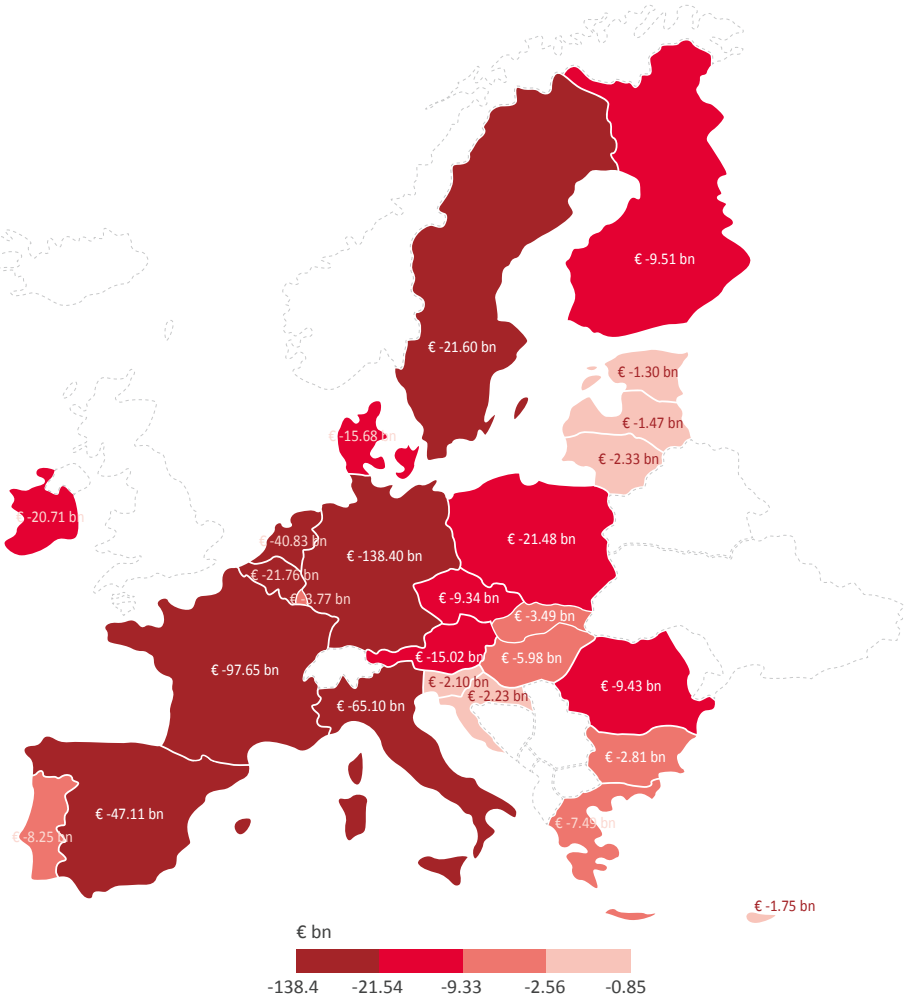
For the broad critical sector coverage scenario, our results also show that the EU's annual GDP losses accumulate over longer periods of time. After 5 years following the implementation of exclusionary EUCS requirements, the annual growth losses for the EU and its Member States remain significant. This is due to the inability of European businesses and the EU's public sector to tap into the worldwide innovation and productivity gains offered by globally accessible

[1] European Commission (2023). Report on the state of the Digital Decade. 27 September 2023. Available at https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade.

[2] EU Agency for Network and Information Security (ENISA) 2023 draft EUCS, version V1.0.335, as of August 2023. This study has been conducted based on the publicly available EUCS draft versions from May and August 23, and is without prejudice to any future versions of the scheme.

technologies and services. For the EU, we estimate the annual GDP loss to be -3.6%, with a trend to further accumulate in subsequent years.

EUCS IMPACT: DISTRIBUTION OF ANNUAL REAL GDP LOSSES, IN BILLION EUR, FOLLOWING 5 YEARS OF IMPLEMENTATION

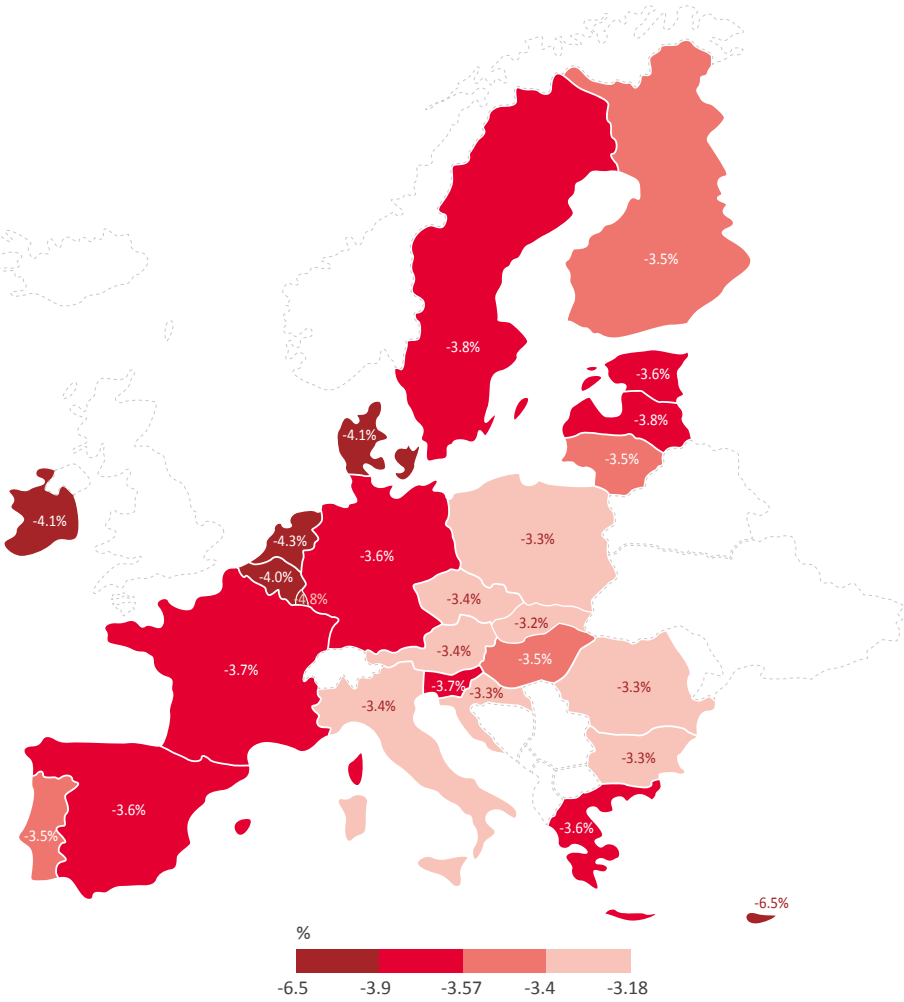


Our estimations also reveal that smaller EU countries would be disproportionately impacted by GDP losses compared to larger countries. In the short-term, small EU countries that are characterised by high-value-added production, including digital and digitally enabled services, and which rely heavily on imported ICT services, show the largest relative losses in annual GDP. In the most restrictive scenario with broad critical sector coverage, short-term losses in aggregate GDP would be most pronounced in Cyprus (-10.2%), Luxembourg (-9.3%), Malta (-8.5%), the Netherlands (-5.8%), Belgium (-5.4%), Denmark (-4.9%), Ireland (-4.7%), and Sweden (-4.6%). The largest EU economies, Germany, France, Italy, the Netherlands, and Spain would generally experience the highest absolute losses in economic output.

Looking into the future, the same pattern will apply following 5 years of the implementation of exclusionary requirements, where Cyprus (-6.5%), Malta (-5%), Luxembourg (-4.8%), the Netherlands (-4.3%), Denmark (-4.1%), Ireland (-4.1%), Belgium (-4%), Latvia (-3.8%), Slovenia (-3.7%), Sweden (-3.8%), Greece (-3.6%), and Estonia (-3.6%) would be the most disproportionately hit.

Following the same 5-year period, Germany, France, Italy, the Netherlands, and Spain would also experience the highest absolute losses in economic output. Over longer time horizons, small and less economically developed countries, such as Bulgaria, Croatia, Greece, Lithuania, Poland, Portugal, and Romania stand to lose long-term growth potential due to exclusionary cloud „immunity" rules, which would have detrimental effects on these countries' economic advancement and efforts towards achieving economic convergence with more prosperous EU nations.

EUCS IMPACT: DISTRIBUTION OF ANNUAL REAL GDP LOSSES, IN %, FOLLOWING 5 YEARS OF IMPLEMENTATION



The study's findings underscore the potential economic repercussions of limiting EU access to global cloud services, with smaller EU countries and sectors reliant on ICT services being particularly vulnerable. The economic impacts extend to larger EU economies as well, emphasising the importance of considering the broader short- and long-term implications of restrictions on cloud and ICT services imports on Europe's economies. EU Member States should thus call on ENISA and the European Commission to abandon discriminatory and potentially far-reaching "immunity" requirements in the proposed cloud certification scheme, EUCS.

TABLE OF CONTENTS

1. INTRODUCTION

The EU Agency for Network and Information Security (ENISA) is proposing a far-reaching "European Cybersecurity Certification Scheme for Cloud Services" (EUCS) to be established in the European Union (EU). According to the latest draft of August 2023, the proposed EUCS would by design prevent non-European vendors from providing "high assurance level" cloud services in the EU.[3]

In a previous ECIPE study, we found that the EUCS exclusionary requirements would have a detrimental impact on Europe in four key areas. They would 1) reduce Europe's cloud computing capacity, 2) lead to fragmentation of the EU digital single market, 3) increase cybersecurity risks, and 4) break international trade rules.[4]

The present study focuses on the economic impacts of immunity requirements. The broad sectoral scope of immunity requirements[5] and substantial room for discretion at Member State level could lead to foreign cloud providers being excluded from public services and a broad range of use cases in commercial sectors. This in turn could result in capacity bottlenecks, significant cost increases for the adopters of cloud services, and deteriorating supply, especially for advanced cloud services.

Data localisation and country of headquarter requirements

Annex I of the latest EUCS draft includes several discriminatory requirements for the highest evaluation levels under the "high" assurance level, known as "CS-EL3" and "CS-EL4":

- "Data localisation" requirement (PUA-02.1H on page 194), applicable under assurance level "CS-EL4": Broad data localisation requirement: all locations for the storage and processing of data shall be located in the EU. Some technical and maintenance support can take place outside the EU only in exceptional circumstances. Cloud services providers shall offer an option to their customers to guarantee that all activities are always performed in the EU. This requirement was also applicable to the assurance level "CS-EL3" in the previous draft EUCS, dated May 2023, but only applies to "CS-EL4" in the latest draft.[6]

- "Country of headquarter" requirement (PUA-04.1H on page 196), applicable under assurance level "CS-EL4": The certified cloud services provider (CSP) must be headquartered in the EU.

---

[3] See ENISA (2023). EUCS – Cloud Services Scheme EUCS, a candidate cybersecurity certification scheme for cloud services, V1.0.335, August 2023.

[4] ECIPE (2023). Building Resilience? The Cybersecurity, Economic & Trade Impacts of Cloud Immunity Requirements. Available at https://ecipe.org/wp-content/uploads/2023/02/ECI_23_PolicyBrief_01-2023_LY07.pdf?_gl=1*1e01wlx*_up*MQ..*_ga*MjA2NTQ2MjI1OS4xNjk1Mzk4OTEy*_ga_T9CCK5HNCL*MTY5NTM5ODkxMi4xLjAuMTY5NTM5ODkxMi4wLjAuMA.

[5] Also commonly referred to as "sovereignty" requirements.

[6] See ENISA (2023). EUCS – Cloud Services Scheme EUCS, a candidate cybersecurity certification scheme for cloud services, V1.0.319, May 2023.

- "Foreign minority and majority ownership" requirement (PUA-04.2H on page 196), applicable under assurance level "CS-EL4": Companies headquartered outside the EU "shall not, directly or indirectly, solely or jointly, hold positive or negative effective control of the CSP applying for the certification of a cloud service." This also includes companies headquartered in Europe with foreign investors and foreign board members. A company which is majority owned by a foreign firm (headquartered outside the EU) cannot certify under the highest evaluation level. The same goes for a company whose foreign investors own minority shares but nonetheless hold veto powers.

- "Local staff" requirement (PUA-03.1Hon page 195), applicable to assurance levels "CS-EL3" and "CS-EL4": Restrictions for employees with direct or indirect access to data. Such employees must be located in the EU or are supervised by an employee who passed an appropriate review and is located in the EU.

– "Expansion of scope" PUA-01.4H (EL3 and EL4 on pages 192 and 193): The CSP shall extend the requirements from PUA-02, PUA-03 and PUA-04 that apply to CSC data to all account data processed throughout the life cycle of the relationship between the CSP and the CSC (pre-sales, operation, maintenance and exit).

– "Investigation request arrangements" PUA-01.5H (EL4 on page 193): The CSP shall define and implement technical, legal and organisational measures, including contractual arrangements, needed to ensure that only investigation requests related to the provision of the cloud service that are issued upon EU law or EU Member State law are considered.

Each and every EU Member State granted substantial authority to prohibit foreign cloud services from participating in the domestic economy

EU Member States are left with significant discretion to mandate discriminatory requirements. For example, the draft scheme provides no specific guidance as to which sector or what workload would fall within the scope of the different assurance levels.

Compared to previous versions of the scheme, the latest proposal introduces a new "evaluation level" CS-EL4 within the assurance level "high", which, however, would not in itself reduce discretion at Member State level:

- Page 29 of the draft EUCS explains that CS-EL4, the highest evaluation level, "is suitable for cloud services that are designed to meet specific (exceeding assurance level CS-EL3) security requirements on services for mission critical data and systems, in particular those related to the fundamental interest to society and that process data, whether personal or not, of particular sensitivity, and the breach of which is likely to result in a breach in the protection of public order, public safety, human life or health, or the protection of intellectual property."

- Page 30 of the draft also refers to broad datasets where the use of "immune" cloud technologies may be mandated, including: "data of particular sensitivity [...] whose breach could reasonably be expected to cause serious injury, for example, loss of reputation or competitive advantage, or to cause extremely grave injury, for example, loss of life." While the terminology around the scope has been slightly changed from the previous EUCS draft, the reference to "loss of reputation or competitive advantage" remains broad and vague and CS-EL4 could apply to any workloads, at member states' discretion. The previous EUCS draft, dated May 2023, referred to "data related to secrets protected by law, for example, secrets relating to [...] the protection of privacy, to medical secrecy, and to trade secrets, which includes the secrecy of production methods, economic and financial information, and of information on commercial or industrial strategies."

The combination of so-called immunity requirements and substantial discretion over national classifications of high assurance (CS-EL4) use cases might encourage some Member State administrations to bar foreign cloud service providers from catering to a wide array of public services and commercial customers. Against this background, the aspirations of the French government give particular cause for concern. The thinking behind EU-wide discriminatory requirements in cybersecurity certification originated in France. ENISA explicitly states in its initial proposal[7] that Annex I (formerly 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).[8] 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 (as of 22 August 2023).[9]

For the French government, the EUCS negotiations, which have been taking place behind closed doors since late 2020, are considered an important opportunity to establish the French legal framework for the entire EU and to expand its scope to the entire European economy. Recent statements by the French Minister for Digital Transition and Telecommunications, Jean-Noël Barrot, indicate that the French government wants exclusionary requirements to be adopted well beyond public authorities and OVIs. On June 1, 2023, the Minister spoke about EUCS in France's national assembly arguing that European countries must in the future comply with the French model. Barrot said that the latest EUCS draft to a large extent is a copy of France's SecNumCloud: "Nothing has changed, and nothing should change." In strong rhetoric Minister

---

7 See V1.0.220 from 2022. References made in Annex J: Independence from non-EU laws.

8 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.

9 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 as of 22 August 2023. Available at 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/.

Barrot argued that the "battle is not over" and that "it is vital that we win our case". Finally, Minister Barrot stated that the French government still supports extending exclusionary requirements well beyond procurement, to critical infrastructure and other large parts of the economy. The Minister admitted, however, that France would not be pushing for an extension yet because of optics as it would provide reasons for European governments to oppose the scope of the scheme.[10]

Earlier, in September 2022, Bruno Le Maire, France's Minister of the Economy, already said publicly: "I also want private companies to make a greater commitment in securing their data. And I think we need to start off on a voluntary basis. But I say this very seriously: if our companies, which have extraordinarily sensitive data, were not free to take advantage of this offer to secure their data, I can't rule out the possibility that, at some point, we'll have to adopt a mandatory standard to protect our industrial sovereignty and protect our independence."[11]

It is important to note that the provisions of the latest version of the EUCS could be adopted by the European Commission through an implementing act on the basis of Article 49(7) of the EU Cybersecurity Act.[12] ENISA is indeed following a formal request from the European Commission, which is considering mandatory cybersecurity certification in several EU policies targeting providers of ICT products and services in the EU.[13] These include the EU Cybersecurity Act (CSA)[14] and the Network and Information Security (NIS2) Directive[15], and the proposed Data

[10] Portail vidéo de l'Assemblée nationale (2023). Speech by the French Minister for Digital Transition and Telecommunications, Jean-Noël Barrot. Available at https://videos.assemblee-nationale.fr/video.13515356_64783e7190d52.1ere-seance--programmation-militaire-pour-les-annees-2024-a-2030-suite-1-juin-2023.

[11] Le ministère de l'Économie et des Finances (2022). Discours de Bruno Le Maire sur la stratégie nationale pour le Cloud. 12 September 2022, Strasbourg. Available at https://presse.economie.gouv.fr/download?id=99457&pn=116%20-Discours%20de%20Bruno%20Le%20Maire%20sur%20la%20stratégie%20nationale%20pour%20le%20Cloud.pdf.

[12] An implementing act under EU law is a mechanism through which the European Commission can further specify the details or technical aspects of a broader legislative framework. A delegated act allows the European Commission to supplement or amend certain parts of a legislative act adopted by the European Parliament and the Council of the European Union. According to Article 49.7 of the EU Cybersecurity Act, "[t]he Commission, based on the candidate scheme prepared by ENISA, may adopt implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services and ICT processes which meets the requirements set out in Articles 51, 52 and 54. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2)." See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881.

[13] 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."

[14] 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."

[15] According to Article 24.1 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 par- ties, 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."

Act[16], and the proposed Cyber Resilience Act (CRA)[17].[18] 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. Accordingly, even if 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.[19] Governments and the European Commission have full discretion to mandate any assurance level in national or EU laws.[20]

Key EUCS Annex I provisions are discriminatory by design. The nature of effective foreign control, local establishment, and data localisation in the latest EUCS proposal corresponds to policies imposed by several authoritarian regimes such as China and Russia.[21] 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 personal and non-personal 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.[22] 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."[23] Similar considerations 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 personal

---

16 Article 27 compels cloud computing providers to take all reasonable technical, legal and organisational measures, including contractual arrangements to "prevent international trans- fer 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.

17 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 Cyber- security 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.

18 Also see Bauer (2023). Building Resilience? The Cybersecurity, Economic & Trade Impacts of Cloud Immunity Requirements. ECIPE Policy Brief 01/2023. Available at https://ecipe.org/publications/resilience-cybersecurity-economic-trade-impacts-cloud-immunity/.

19 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.

20 While NIS2 does say EC needs to adopt a delegated act to identify which sector is required to use an EU certification scheme, the EU has already set a precedent with the eIDAS regulation (establishing a framework for a European Digital Identity), whereby any regulation / directive may mandate a certification scheme, or any assurance level of such scheme Member States consider appropriate like: "The revised regulation should leverage, rely on, and mandate the use of relevant and existing cybersecurity act certification schemes to certify the compliance of wallets with the applicable cybersecurity requirements." See https://www.consilium.europa.eu/en/press/press-releases/2023/06/29/council-and-parliament-strike-a-deal-on-a-european-digital-identity-eid/.

21 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.

22 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.

23 See Regulation (EU) 2018/1807.

and non-personal data in the recent past.[24] Also, in July 2023, the European Commission adopted its adequacy decision for the EU-US Data Privacy Framework. Based on this adequacy decision, personal data can flow freely from the EU to companies in the United States that are part of the Data Privacy Framework. The adequacy decision followed the adoption of US safeguard measures codified under US law, which apply to all data transfers under the EU's General Data Protection Regulation (GDPR) to companies in the US, regardless of the transfer mechanisms used.[25]

Recognising the substantial room for national political discretion over the exclusion of foreign cloud services providers, this study discusses and estimates the GDP and production effects of three implementation scenarios reflecting different levels of restrictiveness. The paper is organised as follows:

- Based on a rich account of data, Section 2 discusses the economic importance of access to global cloud services solutions for EU Member States.
- Accounting for the definition of "immunity" requirements in the EUCS proposal from August 2023, Section 3 discusses potential impact of "immunity" requirements.
- Section 4 provides an overview of key assumptions and the modelling approach before presenting the findings of the estimations.
- Section 5 concludes with policy recommendations.

2. THE ECONOMIC IMPORTANCE OF ACCESS TO CLOUD AND DATA SERVICES

Cloud computing and data processing capacities fuel Europe's economic development, drive digital innovation, and help EU businesses to maintain a competitive edge in global markets. Advanced cloud services technologies facilitate international economic cooperation and grant access to cutting-edge technology. Below we discuss the economic importance of access to cloud and data services solutions in more detail.

2.1. Cloud Services Adoption in the EU

Cloud services level the playing field for businesses of all sizes, reducing the barriers to entry in international trade. Cloud solutions also offer businesses a platform to easily access and exchange data, applications, and resources from any location around the globe. Enhanced global accessibility fosters improved communication and collaboration among trade partners, facilitating seamless international operations for businesses. Smaller businesses in particular

[24] 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. "Enterprises should not be restricted by requirements to localise data or computer facilities in a given member's territory. At the same time, members need to be free to adopt rules that protect personal data and privacy, as they deem necessary."

[25] European Commission (2023). Commercial sector: adequacy decision on the EU-US Data Privacy Framework. 10 July 2023. Available at https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.

benefit from easier access to the same advanced IT capabilities as larger enterprises, enabling them to compete on a global scale. A prominent example is cloud-based supply chain management systems, which enhance visibility, traceability, and collaboration across the supply chain. This ensures smoother trade operations by enabling real-time monitoring of shipments, inventory levels, and production processes.[26]

Cloud services adoption has been on the rise globally. It is projected to continue increasing at very high growth rates. The global cloud computing market size was valued at EUR 529 billion (USD 567 billion) in 2022.[27] It is expected to grow from approx. EUR 588 billion (USD 630 billion) in 2023 to EUR 2,080 billion (USD 2,230 billion) by 2030.[28] Industry data reveals that Europe's cloud market has also expanded significantly. The European cloud market of 2022 is about five times as big as it was in 2017. Between 2017 and 2022, European cloud services providers have expanded at a lower rate of approx. 167%.[29]

European businesses have experienced a consistent increase in cloud adoption over the past decade. However, a significant portion of the potential offered by cloud computing solutions within Europe remains untapped. Recent Eurostat data reveal that the essential precondition for the integration of cloud computing services, Internet accessibility, is already met by 98% of EU enterprises.[30] The adoption of cloud computing services exhibits a more constrained scope, especially among small and medium-sized businesses, which, compared to large enterprises, still show relatively low adoption rates (see Figure 1Figure 2).[31] Notably, the use of cloud computing solutions becomes more evident among larger enterprises. In 2021, an impressive 72% of such large businesses incorporated cloud technology into their operations. This marked progression is underscored by an increase of 7 percentage points in comparison to the preceding year. Concomitantly, medium-sized enterprises also show a discernible surge in cloud utilisation: 53% of medium-sizes companies use cloud technology, signifying a noteworthy ascent from the 22% recorded in 2014. Equally important is the incremental venture of small enterprises into cloud adoption, reflected by a 21-percentage-point rise, culminating in an aggregated 38% cloud adoption rate.

---

[26] See, e.g., Khan (2023). Cloud-Based Supply Chain Management: Optimizing Logistics and Operations. Available at https://osf.io/v72e4.

[27] EUR/USD conversions based on exchange rate of 5 September 2023. Conversions calculated with Mconvert. Available at https://usd.mconvert.net/eur/.

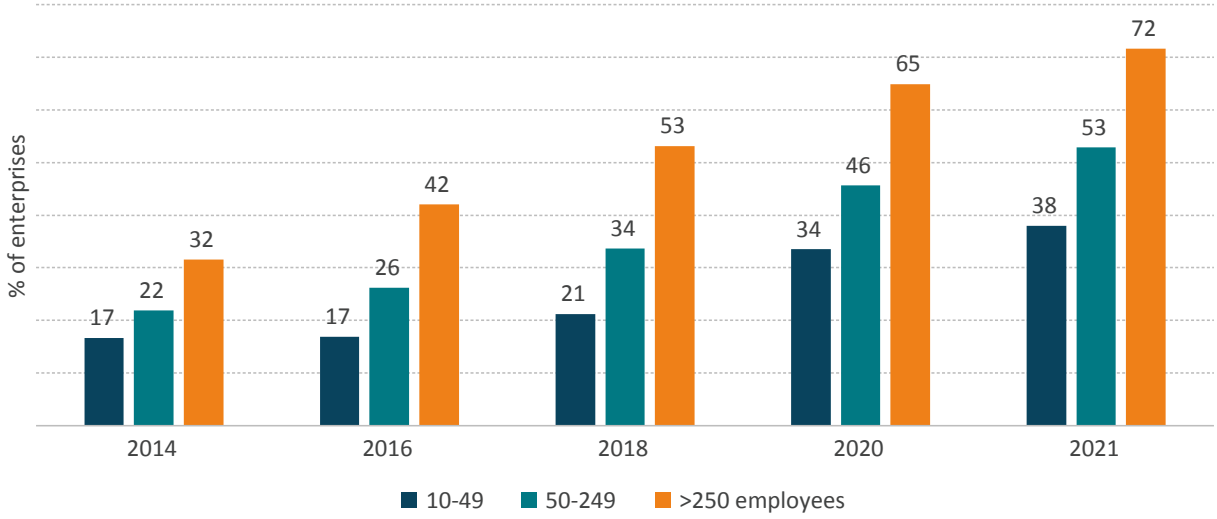
[28] See, e.g., Fortune Business Insights (2022). The global cloud computing market size. Available at https://www.fortunebusinessinsights.com/cloud-computing-market-102697. Also see GMI (2022). Europe Cloud Computing Market Size. Available at https://www.gminsights.com/industry-analysis/europe-cloud-computing-market.

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

[30] Encompassing businesses with a workforce of 10 or more employees and self-employed individuals.

[31] Eurostat. (2023). Cloud computing services by size class of enterprise [dataset]. https://ec.europa.eu/eurostat/databrowser/view/isoc_cicce_use/default/table?lang=en

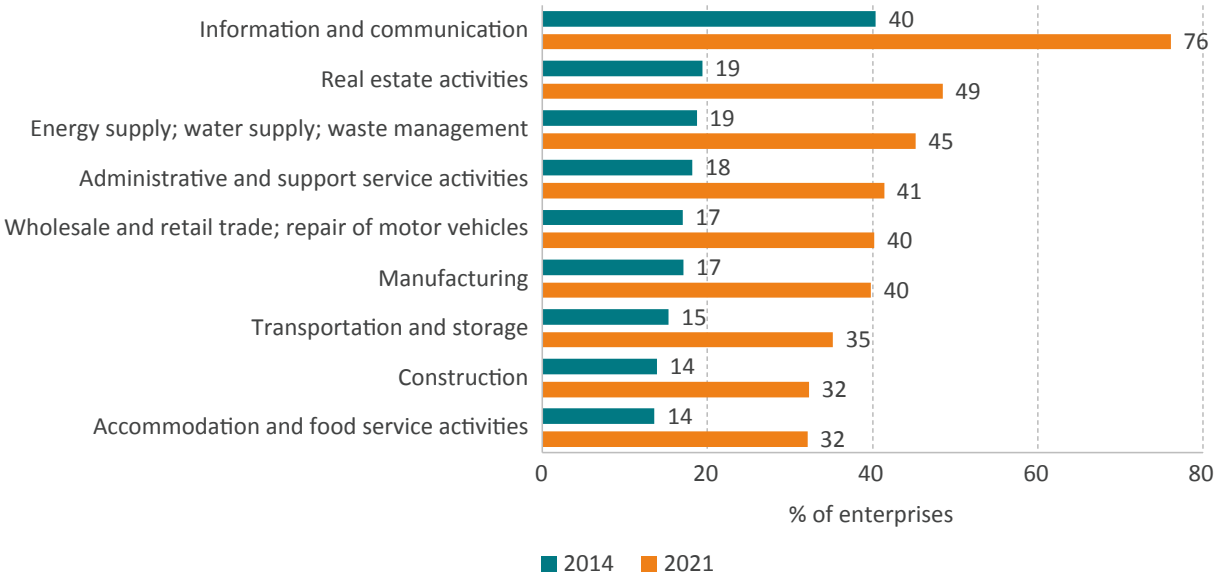
FIGURE 1: USE OF CLOUD COMPUTING SERVICES IN THE EU27, BY SIZE COMPANY SIZE CLASS



Source: Eurostat. Note: All activities, without financial sector.

The information and communication sector, which has always been at the forefront of technological development, is leading in the utilisation of computing advancements, with 76% of firms in this domain utilising cloud computing technologies. This contrasts with other economic sectors, spanning from a modest 32% to a more significant 48%. At the same time, a considerable increase can be observed for all industries between 2014 and 2021 from 18% to 41% of entities using CC (see Figure 2).

FIGURE 2: USE OF CLOUD COMPUTING SERVICES IN THE EU27, BY ECONOMIC ACTIVITY



Source: Eurostat. Note: professional, scientific and technical activities [M] is not included as data is too sparse across EU member states but ranks second just behind Information and communication in the available countries. Note: Professional, scientific and technical activities [M] is not included as data is too sparse across EU member states but ranks second just behind Information and communication in the available countries.

2.2. The Significance of Cloud Services in Facilitating Trade

The importance of data and the economic benefits from exchanging data across-borders have been widely discussed in numerous publications.[32] Studies explicitly quantifying the impact of data and cross-border data on the global economy exist but are less frequent.[33] The OECD, UNCTAD, and other organisations both at a national and supranational level, acknowledge that the statistical basis for quantifying cross-border data flows is limited.[34] Important building blocks – such as the OECD Services Trade Restrictiveness Index (STRI)[35], the measurement of ICT enabled services[36] and ECIPE's Digital Trade Estimates Index[37] – have been put in place. However, due to complex economic relationships, the measurement of cross-border data flows and their economic impacts remains conceptually challenging.

Empirical assessments of the link between cloud services adoption and international trade are still scarce. However, empirical findings of the effects of digitalisation on trade flows and trade costs indicate that Software-as-a-Service (SaaS), Platform-as-a-Services (PaaS), and Infrastructure-as-a-Service (IaaS) solutions, which facilitate to the digitisation of businesses, boost international trade in goods and services. These services also play a pivotal role in enhancing collaboration among businesses and between businesses and consumers.

The economic literature has so far predominantly assessed the enabling role of data, digital infrastructure and digital connectivity. Notably, numerous studies highlight the significant positive impact of digital connectivity on boosting international trade, encompassing both goods and services.[38]

The regulation of digital services markets, by contrast, can counteract these effects. Regulatory frameworks for digital trade as measured, for example, by the Digital Services Trade Restrictiveness Index (DSTRI), typically result in greater international trade costs. Examining the effects of various types of trade barriers, a recent OECD study finds that higher barriers to digital trade, as reflected by the DSTRI, have a negative impact on trade volumes. The biggest effect is held by regulatory measures affecting electronic transactions, followed by infrastructure and

---

[32] See, e.g., Flanagan et al. (2020). A Roadmap for Cross Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy, World Economic Forum; Cattaneo, et al. (2020). The European data market monitoring tool: key facts and figures, first policy conclusions, data landscape, and quantified stories", European Commission; Cory et al. (2020). Schrems II: What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation, Information Technology & Innovation Foundation (ITIF).

[33] See, e.g., Ferracane at al. (2018). Do Data Policy Restrictions Impact the Productivity Performance of Firms?, ECIPE Working Paper No. 2018/1, Brussels, ECIPE; Huang et al. (2019) "Analysis of Cross-border Data Trade Restrictions using Mixture-based Clustering, MIT Sloan School of Management; Bauer et al. (2013). The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce", ECIPE; Bauer and van der Marel (2021). The economic costs of restricting the cross-border flow of data. Joint publication of ECIPE and Kearney Global Business Policy Council.

[34] See, e.g., UNCTAD (2021). Cross-border data flows and development: For whom the data flow. Available at https://unctad.org/system/files/official-document/der2021_annex1_en.pdf.

[35] OECD (2023). Services Trade Restrictiveness Index. Available at https://stats.oecd.org/Index.aspx?DataSetCode=STRI.

[36] See, e.g., OECD (2023). Handbook on Measuring Digital Trade. Available at https://www.oecd.org/sdd/its/Handbook-on-Measuring-Digital-Trade.htm.

[37] See Ferracane et al. (2018). Digital Trade Restrictiveness Index, European Centre for International Political Economy.

[38] For example, digitalization and digital trade policy have played an important role in lowering trade costs, both domestically and internationally. According to a recent study by the OECD, a 1% increase in digital connection is related with a 0.3% decrease in local trade costs and a 0.1% decrease in international trade expenses. See, e.g., López González, J., S. Sorescu and P. Kaynak (2023). Of bytes and trade: Quantifying the impact of digitalisation on trade. OECD Trade Policy Papers, No. 273, OECD Publishing, Paris. Available at https://doi.org/10.1787/11889f2a-en.

connectivity measures.[39] Similarly, 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.[40]

Cloud and data analytics solutions are also increasingly relevant for trade in digitally enabled services due to the ability of cloud infrastructure to provide a scalable, flexible, and accessible platform that supports trade in a broad range of services sectors. Large 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.[41] The use of internal cloud-based services ranges from email, videoconferencing, Internet protocol telephony, document sharing, shared workspaces, and project management. These sectors include information and communication technology (ICT) services (e.g., computer and telecommunications services) and other digitally deliverable services (e.g., financial and business services). Projections indicate trade in these sectors will be increasing faster than traditional, non-digital trade.[42]

The enabling features of cloud services solutions are also reflected by developments outside the field of digitally enabled services. Cloud services play a significant role in promoting trade and benefiting various industries in several ways. Generally, cloud computing enables individuals and organisations to access computing assets via the Internet. Through the adoption of cloud-based services offerings, businesses can reallocate resources from substantial investments in hardware and software. By entrusting the supervision and upkeep of their computing framework to external providers, companies can free-up significant time to concentrate on other essential aspects of their activities, resulting in enhanced efficiency and the development of superior products and processes, improving companies' international competitiveness.[43]

Many technology-intensive businesses are increasingly relying on cutting-edge tech solutions of which many are provided by the world's largest technology companies. Data analytics and cloud services solutions from some of the world's largest cloud service providers are, for

---

[39] See, e.g., López González, J., S. Sorescu and P. Kaynak (2023). Of bytes and trade: Quantifying the impact of digitalisation on trade. OECD Trade Policy Papers, No. 273, OECD Publishing, Paris. Available at https://doi.org/10.1787/11889f2a-en. Also see López González, J. and J. Ferencz (2018). Digital Trade and Market Openness. OECD Trade Policy Papers, No. 217, OECD Publishing, Paris. Available at https://doi.org/10.1787/1bd89c9a-en.

[40] 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.

[41] 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.

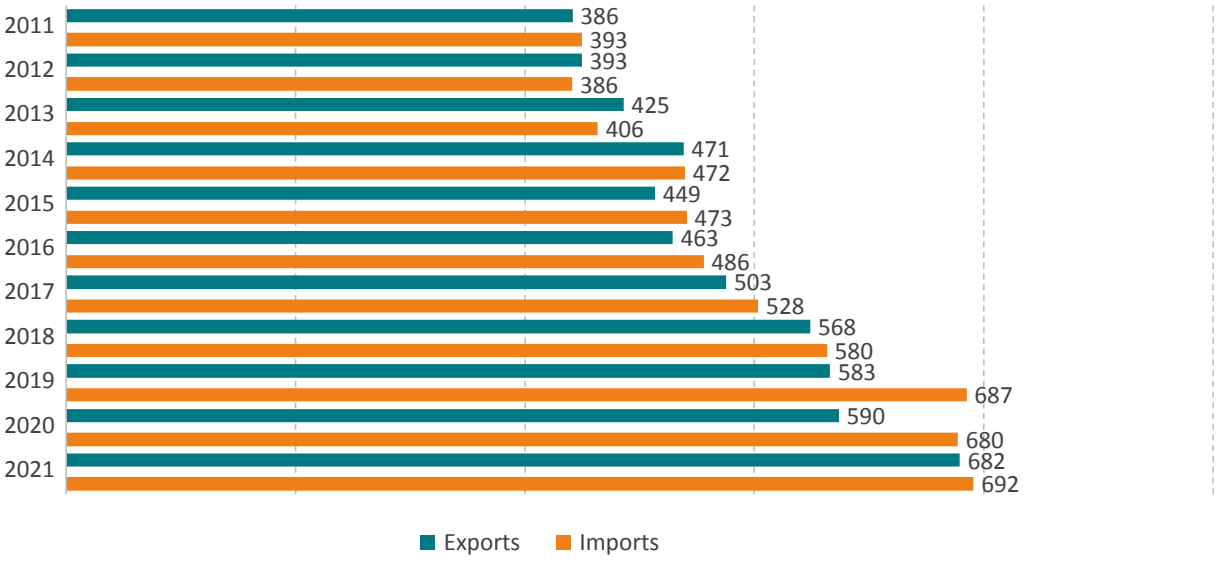
[42] See, e.g., López González, J., S. Sorescu and P. Kaynak (2023). Of bytes and trade: Quantifying the impact of digitalisation on trade. OECD Trade Policy Papers, No. 273, OECD Publishing, Paris. Available at https://doi.org/10.1787/11889f2a-en.

[43] See, e.g., Siemens (2023). Globalization and cloud computing. 7 June 2023. Available at https://blogs.sw.siemens.com/xcelerator/2023/06/07/globalization-and-cloud-computing/.

example, boosting healthcare services and pharmaceutical development.[44] Cloud solutions are also supporting carmakers and automotive suppliers in enhancing connectivity, advancing sustainability, and addressing the complexities of autonomous driving.[45] Advanced platform-based cloud services even enable farmers to enhance crop yields by saving water, agrochemicals, labour, and energy, minimising farmers' ecological footprint.[46]

Contrary to popular notions, trade in ICT and digitally enabled services is not a one-way-street for the EU. Recent trade data demonstrates that total EU exports of digital and digitally enabled services to the rest of the world roughly match the value of total EU imports from the rest of the world (see Figure 3). A similar pattern can be observed for EU digital trade with the US. EU ICT services exports to the US are largely on par with US exports of digital services to the EU. In 2022, EU ICT services exports to the US amounted to USD 14.4 billion (EUR 13.4 billion), while US ICT services exports to the EU amounted to USD 16.4 billion (EUR 15.2 billion) (see Figure 4).

FIGURE 3: TOTAL EXTRA-EU TRADE IN DIGITAL (ICT) AND DIGITALLY ENABLED SERVICES, IN BILLION USD



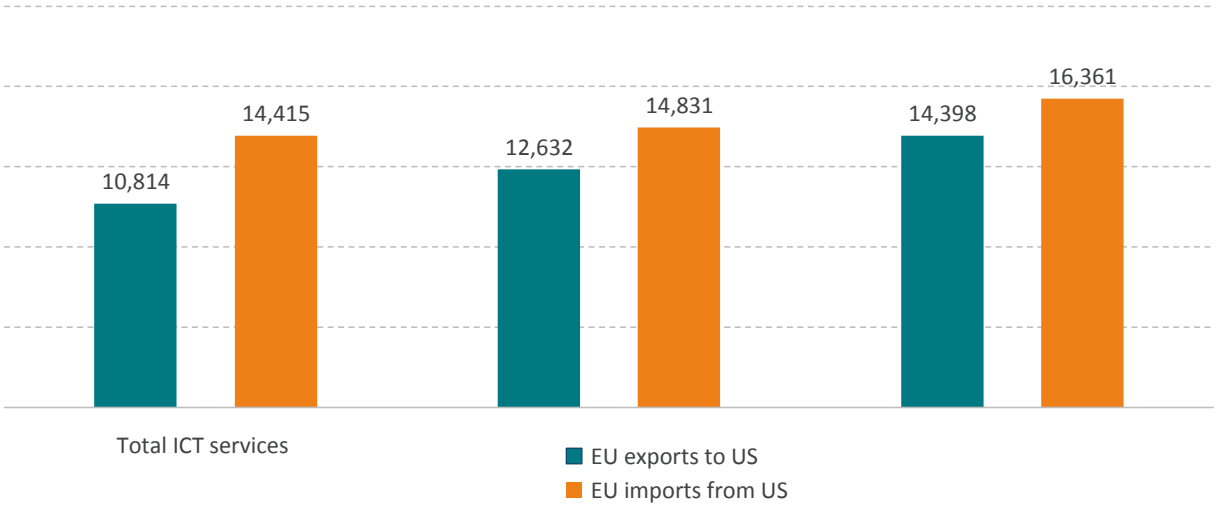
Source: Eurostat. Note: digitally enabled services include insurance and pension services (SF), financial services (SG), charges for the use of intellectual property (SH), other business services (SJ), and personal, cultural, and recreational services (SK). While digital services are the telecommunications, computer and information services industry (SI). Source: OECD-WTO BaTIS and authors' calculation.

[44] See, e.g., Business Today (2023). Amazon Web Services, Google, Microsoft cloud: How cloud services are boosting the pharma sector. 16 April 2023. Available at https://www.businesstoday.in/magazine/deep-dive/story/amazon-web-services-google-microsoft-cloud-how-cloud-services-are-boosting-the-pharma-sector-376113-2023-04-05.

[45] See, e.g., CB Insights (2022). The Big Tech in Auto & Mobility Report: How Google, Amazon, Microsoft, and Apple are changing the automotive industry. 3 November 2022. Available at https://www.cbinsights.com/research/report/big-tech-auto-mobility/.

[46] Amazon (2023). How an agriculture company uses AWS Cloud computing to increase sustainability and feed more people. 17 January 2023. Available at https://www.aboutamazon.com/news/aws/how-cropx-uses-aws-cloud-computing-for-farming.

FIGURE 4: TOTAL EU27-US TRADE IN ICT SERVICES, 2020-2022, IN BILLION USD



Source: US Bureau of Economic Analysis (BEA). Note: numbers provided include news agency services, which, however, show relatively low bilateral trade values.

Market intelligence and trade data indicates, however, that "native" EU cloud services providers do not have the capacity to meet increasing demand. Industry data reveals that for a broad variety of PaaS, Iaas, and SaaS solutions there are no satisfactory European alternatives that could allow European users to reduce costs, improve resilience, and enhance innovation. For example, data by Synergy Research states that IaaS and PaaS solutions indeed are among the fastest growing services in the EU market, currently accounting for over 80% of the European cloud market. The data also shows that while European cloud providers have seen their revenue increase by 167% between 2017 and 2022, the collective share of cloud computing services has also significantly increased over the same period.[47] In 2022, the EU imported cloud services from the US worth USD 2.2 billion (EUR 2 billion), while EU cloud services exports to the US amounted to only USD 0.2 billion (EUR 0.19 billion). A similar pattern can be observed for database and other information services (see Figure 5).[48]

The data also shows that while European cloud providers have seen their revenue increase by 167% between 2017 and 2022, 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.[49] The lack of native EU cloud capacity is also reflected by EU imports of cloud and database services from the US. In 2022, the EU imported cloud services from the US worth USD 2.2 billion (EUR 2 billion), while US cloud services exports to the US amounted to only USD 0.2 billion (EUR 0.19 billion). A similar pattern can be observed for database and other information services (see Figure 5). It

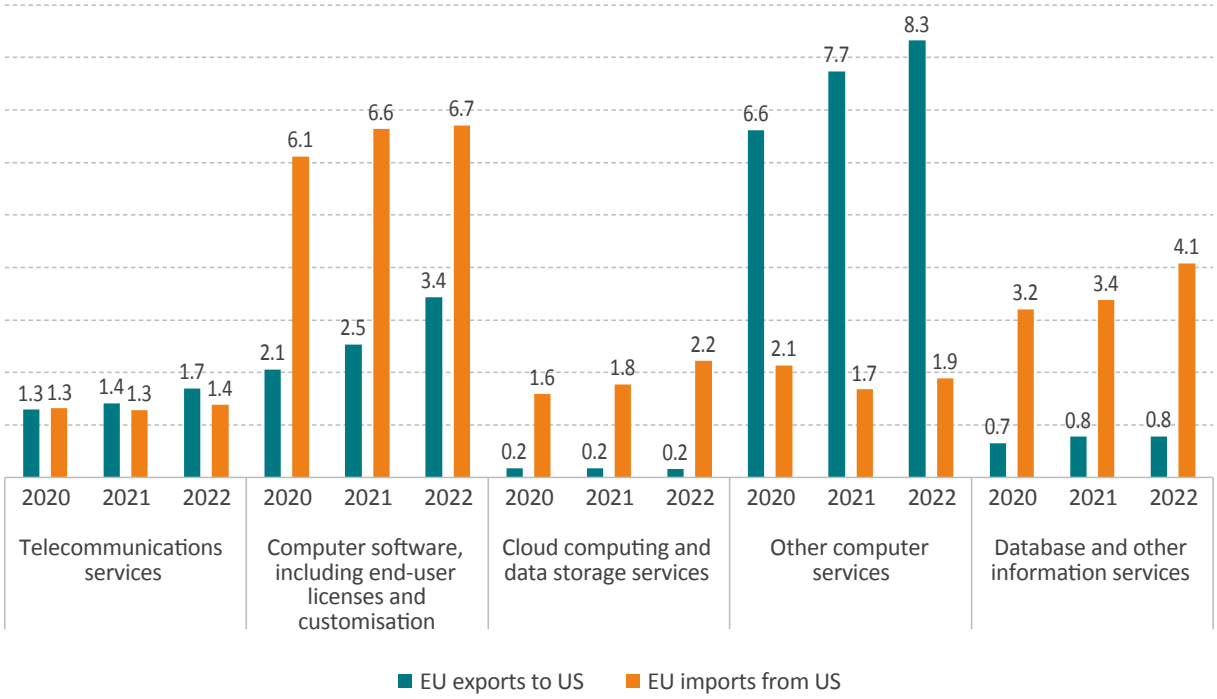
[47] Synergy Research (2022). European Cloud Providers Continue to Grow but Still Lose Market Share. Available at https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share.

[48] It should be noted that the US is so far the only jurisdiction that provides trade statistics for cloud services as a sub-component of ICT services trade.

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

should be noted that the US is so far the only jurisdiction that provides trade statistics for cloud services as a sub-component of ICT services trade.

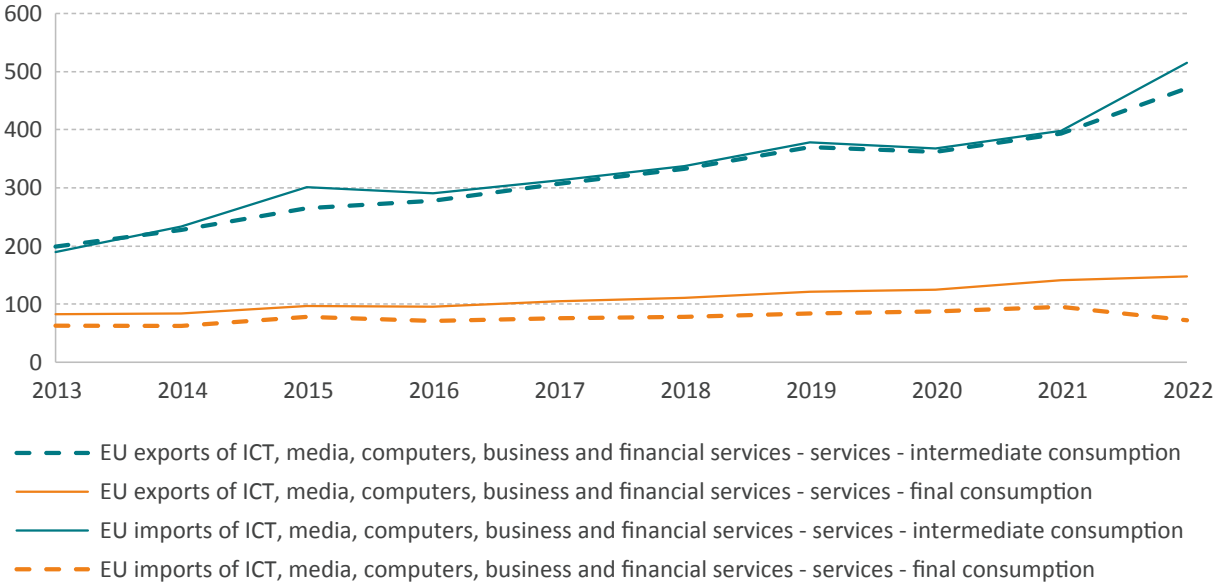
FIGURE 5: EU27-US TRADE IN ICT SERVICES BY SUB-CATEGORY, 2020-2022, IN BILLION USD



Source: US Bureau of Economic Analysis (BEA). Note: due to relatively low bilateral trade values, news agency services, which statistically is a component of ICT services, have been excluded from the data.

That said, trade data demonstrates that total EU exports of ICT and digitally enabled services roughly matches the value of total EU imports of ICT and digitally enabled services (see Figure 6). This applies to both intermediate consumption, i.e., B2B trade, and final consumption. In 2022, 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 approx. EUR 515 billion. EU exports amounted to approx. EUR 471 billion. As discussed above, many digital and digitally enabled services are increasingly provided cloud-based. The numbers show that imports of digitally enabled services from outside the EU more than doubled over the past decade, indicating that domestic EU capacities are either inadequate or insufficient to meet EU businesses' and public sector demand for high quality ICT and digitally enabled services, including cloud services solutions with a strong value proposition.

FIGURE 6: EU TRADE IN DIGITAL AND DIGITALLY ENABLED SERVICES FOR INTERMEDIATE CONSUMPTION AND FINAL CONSUMPTION, IN MILLION EUR



Source: Eurostat, International trade in services and (BPM6). Note: 2022 data is provisional.

2.3. The Importance of Cloud Services for EU Public Services

Cloud computing solutions play an indispensable role in upgrading public services, mirroring its significance in the business sector. Multiple cloud computing solutions are already used extensively by governments and public institutions, and they have a significant transformative potential for the administration of public services and the quality of public services offerings.

European governments are recognising the benefits of cloud computing solutions for the public sector. In tandem with e-government, cloud services have been pivotal in steering the digital transformation of public services across the EU. Modern cloud services help governments upgrade and streamline public services and solve infrastructure issues, cost issues, and improve service delivery and transparency.[50] E-government initiatives have witnessed considerable progress within the EU, leveraging cloud services to, for example, facilitate digital identity verification, the establishment of citizen portals, and online voting. Government entities have transitioned diverse services to the cloud infrastructure, ranging from tax filings[51] to social security applications and public procurement platforms. Healthcare services are experiencing a substantial transformation through the adoption of cloud and advanced data analytics services. Cloud services have also revolutionised the management of Electronic Health Records (EHRs)

[50] 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.

[51] Poland, a pioneer in Central Europe when it comes to the level of digitisation of public services, has successfully integrated cloud services into its public administration, particularly in the finance sector with applications like e-PIT and e-Tax.

within the EU. Cloud-based EHR systems empower healthcare professionals to securely access patient records in real-time, irrespective of geographical boundaries. This technological integration enhances care coordination, mitigates medical errors, and contributes to enhanced patient outcomes.

Several notable government strategies and initiatives have emerged in the recent past, such as France's "Cloud at the centre", which underscores the centrality of cloud computing in their national cloud strategy. The Italian government launched the national cloud hub, while the French government initiated the creation of the French Health Data Space. Similarly, the German government has promoted cloud computing partnerships, with T-Systems, a subsidiary of Germany-headquartered Deutsche Telekom, collaborating with Google to provide sovereign cloud services for public institutions and healthcare organisations.[52] Spain distinguishes itself through innovative integration, seamlessly blending cloud computing and AI in administration programs like Kid Digital and My Citizen Folder, which is further catalysed by access to "NextGenerationEU" funds aimed at propelling public administration digitalisation.[53] At the EU-level, a collaborative private-public initiative, GAIA-X, is emblematic of the region's pursuit of cloud and data infrastructure, embodying both public and private stakeholders, all striving to foster a diverse EU ecosystem for cloud and data services while emphasizing data sovereignty.

Data security has long been of relevance in the EU. At the same time, both domestic and foreign providers of digital services, including cloud computing services, have continued to enhance technology to further increase data protection. As concerns foreign providers, the issue of Data Residency, i.e., the localisation of data within a particular jurisdiction, was addressed by prominent cloud services providers, which have established numerous data centres within the EU, offering a specific type of cloud service that operate within the EU jurisdiction. This is part of broader investment efforts from foreign cloud providers in other areas, such as digital, cloud, quantum, and AI, reflecting broad commitments and contributions of non-EU cloud providers to the EU economy.

Despite those significant investments across the continent, the perception of data safety remains subject to political controversies in some EU Member States. In France, for example, considerable political pressure on the "French Health Data Hub", a public institution, meant that the most suitable provider was US-headquartered Microsoft and was not allowed to exclusively offer the advanced cloud services anymore. Following the cancellation of the original award to a US-based company in 2019, no alternative solution has yet been able to go into operation. In fact, the project is not anticipated to be fully realised until after 2025.[54]

---

[52] T-Systems and Google Cloud partner to deliver sovereign cloud for Germany. Available at https://www.t-systems.com/de/en/newsroom/news/t-systems-and-google-cloud-partner-to-deliver-sovereign-cloud-for-germany-450474.

[53] La Moncloa. (2022, November 24). The Government of Spain launches the National Cloud Services Strategy for Public Administrations. Available at https://www.lamoncloa.gob.es/lang/en/gobierno/news/Paginas/2022/20221124_cloud-services-strategy.aspx

[54] Presently, the French Health Data Hub (HDH) is actively exploring a hybrid approach that leverages both French and American companies. This model envisions French companies handling the data hosting aspect, while American counterparts provide specialised software solutions (Orange and Capgemini, Thales and Amazon, or OVH and Google). This collaboration is seen as a promising way to strike a balance between data security and the efficient utilisation of cutting-edge technology. Nevertheless, the process of migrating the HDH to a new company and ensuring a seamless transition is a complex undertaking. As a result, the project is not anticipated to be fully realised until after 2025.

3. THE ECONOMIC IMPACTS OF EUCS EXCLUSIONARY REQUIREMENTS

With the draft EUCS, ENISA and the European Commission propose to incorporate exclusionary requirements concerning data localisation, country of global headquarter and effective corporate control. This would imply that European users subject to a recommendation or requirement to use high-assurance level cloud services would no longer have access to the cloud services of foreign providers, entailing that their data must be effectively stored and processed within the EU borders by eligible "native" EU companies. This section addresses several economic implications of these immunity requirements.

3.1. Impacts of Measures That Effectively Require Data Localisation in the EU

The overall economic impacts of cloud data localisation measures tend to be complex and depend on various factors, including the state of development of the economy, international economic interdependencies, and the adaptability of cloud users and cloud providers. Accordingly, policymakers must carefully consider a broad range of general implications when designing restrictions to the free cross-border flow of data. The major impacts identified in this research include:

- Operational inefficiencies and increased cost of production: Data localisation measures lead to increased compliance costs for cloud service providers as well as their customers. Companies need to establish and maintain local data storage infrastructure or source services from local suppliers, which lack economies of scale. Additional expenses are particularly burdensome for small enterprises and start-ups. In addition, due to the legal fragmentation of the Internet multinational companies would have to comply with different regulations in each country. This complicates operations for global companies using cloud services and leads to inefficiencies in delivering goods and services across borders. Companies would lose their comparative advantage in and beyond data-intensive industries if they cannot efficiently transfer and utilise data from various locations to conduct business efficiently and improve their products and services offerings.

- Reduced investments in the domestic economy: Restrictive data localisation requirements may deter domestic and foreign companies from investing in a country. Investment in business expansion and innovation will likely decline when companies find it overly challenging to navigate complex regulations or anticipate trade bans, operational limitations, and retaliatory measures.

- Reduced international trade: Restrictive data localisation measures hinder international trade. Businesses that rely on cross-border data transfers to operate,

including cloud customers, may face severe value chain disruptions or reduced efficiency. Due to the nature of value-added, the direct impacts tend to be strongest for cross-border e-commerce, ICT and software developers, and digitally enabled industries, such as financial services and healthcare services. However, data localisation policies also impact companies that use data and data driven services less intensively, e.g., traditional businesses transitioning to cloud services solutions. Foreign Non-EU governments may reciprocate with similar policies. This can create a dangerous domino effect, leading to more significant restrictions on cross-border data flows, global trade, and domestic economic activity.

- Reduced innovation and competition: Data localisation policies, by default, restrict access to a broad range of data that is processed in other jurisdictions, curbing research opportunities and innovation in the domestic economy. Data-driven industries in particular will experience decreases in competitiveness due to reduced competition and reduced possibilities for innovation. On aggregate, data localisation measures will severely slow-down economic development in a wide array of industries.

Adverse environmental impacts: Data localisation measures by design lead to increased energy consumption, excess land use, excess use of water, and more electronic waste. The implications stem from the need to establish new local data centres to store and process data within a country's borders. Data centres consume significant amounts of electricity for cooling and running servers. If the local power generation relies heavily on fossil fuels, data localisation could lead to increased greenhouse gas emissions and contribute to climate change. Also, data localisation measures can necessitate an enormous amount of data replication to ensure redundancy and data availability. Replicating data across multiple data centres in different legal jurisdictions can increase energy consumption and carbon emissions due to the need for data synchronisation. Moreover, building data centres and related infrastructure may require substantial land use. Large data centres can occupy vast areas, potentially leading to habitat loss, or disruption of ecosystems if not planned and executed responsibly. Data centres also typically require significant amounts of water for cooling purposes. And finally, as data centres and related technology rapidly evolve, older infrastructure might become obsolete or less efficient. This will lead to an increase in electronic waste as companies will continue to upgrade their facilities or equipment to comply with data localisation regulations.

- Cybersecurity risks and data mismanagement: Data localisation measures can lead to a concentration of data within a single jurisdiction, potentially increasing the risk of cyberattacks or targeted government surveillance. Data localisation often creates obstacles to an integrated data management approach towards cybersecurity risks. Because of non-EU exclusionary requirements (country of headquarter and foreign ownership restrictions) proposed in the EUCS, cloud service providers eligible for the highest assurance level are effectively locked-in to the EU for their cybersecurity measures and threat intelligence. These cloud providers are not likely to benefit or learn from global security learnings, threats, and insights. 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. Further, the overall EUCS approach including its exclusionary criteria appear to create the false perception that EUCS-High certified services are categorically and comprehensively "secure". In practice, certification is only one of many elements to demonstrate and implement appropriate security. The security benefits delivered by non-EU cloud service providers extend beyond a single certification scheme.

3.2. Substantial Shortages in the Supply of ICT Solutions

EUCS exclusionary requirements for cloud-based ICT services would severely limit the options available to users in the EU as foreign providers may be hesitant to invest in storage and processing capacities in the EU and/or enter into joint ventures and minority stakes with native EU businesses. Requirements for cloud services providers to store and process data within EU borders together with country of headquarter requirements would severely restrict or bring to a halt the international flow of data that is facilitated through cloud solutions. Due to the high penetration of cloud solutions offered by foreign companies, immunity requirements would significantly restrict EU users in their ability to access cloud and data-intensive services with a strong value proposition, including many digitally enabled services, data analytics solutions, machine learning, and AI-based software applications.

As outlined above, non-EU ICT providers are well established in the EU and create and integral part of the customer choice. If this supply were to be cut off or strictly limited to EU providers only (under the current very restrictive definition of European ownership and control in the requirements and due to the broad and vague scope of highest evaluation level) EU customers (public and private) would face severe service disruption and reduced choices. This would also undermine the massive investments underway. While some EU providers may continue to expand, their impact on the overall European market share is likely to be limited. This suggests that the substantial presence of non-EU ICT providers in the EU can be attributed not only to significant financial investments but also to their longstanding presence in the industry, which instils greater trust among businesses compared to smaller and much less developed European cloud providers.[55]

These impacts on the cloud services market in Europe should also be seen in the light of broader impacts from foreign investments in the Member States and the productivity and trade competitiveness of European companies. Imports of high value-added cloud services from highly competitive non-EU companies are not a zero-sum game for EU countries, where non-EU success stories equates to the EU's failure. Instead, Europe's level of competitiveness critically relies on opportunities for investment attractiveness, cross-border exchange, and competition. Access to high-quality cloud services make European firms more competitive, whilst international

[55] 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 US 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/.

trade exposes domestic cloud services firms to competition, requiring constant innovation and productivity improvements to succeed in the market. FDI thereby is a vital catalyst for enhancing Europe's productivity across industries. Recent analyses of company-level data reveal a strong positive impact of FDI on productivity, which includes a boost in the productivity of domestic firms engaged in business with foreign entities. Furthermore, a mutually beneficial relationship exists between trade (both exports and imports) and FDI. First, FDI leads to EU firms expanding their trade activities and involvement in global supply chains. And second, foreign subsidiaries play a significant role in driving EU export activities. In fact, a large proportion of EU Member States exports is generated by non-EU multinationals. Accordingly, EU inward FDI, including substantial investments by non-EU cloud services companies, emerges as a potent element in Europe's competitiveness, serving as an effective mechanism that links smaller businesses to global supply chains.[56]

3.3. Less Resourceful and Potentially More Vulnerable EU Suppliers of Cloud and Data Services Solutions

Assessing the impact also requires an intertemporal perspective on the path of technology development and the commercialisation of innovative cloud services solutions and technologies that critically rely on. Restrictions on data movement would effectively limit European users' ability to benefit from new services and datasets from multiple sources or locations. There is a widespread misconception that cloud services are limited to file storage. However, cloud-based data storage functions are only a small fraction from the scale of possibilities cloud solutions offer especially to business users already today. In fact, cloud services have been at the centre for advancing Europe's digital transition. And while many industries could see potential benefits for relying upon cloud infrastructure, these services would be crucial for the development of AI technology, especially in healthcare, manufacturing and financial services. Access to global cloud solutions would enable EU companies to have a competitive advantage by allowing the adoption of the latest technologies. Similarly, under a global infrastructure, cloud solutions enable companies to design their business models in line with accelerating digitalisation trends. Moreover, cloud providers offer advanced security measures like encryption, data protection, and recovery capabilities, which come in tandem with potential cybersecurity risks that these companies could face.

European businesses and final customers would miss out on the benefits of many cutting-edge technologies if foreign service providers are being excluded from EU Member States due to cloud data localisation requirements and ownership restrictions. There are already numerous collaborations between European companies from a wide variety of industries and cloud services suppliers from outside the EU (see Table 1). With immunity requirements in place, it would be challenging for European enterprises to leverage cloud services and transfer data across countries. Strict immunity requirements would disrupt global collaborations and workflows, create inefficiencies, and will ultimately erode European companies' competitiveness in international markets. Being cut-off from non-EU solutions would limit European users' ability

[56] See, e.g., ECIPE (2023). Trade and Competitiveness: Putting the Firm at the Centre of the Analysis. Available at https://ecipe.org/publications/trade-and-competitiveness-putting-firm-at-centre-of-analysis/.

chose the best partners or switch providers if they are dissatisfied with the service or if better alternatives become available. In other words, users that classified critical under the CS-EL4 assurance level might become locked into less favourable offerings by native EU cloud service providers.

TABLE 1: PARTNERSHIPS AND JOINT VENTURES IN CLOUD SERVICES

Partnership	Description
AWS and T-Systems[57]	AWS' trusted partners play a prominent role in bringing solutions to customers. For example, in Germany, T-Systems (part of Deutsche Telekom) offers Data Protection as a Managed Service on AWS. It provides guidance to ensure data residency controls are properly configured, offering services for the configuration and management of encryption keys and expertise to help guide their customers in addressing their digital sovereignty requirements in the AWS Cloud.
Cloud Software Group & Midis Group[58]	In a significant milestone, Cloud Software Group has announced a strategic partnership with Midis Group, through its subsidiary MiCloudSW Ltd. This strategic alliance represents a turning point in Cloud Software Group's efforts to improve the services it offers to its channel partners and customers across a significant part of Eastern Europe, the Middle East and Africa. As a result of the agreement, Cloud Software Group now has strategic access to invaluable local resources, which is an important tool in support of customers' technology transformation efforts. It will also provide the scale needed to substantially increase its presence and impact in these regions.
Deutche Telekom and GoogleCloud[59]	Deutsche Telekom and Google Cloud have unveiled a robust expansion of their partnership to chart a joint course to shape the future of the telecommunications industry. This strategic collaboration aims to harness the power of cloud technology and position it in close proximity to mobile and connected devices, strategically placed at the edge of Deutsche Telekom's extensive network infrastructure.
HCL Software and Google Cloud[60]	An important player in the field of business software solutions, HCLSoftware, has partnered strategically with Google Cloud. With this partnership, HCLSoftware will work to effortlessly combine Google Cloud's cutting-edge generative AI capabilities into its software offerings, which is an intriguing potential. Customers will have unrestricted access to the cutting edge of Google Cloud's AI capabilities, including its powerful big language models, thanks to this integration. Together, HCLSoftware and Google Cloud want to usher in a new age of intelligent business applications via the combination of their respective strengths in software development and AI research. These applications are expected to revolutionize industries, improve operational procedures, and increase the overall effectiveness of organizational initiatives. They are seen as catalysts for radical change.

[57] Deutsche Telekom (2022). T-Systems partners with AWS to launch Data Protection as a Managed Service in the cloud. Available at https://www.telekom.com/en/company/details/t-systems-data-protection-for-the-aws-cloud-649324.

[58] Businesswire (2023). Cloud Software Group Establishes Strategic Partner Agreement with Midis Group in Eastern Europe, Middle East and Africa. Available at https://www.businesswire.com/news/home/20230608005690/en/Cloud-Software-Group-Establishes-Strategic-Partner-Agreement-with-Midis-Group-in-Eastern-Europe-Middle-East-and-Africa

[59] CISION (2022). Deutsche Telekom and Google Cloud Sign Partnership Agreement Focused on Network Transformation. Available at https://www.prnewswire.com/news-releases/deutsche-telekom-and-google-cloud-sign-partnership-agreement-focused-on-network-transformation-301584020.html

[60] Businesswire (2023). HCLSoftware Partners with Google Cloud to Create a New Generation of Generative AI-Powered Business Applications. Available at https://www.businesswire.com/news/home/20230822781481/en/HCLSoftware-Partners-with-Google-Cloud-to-Create-a-New-Generation-of-Generative-AI-Powered-Business-Applications

Partnership	Description
Lenovo and VMware Inc.[61]	Lenovo and VMware announced their partnership to deliver the first turnkey solutions from their joint Edge and Cloud Innovation Labs. These solutions are tailored to the needs of mid-market organisations, providing them with modern hybrid multi-cloud capabilities. The aim is to help customers leverage their data assets more seamlessly. These innovative solutions are an integral facet of an expanded partnership with VMware focused on providing organisations across the spectrum with an accelerated path to digital transformation. Likewise, this joint initiative introduces new integrated edge-to-cloud offerings designed to streamline the implementation of cutting-edge AI and data intelligence capabilities, fostering a more accessible path for organisations to embark on their transformative projects.
Mapbox and Toyota Motor Europe[62]	Toyota Motor Europe and Mapbox have partnered to deliver Cloud Navigation powered by Mapbox Dash, the industry-leading maps and location platform enabling a new generation of location-aware applications.
OVH and Google[63]	To expand its cloud computing capabilities, Google is working with the French technology company OVH. In a statement, OVH claimed that its collaboration with Google Cloud would enable it to incorporate some of the American company's technologies into services that its staff would manage and administer in Europe.
OVHvcloud and Unisys[64]	Unisys and OVHcloud, leaders in cloud infrastructure solutions, have partnered to provide a European, data-sovereign cloud infrastructure. By integrating OVHcloud's public cloud solutions into Unisys' suite of services, it will be possible to offer a European-based, data-sovereign cloud infrastructure with a clear focus on serving the needs of the public sector. The partnership primarily focuses on programs and service options aimed at European Union-wide public sector organizations.
Proximus and Google Cloud[65]	Proximus and Google Cloud have jointly announced a significant five-year agreement to provide sovereign cloud services in the regions of Belgium and Luxembourg. The essence of this collaboration lies in the secure deployment of sensitive and mission-critical workloads, coupled with the implementation of advanced digital sovereignty controls. These strategic efforts are aimed in particular at governments, regulated enterprises and international organisations. The partnership aims to strengthen the ability to manage critical operations in a secure and domestically managed cloud environment.
The Serviceplan Group and Box[66]	The Serviceplan Group, Europe's largest Independent and Partner-Managed Agency group established a partnership with Box for Cloud content management. This partnership will provide secure forms of collaboration, enterprise security and compliance. Box will play a central role in helping Serviceplan Group's partners and teams to collaborate regardless of where they are located.

[61] Inside BigData (2023). Lenovo and VMware Expand Partnership to Bring New NVIDIA-Powered Turnkey Generative AI and Multi-Cloud Solutions to Every Business. Available at https://insidebigdata.com/2023/08/22/lenovo-and-vmware-expand-partnership-to-bring-new-nvidia-powered-turnkey-generative-ai-and-multi-cloud-solutions-to-every-business/

[62] Murphy, D. (2023). Toyota to offer Mapbox cloud navigation in three European models. Available at https://mobilemarketingmagazine.com/toyota-to-offer-mapbox-cloud-navigation-in-three-european-models

[63] OVH Cloud (2020). OVHcloud and Google Cloud announce a strategic partnership to co-build a trusted cloud solution in Europe. Available at https://corporate.ovhcloud.com/en/newsroom/news/ovhcloud-and-google-cloud-announce-strategic-partnership-co-build-trusted-cloud-solution-europe/

[64] OVH Cloud (2023). OVHcloud and Unisys form partnership for data-sovereign cloud offerings. Available at https://corporate.ovhcloud.com/en/newsroom/partnerannouncementunisys/-

[65] Proximus (2023). Proximus and Google Cloud to Deliver Sovereign Cloud Services in Belgium and Luxembourg. Available at https://www.proximus.com/news/2023/20230315-disconnected-sovereign-cloud-platform.html

[66] Businesswire (2023). The Serviceplan Group, Europe's Largest Independent and Partner-Managed Agency Group, Chooses Box for Cloud Content Management. Available at https://www.businesswire.com/news/home/20230622174329/en/The-Serviceplan-Group-Europe%E2%80%99s-Largest-Independent-and-Partner-Managed-Agency-Group-Chooses-Box-for-Cloud-Content-Management

Partnership	Description
Thales and Google cloud[67]	Thales and Google Cloud have jointly announced a major strategic agreement to jointly build a sovereign hyperscale cloud solution tailored for France. This project will be managed by a joint company in which Thales will have a majority stake. The essence of this initiative is based on compliance with the criteria defined by the French "Trusted Cloud" framework. The combined efforts of Thales and Google Cloud aim to facilitate cloud computing services that are congruent with France's sovereign cloud strategy.

Restricting the use of foreign cloud-based data processing solutions in the EU would prevent or at least slow-down the deployment of advanced cloud applications and AI models, which typically rely on large globally sourced datasets for innovation and improvements. Take deep learning as an example. Deep learning is a critical component of most artificial intelligence endeavours, centred on the concept of deep neural networks that process inputs through numerous interconnected layers. These networks excel at intricate cognitive tasks, outperforming traditional machine learning methods. However, they often demand extensive data for training and substantial computational power. Cloud computing services play a pivotal role in enhancing the accessibility of deep learning by facilitating the management of substantial datasets and the training of algorithms on distributed hardware. Cloud platforms offer immediate access to large-scale computational resources, enabling the distribution of model training across multiple machines. Cloud services provide access to specialized hardware configurations like processing units and high-performance computing systems with massive parallel processing capabilities.

Moreover, users can access advanced or substantial hardware resources without the need for upfront investments. In essence, cloud computing services democratise deep learning by offering flexible and affordable resources for training and deploying models effectively. Businesses from outside the EU are currently leading in deep learning cloud applications.[68]

European businesses and consumers would miss-out on cutting-edge technologies and, with it, fail to tap into huge economic opportunities. Notably, the global market size of AI technology, especially in healthcare, manufacturing and financial services, was valued at EUR 398 billion in 2022. It is projected to grow to EUR 1,880 billion by 2030. For example, the market for AI technologies for pharmaceutical and medical industries is expected to grow from EUR 56 billion to EUR 102 billion annually. The economic opportunities derived from AI's ability to process massive amounts of data and model options to accelerate the processes of discovering new drugs.[69] Likewise, in the case of manufacturing, self-learning systems could transform the manufacturing process in a more predictable way, reducing costs, delays, or defects. According to forecasts, the global AI in manufacturing is expected to reach around EUR 63 billion by 2032.

[67] Thales (2021). Thales and Google Cloud Announce Strategic Partnership To Jointly Develop A Trusted Cloud Offering In France. Available at https://www.thalesgroup.com/en/group/investors/press_release/thales-and-google-cloud-announce-strategic-partnership-jointly

[68] See, e.g., Run ai (2023). Cloud Deep Learning. Top Three Platforms Compared. Available at https://www.run.ai/guides/cloud-deep-learning. Examples include AWS SageMaker, CloudAI, and Azure Machine Learning.

[69] Berglind, A. and Isherwood, T. (2022) The potential value of AI and how governments could look to capture it. McKinsey and Company. Available at: https://www.mckinsey.com/industries/public-sector/our-insights/the-potential-value-of-ai-and-how-governments-could-look-to-capture-it

3.4. Widening of the EU's ICT Technology Gap

Cloud services are transversal technologies, also known as cross-cutting or horizontal technologies. They have a broad impact across various industries. Cloud services provide a wide range of computing, storage, and networking capacities that can be applied to various applications and industries. Due to their transversal nature, cloud services play a foundational role in modern technology ecosystems, enabling innovation, efficiency, and agility across various sectors.[70] If technology-intensive industries in the EU were cut off from access to foreign cloud services, this would have consequences for the innovative ability and future competitiveness of European companies. It would thus contribute to a widening of the EU's technology gap beyond ICT and digitally enabled services.

The EU is already experiencing a technology gap, which has been growing over the past decade.[71] Corporate data reveals that the EU's underperformance in technology development, investment, and international competitiveness is largely caused by European businesses struggling to successfully grow and invest in international markets. For example, a recent analysis of corporate data conducted by McKinsey (2022) shows that between 2014 and 2019, large European companies with more than USD 1 billion (EUR 930 million) in annual revenue were on average 20% less profitable than their US counterparts. Also, European businesses' revenues have grown 40% less than those of US companies, and European businesses spent about 40% less on corporate R&D (see Figure 7)[72] It is explicitly highlighted that such remarkable underperformance cannot be merely attributed to a few "US superstar companies" in computer and digital services industries. Indeed, the largest part of EU corporate underperformance in EU Member States can be attributed to underperformance in a broader spectrum of technology-creating (general purpose technologies) industries, including ICT and pharmaceuticals, which "together account for more than 70% of the EU's R&D intensity gap".[73]

EU trade and technology openness are the prime roots of its high living standards, resilience, and global geopolitical influence. EU Member States can look back on decades of robust economic growth, but the rates of growth have been poor for a long time. The consequences are now increasingly visible: China is not only catching up but surpassing in many industries. In the Transatlantic relationship, the EU risks becoming the junior partner, driven by its profound and rising technology, productivity, and income gap vis-à-vis the United States. In fact, if EU Member States were states in the US, many of them would belong to the group of poorest countries. And if the growth trend continues, the prosperity gap between the

---

[70] See, e.g., European Commission (2021). European industrial technology roadmap for the next generation cloud-edge offering. May 2021. Available at https://ec.europa.eu/newsroom/repository/document/2021-18/European_CloudEdge_Technology_Investment_Roadmap_for_publication_pMdz85DSw6nqPppq8hE9S9RbB8_76223.pdf.

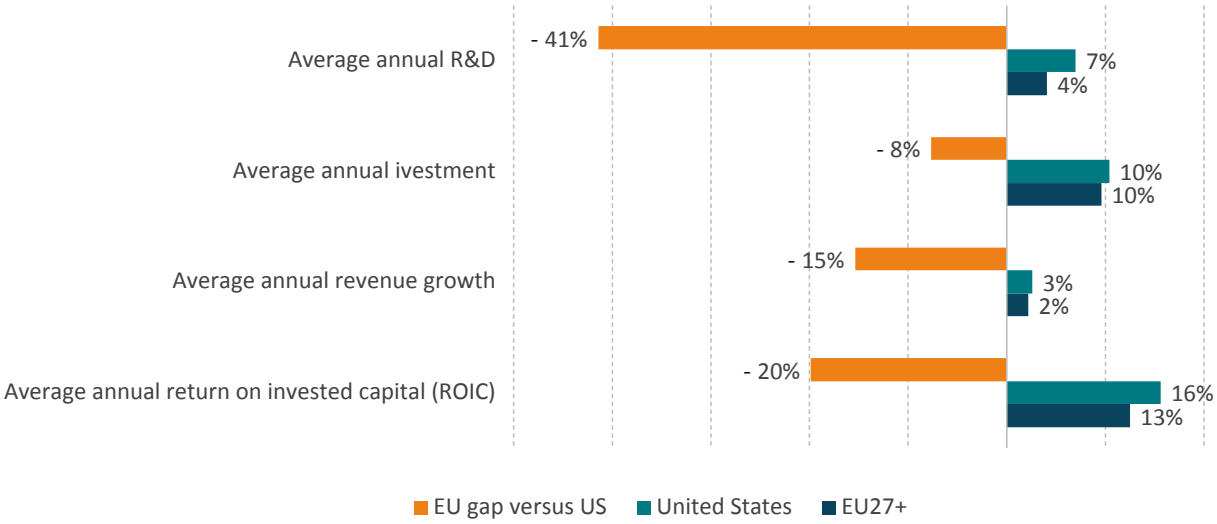
[71] See, e.g., EU industrial R&D investment scoreboard reports. Available at https://iri.jrc.ec.europa.eu/scoreboard.

[72] McKinsey (2022). Securing Europe's competitiveness – Addressing its technology gap. September 2022. Available at https://www.mckinsey.com/~/media/mckinsey/business%20functions/strategy%20and%20corporate%20finance/our%20insights/securing%20europes%20competitiveness%20addressing%20its%20technology%20gap/securing-europes-competitiveness-addressing-its-technology-gap-september-2022.pdf. Also see McKinsey (2023). The economic potential of generative AI The next productivity frontier. Available at https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-AI-the-next-productivity-frontier#/.

[73] The authors stress that high ROIC can reflect entrenched market positions and pricing power. However, "the growth and R&D gaps are clearly not sustainable for Europe."

average European and American in 2035 will be as big as between the average European and Indian today.[74]

FIGURE 7: EUROPE'S TECHNOLOGY AND CORPORATE PERFORMANCE GAP VIS-À-VIS THE UNITED STATES



Source: McKinsey (2022). Weighted average, 2014–19, % (companies with > USD 1 billion in revenue). EU27+ = EU27 plus Norway, Switzerland, and the UK. Average annual return on invested capital (ROIC) = NOPLAT/ invested capital (NOPLAT = net operating profit less adjusted taxes). Average annual revenue growth = change in revenues. Average annual investment = capital expenditures / invested capital. Average annual R&D = R&D spending/revenue, top 2,500 R&D spenders.[75]

4. ESTIMATION OF THE ECONOMIC IMPACTS OF EUCS IMMUNITY REQUIREMENTS

This Section is devoted to the modelling of potential GDP and industrial production effects of EUCS CS-EL4 immunity requirements. We begin with an outline of the modelling approach and a description of the applied scenarios and their underlying assumptions. We then illustrate the results of the model estimations.

4.1. Modelling Approach

EUCS immunity requirements would effectively prevent high-assurance users in EU Member States from using cloud services from non-EU providers. Depending on the sectoral coverage of CS-EL4 requirements, in particular the discriminatory cloud data localisation and EU ownership requirements, European cloud adopters would, to varying extents, lose access to global cloud

[74] See ECIPE (2023). If the EU was a State in the United States: Comparing Economic Growth between EU and US States. Available at https://ecipe.org/publications/comparing-economic-growth-between-eu-and-us-states/?_gl=1*d1k90x*_up*MQ..*_ga*MTAyOTE5MjMxMi4xNjk0NzcwNzkx*_ga_T9CCK5HNCL*MTY5NDc3MDc5MS4xLjAuMTY5NDc3MDc5MS4wLjAuMA.

[75] McKinsey (2022). Securing Europe's competitiveness – Addressing its technology gap. September 2022. Available at https://www.mckinsey.com/~/media/mckinsey/business%20functions/strategy%20and%20corporate%20finance/our%20insights/securing%20europes%20competitiveness%20addressing%20its%20technology%20gap/securing-europes-competitiveness-addressing-its-technology-gap-september-2022.pdf.

solutions and be unable to benefit from the continuing growth of non-EU capacities and future productivity gains of cloud and cloud-enabled services.

We will assess the effects of immunity requirements on cross-border trade of cloud services and estimate associated economic trickle-down (spill-over) effects across domestic industries, including commodity, agriculture, manufacturing, and services sectors.

Similar to related studies, we treat restrictions to the free cross-border flow of data as non-tariff trade barriers (NTBs) that increase the cost of trading goods and services including data and data-based products and services. For the purpose of this study, we simulate a rise of ad valorem tariff equivalents (AVEs) of these NTBs to a level that is prohibitive to cross-border trade of cloud services as part of trade in ICT services.

We also account for cloud services replacement rates in the EU. Industry intelligence suggests that the collective share of cloud computing services provided by European CSPs in their home territory amounts to only 13% (see analysis above). Assuming, for instance, that shares in the segment of high assurance services would correspond with overall shares of cloud services providers in the EU, "EU-only" or "native EU" cloud providers" would have to meet a rapidly surging demand of about 80% of the current market value, excluding future growth of the sector. Many native EU cloud providers would likely continue to grow, but on aggregate, native EU cloud providers would be unable to meet massive and abrupt rises in the demand for advanced cloud and cloud-enabled services, particularly for advanced cloud, data analytics, AI, quantum, and edge-computing services. This would result in an unmet demand and, potentially, in significant increases in the prices of a few competitive EU services. Accounting for the demand effects, we will apply different cloud services replacement rates. We generally differentiate between short- and medium-term replacement in each of our implementation scenarios, applying assumptions for a 2-year and 5-year time horizon respectively.

Our modelling approach accounts for future changes in EU access to global capacities and higher productivity growth including global productivity gains from innovation. ICT and cloud services undergo a constant process of upgrading and innovation, resulting, for example, in faster, more secure, and more customised services for demanding clients and complex use cases. Current market shares and the substantial technological lead of non-EU cloud services providers suggest that EU providers will not be able to offer internationally competitive services in the near and medium term.[76] This means that domestic services will either become too expensive or not economically viable compared to cloud services provided by non-European entities, resulting, for instance, in ineffective spending of taxpayer money and productivity losses for European businesses. Accounting for these effects, we estimate the combined effects from cloud services capacity losses and forgone productivity growth in the EU for each scenario.

[76] The "French Health Data Space", a public institution, is a case in point. US-headquartered Microsoft, the company offering the functionalities and cybersecurity requirements demanded by the tendering authority, was not allowed to exclusively offer the advanced cloud services anymore. Following the cancellation of the original award to Microsoft in 2019, no alternative solution has yet been able to go into operation. In fact, the French Health Data Space is not expected to be realised until after 2025, demonstrating that joint venture requirements do lead of efficiency barriers and delays in the adoption of complex high potential cloud solutions.

4.2. Scenario Definition

Estimations are conducted for three scenarios representing different approaches to implementation at the EU Member State level, reflected by variations in the coverage of high-assurance sectors and use cases respectively (requirements for the highest evaluation levels under the high assurance level CS-EL4).

Based on the taxonomy of sensitive cloud use cases outlined by ENISA for CS-EL4 assurance levels, we developed three scenarios which reflect different sector coverage rates across EU Member States. Taking into account the political preferences of the French government, as stated in June 2023, regarding the expansion of immunity requirements beyond public procurement and critical infrastructure to encompass various other significant sectors of the economy (see introductory part of the study), we consider a "worst-case" scenario. In this scenario, large parts of Europe's private sector economy would be required to comply with CS-EL4 immunity requirements. The remaining two scenarios are considered to be less restrictive in terms of the scope of sectors and use cases. The scenarios are defined as follows:

- Scenario 1 (broad critical sector coverage) reflects an extreme policy environment where all government services and a large portion of commercial users of cloud services in the EU would be banned from using foreign cloud services (the model sought by the French government). CS-EL4 requirements would be applied to sectors of particular sensitivity, which includes the processing of data, whether personal or not, of particular sensitivity, and the breach of which could reasonably be expected to cause serious injury, for example, loss of reputation or competitive advantage, or to cause extremely grave injury, for example, loss of life. [77] The previous EUCS draft, dated May 2023, also explicitly applied CS-EL4 to sectors of particular sensitivity, which includes the processing of data, whether personal or not, of particular sensitivity, and the breach of which may result in a breach of public order, public safety, human life or health, or the protection of intellectual property.[78] Accordingly, all data necessary for the accomplishment of "the functioning of the state" are deemed subject to CS-EL 4 requirements. In our modelling, strict immunity requirements would thus be applied to services executed by public entities (e.g., ministries, local authorities), utilities (e.g., water, gas, electricity), the education sector (e.g., public schools, universities, research institutions), and healthcare services. The requirement to ensure the protection of intellectual property, trade secrets, competitive advantage and loss of reputation would be applied across a broad spectrum of industries in the EU. Strict CS-EL4 immunity requirements are applied to IP-intensive manufacturing and the transportation sector as well as large parts of the financial services industry, the less IP-intensive manufacturing industry, ICT services, and the wholesale and retail industry. By contrast, commodity and agricultural industries, the accommodation

[77] See EU Agency for Network and Information Security (ENISA) 2023 draft EUCS, version V1.0.335, as of August 2023. Application of evaluation levels, pp. 30.

[78] See EU Agency for Network and Information Security (ENISA) 2023 draft EUCS, version V1.0.319, as of May 2023. Application of evaluation levels, pp. 31.

and hospitality sectors, and other less sensitive services sectors would be less affected by CS-EL 4 immunity requirements.

- Scenario 2 (medium critical sector coverage) reflects a less extreme EU policy environment compared to scenario 1. In our modelling, strict CS-EL4 immunity requirements would be applied to services executed by public entities, the education sector, and healthcare services. The requirement to ensure the protection of intellectual property, trade secrets, and business strategies is more narrowly applied across EU industries with high coverage rates for the financial services industry, the transportation sector, and parts of the IP-intensive manufacturing sector. Other industries would be less affected by CS-EL 4 immunity requirements.

- Scenario 3 (narrow critical sector coverage) represents a much narrower approach to the implementation of CS-EL4 immunity requirements where Member States would only ban organisations and entities from using non-EU cloud services in the most sensitive use cases. However, the sector coverage rate is still assumed to be relatively high for public services, the education sector, and the healthcare industry as public services, education and healthcare services are already pressured by regional and federal governments in the EU to ban non-EU providers in some countries.[79] As concerns pervade commercial use cases, many companies and organisations in financial services, transportation services, and the ICT sector might still be subject to CS-EL4 immunity requirements, depending on how a breach of particularly sensitive data that is likely to cause serious injury, such as loss of reputation or competitive advantage, is interpreted. This is because the vague wording of EUCS level CS-EL4 and the definition of data of "particular sensitivity" may cause governments and responsible authorities to cite threats to public order and public safety, the protection of human life or health, the protection of intellectual property and mere business strategies to include many use cases/ entities across industries that may otherwise be considered less sensitive.[80]

The sector aggregation applied in the economic modelling is provided in Table 5 in Annex I. A detailed breakdown of percentage sector coverage rates for the CS-EL 4 requirements applied in the economic modelling is provided in Table 6 in Annex I.[81] Where applicable, sector coverage rates were derived on the basis of the sector taxonomy of the NIS2 Directive for sectors of High

[79] In France and Germany, for example, national and sub-federal data protection authorities aim to ban Microsoft's Office 365 suite and Google Workspace – solutions used by hundreds of millions of firms and individuals globally – from schools to public sector use based on disputed data privacy grounds. 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/. See also 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. As concerns healthcare, see Pollet, M. (2021). French decision to have Microsoft host Health Data Hub still attracts criticism. Available at https://www.euractiv.com/section/health-consumers/news/french-decision-to-have-microsoft-host-health-data-hub-still-attracts-criticism/.

[80] In the least restrictive scenario, scenario 3, we assume a sector coverage rate of 10% for less critical industries. For the wording of potential selection criteria, see, e.g., suitability rationale underlying CS-EL4 immunity requirements in EUCS proposal of August 2023, page 24.

[81] The sector coverage rate is the share of value-added per sector that is assumed to be affected by CS-EL4 immunity requirements.

Criticality (Annex I of NIS2) and other critical sectors (Annex II of NIS2).[82] For those sectors, estimates of coverage rates for CS-EL4 requirements and sector classifications are provided in Table 7 in Annex I. According to Annex I of NIS2, sectors of high criticality include energy, transportation, banks, financial market infrastructures, and digital infrastructures. Public administration is also explicitly mentioned within this category. The category of other critical sectors encompasses postal and courier services, digital service providers, as well as manufacturers of medical devices, mechanical engineering, and vehicle construction.

Our modelling approach accounts for differences in cloud services replacement rates in the EU as time progresses. It also controls for restrictions on European users' access to a growing, more diversified and more productive (e.g., affordable) portfolio of global cloud solutions in the future, including growth in capacities and productivity gains, e.g., from the adoption of edge and quantum computing.[83] In order to keep the number of simulations manageable, we aggregate two groups of countries, the EU27 and the "rest of the world". In addition, all simulations are carried out for individual EU countries, the "rest of the EU" and the "rest of the world". For the EU and individual Member States, estimation results are provided for changes in domestic (real) GDP and changes in sectoral output (production).

We perform two simulations for each scenario, considering different timeframes for impacts to unfold: short-term (approx. 2 years following the implementations (accounting, e.g., for differences in timeframes for national implementation) and medium-term (approx. 5 years following the implementation. We also account the potential impacts of retaliation by non-EU jurisdictions. For each scenario, major assumptions underlying EU and non-EU cloud market developments are outlined in Table 2.

[82] See (NIS2) DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). ANNEX I - SECTORS OF HIGH CRITICALITY and ANNEX II - OTHER CRITICAL SECTORS. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&qid=1692174613412#d1e32-143-1.

[83] McKinsey, for example, outlines, that technologies like cloud and edge computing have demonstrated consistent growth in innovation and are increasingly finding broader applications across various industries. Remarkably, over 400 distinct use cases for edge computing have been recognised across diverse sectors, and it is anticipated that edge computing will experience substantial global growth in the next half-decade. Furthermore, emerging technologies like quantum computing are still evolving and exhibit considerable promise for generating substantial value in the future. See McKinsey (2023). McKinsey Technology Trends Outlook 2023. Available at https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech.

TABLE 2: SCENARIO ASSUMPTIONS REGARDING CLOUD MARKET DEVELOPMENTS OVER TIME

Scenario 1 (broad critical sector coverage)	
1.1 Short-term (approx. 2 years after implementation)	Native EU suppliers would have to fill a gap of at least EUR 27.7 billion in cloud services previously provided by non-EU suppliers, based on the 2022 market shares of EU and non-EU providers.[84] EU supply cannot meet surging demand for "native" EU cloud services, i.e., replacement of foreign cloud solutions cannot take pace in the short-term mainly because of lacking capacities, lacking capabilities (functionalities) and contractual issues (e.g., the duration of legal procedures).[85] At the same time, non-EU cloud services capacities continue to grow at 20% annually, in line with projected global growth.[86]
1.2 Medium-term (approx. 5 years after implementation)	Native EU cloud providers have created additional capacities (data centres) and cloud services offerings (capabilities and functionalities). Native EU cloud services providers have managed to fill the initial gap created by CS-EL4 requirements. However, native EU cloud services capacities are merely at previous (-5Y) levels,[87] while non-EU cloud services capacities have kept growing at 20% annually since the beginning of the implementation of CS-EL4 requirements, in line with projected global growth.
Scenario 2 (medium critical sector coverage)	
2.1 Short-term (approx. 2 years after implementation)	Native EU cloud services providers would have to fill a gap of at least EUR 19 billion in cloud services previously provided by non-EU cloud services providers, based on the 2022 market shares of EU and non-EU providers.[88] Native EU cloud services providers cannot meet surging demand for EU cloud services, i.e., replacement of foreign cloud solutions cannot take pace in the short-term. Non-EU cloud services capacities continue to grow at 20% annually, in line with projected global growth.
2.2 Medium-term (approx. 5 years after implementation)	See scenario 1.2.

[84] Based on NACE sector weights and sector coverage rates.

[85] Due to their uniqueness and the high degree of international competitiveness, many cloud and related data services that are currently used in the EU are characterised by a very low degree of substitutability. Accordingly, in the short- to medium-term these services imports are unlikely to be replaced by EU suppliers. A ban of foreign cloud services in the EU would therefore result in significant short-term distortions of trade and domestic sectoral output. These short-term distortions can be expected to be largest in data-intensive sectors and sectors that to a large extent rely on cloud and related data services as input for production and the management of international operations, e.g., research-intensive companies and companies that operate in global markets.

[86] See, e.g., Fortune Business Insights (2022). The global cloud computing market size. Available at https://www.fortunebusinessinsights.com/cloud-computing-market-102697. Also see GMI (2022). Europe Cloud Computing Market Size. Available at https://www.gminsights.com/industry-analysis/europe-cloud-computing-market.

[87] The assumption that EU providers will be able to fully replace the capacities of non-EU providers within 5 years is quite optimistic. Consider the example of the "French Health Data Hub" (see above), which even 5 years after the termination of the initial awarding of the contract to Microsoft in 2019, is still not operational, not even as a joint venture between French and non-EU cloud services providers. Our choice of a 5-year time horizon is based on the expectation that the French Health Data Hub is at least partly realised by 2025.

[88] Based on NACE sector weights and sector coverage rates.

Scenario 3 (narrow critical sector coverage)	
3.1 Short-term (approx. 2 years after implementation)	Native EU cloud services providers would have to fill a gap of at least EUR 9.6 billion in cloud services previously provided by non-EU suppliers, based on the 2022 market shares of EU and non-EU providers.[89] EU cloud services providers cannot meet surging demand for "native" EU cloud services, i.e., replacement of foreign cloud solutions cannot take pace in the short-term. Non-EU cloud services capacities continue to grow at 20% annually.[90]
3.2 Medium-term (approx. 5 years after implementation)	See scenario 1.2.

In our simulations, we model the de facto ban on importing cloud services into the EU as a reduction in imported ICT services weighted by sector coverage rates. This is necessary because our model does not treat cloud services as a separate service sector, whereas the ICT services sector is recorded as an independent sector in the model. Changes in EU and non-EU capacities over time are modelled through changes in the productivity of ICT intermediary inputs that are used across all sectors of the economy, including public services. A methodological challenge is to determine the proportion of non-EU cloud services that would be covered by CS-EL4 requirements. Data on cloud services trade is generally sparse. The US Bureau of Economic Analysis provides a rough definition, but it is also currently working on a revision of the definitions and statistical classifications. According to the BEA "[c]loud services represent computing services that customers can access from a shared pool of configurable computing resources in a flexible and on-demand way, without active management by the customer." [91] According to recent US trade statistics, total US cloud services exports amounted to USD 7.4 billion in 2022 (EUR 6.9 billion; 11.2% of total US ICT services exports), while total US imports of cloud services amounted to USD 0.52 billion (EUR 480 million; 1% of total US ICT services imports). As concerns trade with the EU, according to BEA statistics, US cloud services exports to the EU amounted to USD 2.2 billion (EUR 2 billion; 13.4% of total US ICT services exports to the EU), while US cloud services imports from the EU amounted to USD 0.16 billion (EUR 150 million; 1.1% of total US ICT services imports from the EU, see Table 4).

As discussed above, it should be noted that determining whom to exclude from the EU under the proposed EUCS framework proves challenging, as its wide-reaching scope potentially can encompass virtually any entity falling within the extensive definition of a cloud service provider. Considering recent EU cloud market data, these numbers seem far too low. For example, assuming a market volume of USD 44 billion for the EU and a market share of US companies of about 75%, the market value of US cloud services would amount to USD 33

[89] Based on NACE sector weights and sector coverage rates.

[90] One may argue that "native" EU companies can more easily meet demand in this least restrictive scenario. This may indeed be the case for individual use cases. However, the example of the "French Health Data Hub" (see above) shows that this is very unlikely, especially when considering the size of the overall EU cloud services market affected by CS-EL4 requitements under this scenario. Note that even 5 years after the termination of the initial awarding of the contract to Microsoft in 2019, the French Health Data Hub is still not operational, not even as a joint venture between French and non-EU cloud services providers.

[91] See BEA (2022). New and Revised Statistics of the U.S. Digital Economy, 2005–2021. Available at https://www.bea.gov/system/files/2022-11/new-and-revised-statistics-of-the-us-digital-economy-2005-2021.pdf.

billion. This would roughly correspond to the sum of the value of EU imports of computer services from the US, as recorded by Eurostat (EUR 24.5 billion in 2021), and the value of data processing, hosting, and related services supplied to foreign persons by US MNEs in Europe, as recorded by the BEA (EUR 11.7 billion in 2020).

The model we use does not differentiate based on the origin of company owners when estimating the level of EU production. However, we can simulate the share of cloud services as the share of ICT services imported from non-EU countries. We therefore assume that the share of US cloud services provided to EU customers in total EU ICT services imports amounts to 37%. Assuming that US cloud services account for 75% of the market share in the EU and that 13% of marketed services are provided by native EU cloud services providers, the total share of non-EU cloud services (87% of the EU market) in total EU ICT services imported from non-EU jurisdictions amounts to approximately 43% of total EU ICT services imports. In the economic modelling, this share is scaled down on the basis of scenario-specific sector coverage weights. Major EU cloud services trade and market indicators are provided by Table 8 in Annex I.

The 43% share should be considered a conservative measure, which could lead to an underestimation of the negative impacts of immunity requirements over the medium- and long-term horizon. The share of cloud and cloud-enabled services are likely to increase in the future due to the adoption of global AI solutions as well as global quantum and edge computing services.[92] Also, since we apply a comparative-static model that does not endogenously take into account the growth of different industries (economies) over time, both the relative and absolute changes in the indicators are likely larger than estimated.[93] Against this background, it is generally important not to take the estimation findings by their face value, but to consider them as an indicator of the direction of the economic effects and their relative magnitude.

4.3. Estimation Results

Below we outline and discuss the results of our estimations. We start with changes in EU aggregate (real) GDP before discussing GDP impacts in individual EU Member States and finally provide an overview of changes in the output of individual industries.

4.3.1. Impacts on Aggregate GDP in the EU27

The results of our estimations clearly show that for all scenarios, including the least restrictive scenario, the loss of access to global cloud solutions would result in large losses in aggregate economic output, as reflected by significant losses in annual GDP. For the most restrictive scenario with broad critical sector coverage annual EU GDP is estimated to decrease by 3% in the short-term (approx. 2 years) when non-EU cloud services cannot be replaced by native EU capacities. Adding the impact of forgone capacity and productivity growth, i.e., ongoing growth in cloud

[92] See, e.g., McKinsey (2023). McKinsey Technology Trends Outlook 2023. Available at https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech. Also see the economic potential of generative AI The next productivity frontier. Available at https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-AI-the-next-productivity-frontier#/.

[93] Industries and economies keep growing in the future. See, e.g., IMF (2023). World Economic Outlook. Available at https://www.imf.org/en/Publications/WEO.

markets outside the EU, EU GDP is estimated to be 3.9% lower than it would be in absence of broadly applied CS-EL4 immunity requirements. For scenario 2 (medium critical sector coverage) and scenario 3 (narrow critical sector coverage), the estimated decrease in EU27 GDP is -2% and -0.2% respectively (see Figure 8). In terms of 2022 EU GDP, annual output losses of the EU would amount to EUR 610 billion, EUR 317 billion, and EUR 29 billion respectively (see Figure 9). This means that annual EU GDP would be higher by these estimates if the CS-EL4 immunity rules were not implemented as assumed in the underlying scenarios.

Importantly, our estimates demonstrate that aggregate annual output losses accumulate significantly over time. The findings show that EU countries would significantly miss out on global growth trends in cloud services markets. Outside the EU, businesses and public services sectors would continue to benefit from growing capacities and innovation. By contrast, EU businesses and public services sectors would no longer be able benefit from growing global cloud services capacities and only have access to slowly growing EU services capacities and services that are lagging global innovation and productivity growth.

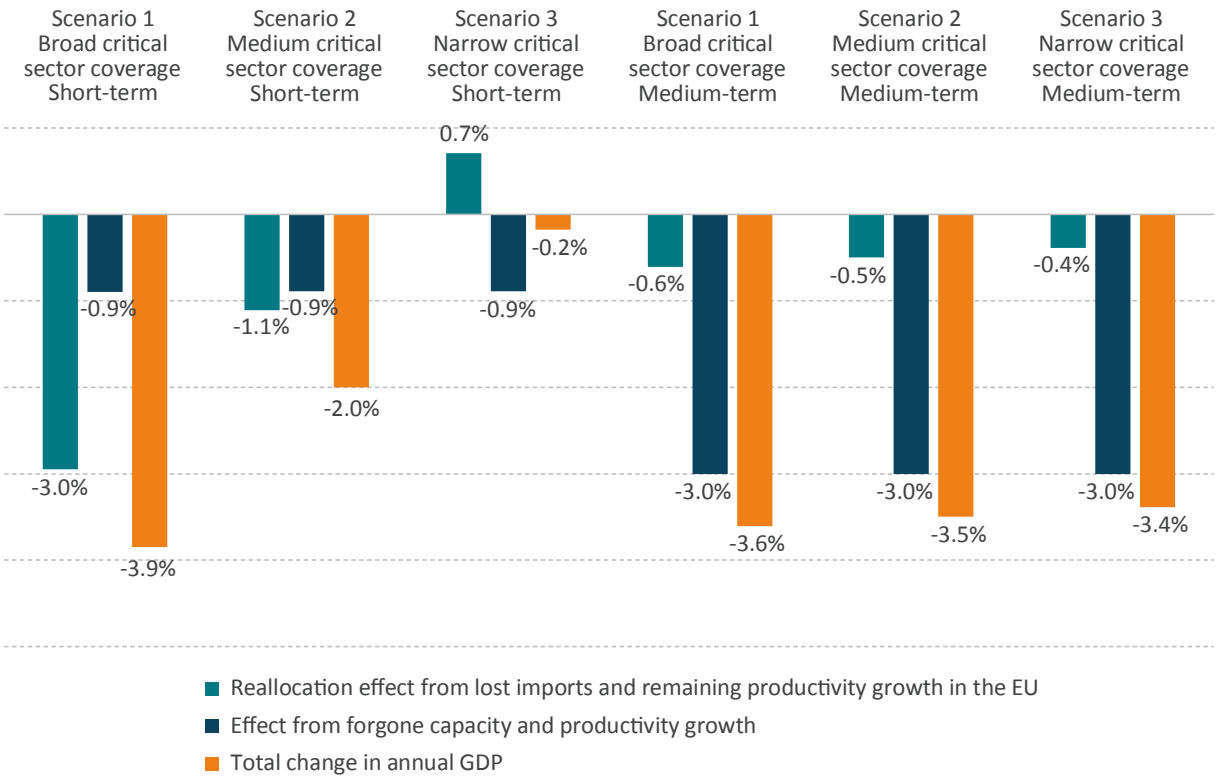
This applies particularly to the most restrictive scenarios, scenario 1 and scenario 2. The estimated output losses are generally lower the more EU companies and public services entities continue to have access to innovative and growing global cloud services solutions. The estimates clearly show that even in the 5-year period, where we optimistically assume that non-EU cloud capacities will be replaced by EU cloud capacities up to the level before the implementation of the immunity rules, the aggregate annual output losses for the EU are enormous, amounting to an estimated EUR 572 billion and EUR 554 billion respectively. For scenario 3 with narrow critical sector coverage, our estimates show that negative reallocation effects and the effects from forgone cloud capacity and productivity growth in the EU tends to be lowest. In Scenario 3, a large part of the EU cloud market would continue to grow through the participation of non-EU providers. Strictly narrowing the scope of high assurance requirements would allow most EU industries and public services to benefit from growth in innovative global cloud capacities, growing cloud-enabled application (such as AI, quantum computing, and edge computing), and associated productivity gains. At the same time, GDP growth would still be considerably lower as a result of the restrictions that still exist for cloud adoption in critical sectors. Overall EU capacities are growing more slowly than in non-EU countries, which results in aggregate losses in GDP in the short- and the medium-term.

It should be noted that equal retaliation against EU cloud services exports by the "rest of the world", a possibility that we accounted for in separate simulations of scenario 1 to 3, would indeed result in additional GDP losses. These additional losses are, however, relatively low compared to the combined effects from EU capacity losses and forgone capacity and productivity growth in the EU. For example, the short-term GDP losses the EU would experience in Scenario 1 would be 0.04% higher, while the rest of the world would also grow at a lower rate because of retaliation. Although the effects are relatively small, their absolute magnitude should not be underestimated.

At the same time, it must be taken into account that punitive measures against the EU are unlikely to be imposed on the relatively small EU cloud services export sector, but, as envisaged in the case of EU digital services taxes, on important EU export sectors. As outlined in a previous

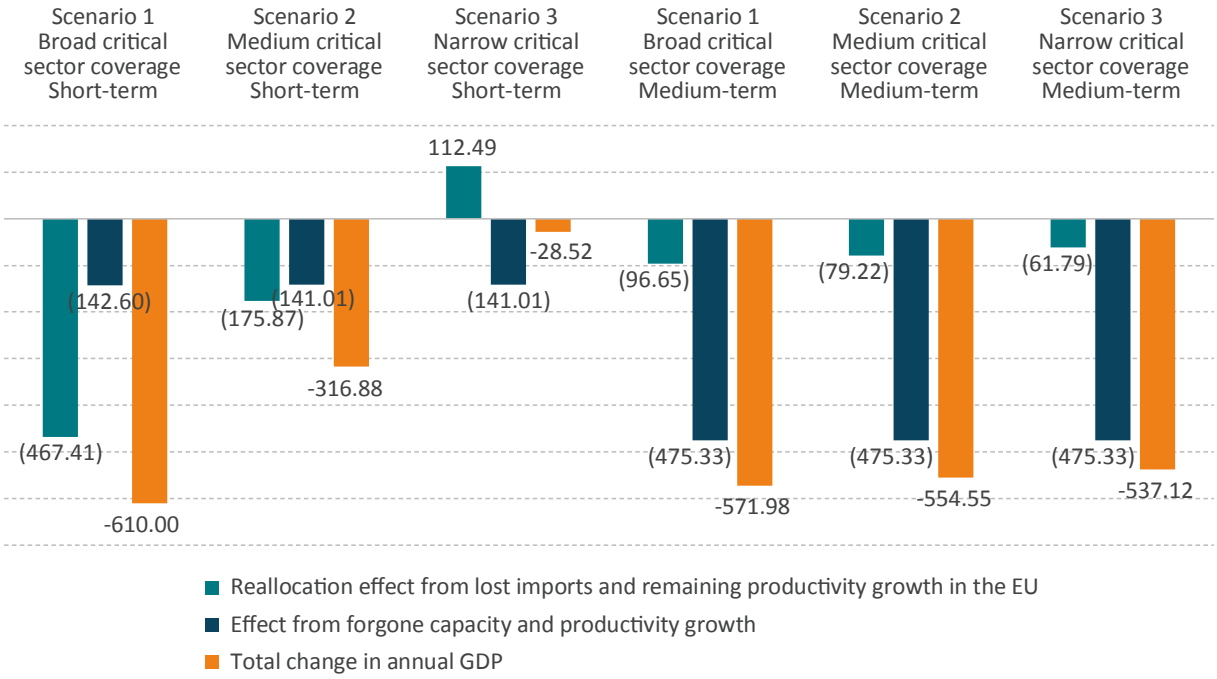
ECIPE publication on the impact of the proposed EUCS scheme, strict local establishment obligations and rigorous foreign ownership limitations could have farther reaching effects than, for example, taxes on digital services. [94] US retaliation could substantially exceed the value of covered trade determined for retaliatory tariffs against EU taxes on digital services. Depending on US preferences, a 25% retaliatory tariff could be imposed on at least about EUR 11 billion worth of goods (or equivalent restrictions for EU services exports to the US). Depending on the exact share of high assurance services in total cloud services, the value of trade covered by retaliation could increase significantly. It should also be noted that 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, and likewise, become target sectors for retaliation against the EU.

FIGURE 8: ESTIMATED LOSSES IN REAL GDP IN %, ALL SCENARIOS, EXCLUDING RETALIATION EFFECTS



[94] ECIPE (2023). Building Resilience? The Cybersecurity, Economic & Trade Impacts of Cloud Immunity Requirements. Available at https://ecipe.org/wp-content/uploads/2023/02/ECI_23_PolicyBrief_01-2023_LY07.pdf?_gl=1*1e01wlx*_up*MQ..*_ga*MjA2NTQ2MjI1OS4xNjk1Mzk4OTEy*_ga_T9CCK5HNCL*MTY5NTM5ODkxMi4xLjAuMTY5NTM5ODkxMi4wLjAuMA.

FIGURE 9: ESTIMATED LOSSES IN REAL GDP, ALL SCENARIOS AND TIME HORIZONS, IN EUR BILLION, EXCLUDING RETALIATION EFFECTS



4.3.2. Impacts on Member States' GDP

Our estimates show that smaller EU countries tend to experience higher GDP losses compared to larger EU countries. The relative losses in national income and corresponding losses in welfare would be greatest in smaller EU Member States which heavily rely on imported ICT services and whose economies are characterised by a high share of high-value-added production, especially high-value added manufacturing, digital services, and digitally enabled services (such as financial services, business and professional services, and ICT services).[95]

As exemplarily outlined for the most restrictive scenario, in the short-term, small ICT-intensive economies like Luxembourg (-9.3%), the Netherlands (-5.8%), Belgium (-5.4%), Denmark (-4.9%), Ireland (-4.7%), and Sweden (-4.6%) would experience the highest relative losses in economic output (see Table 3 and Figure 10 below). However, since our model is comparative static and does not account for changing ICT intensities over time, it does not well capture the additional potential output losses that would accrue because of countries' transitions towards more ICT-intensive production, also known as the servification of economies, which is a general trend in the EU and globally. The relative magnitude of the effects is therefore systematically underestimated in our model, especially over longer periods of time. This affects both economies that already have a relatively high ICT intensity and are less

[95] For a taxonomy of digital and digitally enabled services see BEA (2023). International Trade in ICT and Potentially ICT-Enabled Services. Available at https://www.bea.gov/data/special-topics/digital-economy. Also see OECD (2019). Barriers to trade in digitally enabled services in the G20. Available at https://www.oecd-ilibrary.org/trade/barriers-to-trade-in-digitally-enabled-services-in-the-g20_264c4c02-en.

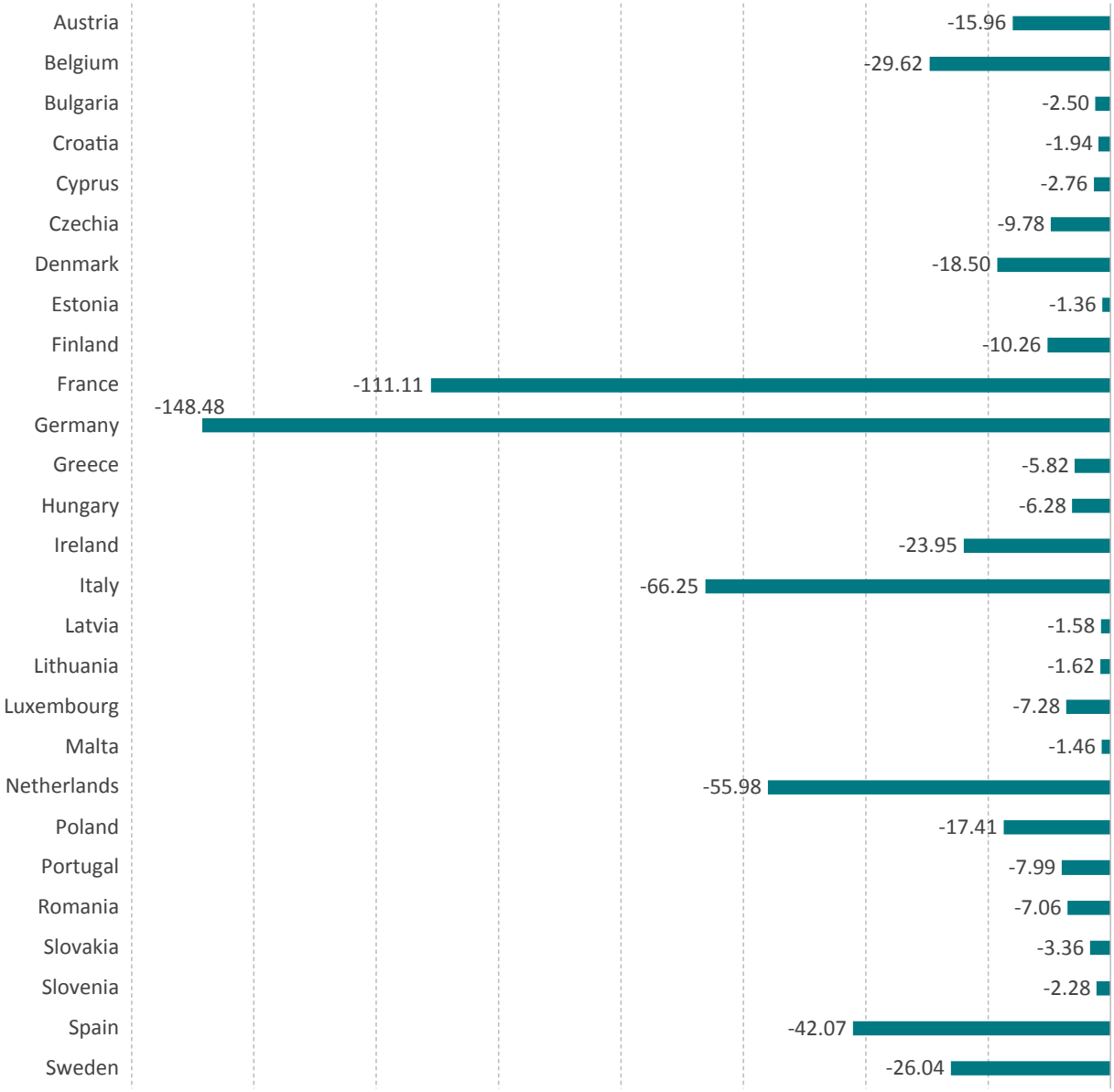
developed EU economies. The latter in particular (e.g., Bulgaria, Croatia, Greece, Lithuania, Poland, Portugal, and Romania) would be deprived of their long-term potential growth by restrictive cloud immunity rules (see, e.g., last column of see Table 3 below). This would slow-down economic development and impede the process of economic convergence of these Member States.

The highest absolute losses in economic output and income respectively would be registered in the largest EU economies. In the most restrictive scenario, scenario 1, annual GDP losses amount EUR 148 billion for namely Germany (-3.8%), EUR 111 billion for France (-4.2%), EUR 66 billion for Italy (-3.5%), and EUR 42 billion for Spain (-3.2%). Again, due to the static treatment of ICT-intensities of production, the relative magnitude of the effects is systematically underestimated in our model, especially over longer periods of time.

TABLE 3: TOTAL ANNUAL LOSSES IN REAL GDP FROM CAPACITY LOSSES AND FORGONE PRODUCTIVITY GROWTH, IN %, SCENARIO 1 (BROAD CRITICAL SECTOR COVERAGE), EXCLUDING RETALIATION EFFECTS

Total forgone growth, in %	Scenario 1 Broad critical sector coverage Short-term (2Y)	Scenario 1 Broad critical sector coverage Medium-term (5Y)
EU27	-3.9%	-3.6%
Austria	-3.6%	-3.4%
Belgium	-5.4%	-4.0%
Bulgaria	-3.0%	-3.3%
Croatia	-2.9%	-3.3%
Cyprus	-10.2%	-6.5%
Czechia	-3.5%	-3.4%
Denmark	-4.9%	-4.1%
Estonia	-3.8%	-3.6%
Finland	-3.8%	-3.5%
France	-4.2%	-3.7%
Germany	-3.8%	-3.6%
Greece	-2.8%	-3.6%
Hungary	-3.7%	-3.5%
Ireland	-4.7%	-4.1%
Italy	-3.5%	-3.4%
Latvia	-4.1%	-3.8%
Lithuania	-2.4%	-3.5%
Luxembourg	-9.3%	-4.8%
Malta	-8.5%	-5.0%
Netherlands	-5.8%	-4.3%
Poland	-2.7%	-3.3%
Portugal	-3.3%	-3.5%
Romania	-2.5%	-3.3%
Slovakia	-3.1%	-3.2%
Slovenia	-4.0%	-3.7%
Spain	-3.2%	-3.6%
Sweden	-4.6%	-3.8%

FIGURE 10: TOTAL LOSSES IN REAL GDP FROM CAPACITY LOSSES AND FORGONE PRODUCTIVITY GROWTH, SCENARIO 1 (BROAD CRITICAL SECTOR COVERAGE), SHORT-TERM TIME HORIZON (APPROX. 2Y AFTER IMPLEMENTATION), EXCLUDING RETALIATION EFFECTS



Note: Changes in EU GDP based on 2022 gross domestic product at market prices as provided by Eurostat.

4.3.3. Impacts on Sectoral Output (Production)

The industries experiencing the largest negative impacts on production are those that would be most susceptible to the CS-EL4 immunity requirements, as entities in these sectors would no longer be able to use global cloud services and, in addition, cannot benefit from global capacity and productivity growth anymore. In general, our output estimates point to a reallocation of productive resources away from ICT-intensive industries to sectors that use ICT services less intensively, e.g., commodity sectors, the agricultural sector, and the manufacturing sectors.

Depending on how restrictive a scenario is, there may be further capacity and productivity growth in cloud services available in the EU from which cloud adopting sectors would benefit. This is accounted for in our simulations (through the application of different sector coverage rates). However, looking at the results, we find for all time horizons that growth in cloud markets not affected by immunity requirements would not be sufficient for the EU to compensate for significant output losses relative to cloud market growth outside the EU. Looking at estimated output growth in sectors that intensively use ICT-services and at the same time would be subject to CS-EL4 immunity requirements, we find a significant output gap in the growth of EU industries and the growth of corresponding sectors outside the EU (see Table 4).

TABLE 4: PERCENTAGE CHANGE IN SECTORAL PRODUCTION OF EU27 AND REST OF WORLD (ROW), EXCLUDING RETALIATION EFFECTS

Percentage change in sectoral production of EU27	Scenario 1 Broad critical sector coverage Short-term	Scenario 2 Medium critical sector coverage Short-term	Scenario 3 Narrow critical sector coverage Short-term	Scenario 1 Broad critical sector coverage Medium-term	Scenario 2 Medium critical sector coverage Medium-term	Scenario 3 Narrow critical sector coverage Medium-term
Financial services	-3.33%	-1.11%	0.85%	0.08%	0.25%	0.41%
Wholesale, retail, e-commerce	-3.02%	-0.64%	0.82%	-0.80%	-0.63%	-0.48%
Healthcare services	-2.95%	-1.43%	0.25%	-0.92%	-0.84%	-0.76%
Education services	-1.41%	-1.09%	-0.40%	0.03%	0.07%	0.11%
Transportation services	-0.18%	0.06%	0.20%	0.95%	1.04%	1.12%
Services provided by govenrmental institutions	-3.76%	-0.92%	0.21%	-0.75%	-0.65%	-0.55%
Percentage change in sectoral production of RoW	**Scenario 1 Broad critical sector coverage Short-term**	**Scenario 2 Medium critical sector coverage Short-term**	**Scenario 3 Narrow critical sector coverage Short-term**	**Scenario 1 Broad critical sector coverage Medium-term**	**Scenario 2 Medium critical sector coverage Medium-term**	**Scenario 3 Narrow critical sector coverage Medium-term**
Financial services	0.79%	0.85%	0.64%	2.15%	2.14%	2.13%
Wholesale, retail, e-commerce	0.83%	0.71%	0.65%	2.32%	2.30%	2.29%
Healthcare services	0.94%	0.91%	0.89%	3.05%	3.06%	3.06%
Education services	0.77%	0.79%	1.07%	2.63%	2.63%	2.63%
Transportation services	0.15%	0.32%	0.45%	1.11%	1.10%	1.09%
Services provided by govenrmental institutions	1.13%	1.11%	1.07%	3.66%	3.66%	3.66%

5. CONCLUSIONS

The EU is proposing the European Cybersecurity Certification Scheme for Cloud Services (EUCS), aimed at preventing non-European cloud vendors from offering "high assurance level" cloud services in the EU. This study examined the potential consequences of EUCS immunity requirements, including data localisation, foreign ownership restrictions, and local staff requirements, revealing significant economic losses and a growing divide between EU and global growth.

Cloud and cloud enabled services have become important drivers of domestic and international commerce, enabling businesses of all sizes to access global data, enhance collaboration, and boost competitiveness. Cloud-based solutions have improved public services and government administration, with transformative potential. While the global cloud computing market has expanded substantially over the past decade, European providers have lagged in innovation and competitiveness compared to non-EU counterparts, resulting in declining market shares.

Exploring the economic impacts of implementing immunity requirements under the EUCS framework, this study shows that strict obligations for cloud services and their providers would further disconnect the EU from technology, innovation, and global industry growth. Even in the least restrictive scenario, EU annual GDP would see a substantial decline, with the most stringent scenario projecting a 3.9% decrease in the short-term when considering lost capacities and forgone capacity and productivity growth. Smaller EU countries, especially those reliant on imported ICT services and high-value-added production, would be disproportionately affected, while the largest EU economies would experience the highest absolute losses in economic output. Considering longer-term impacts, less economically developed EU countries where production is on aggregate still less ICT-intensive would be deprived of their long-term potential growth by restrictive cloud immunity rules.

In conclusion, this research underscores the potential economic ramifications associated with constraining EU access to global cloud services solutions. The negative impacts are significant for both smaller but also larger EU nations, underscoring the imperative of contemplating the broader short- and long-term consequences of immunity prerequisites. The outcomes are in line with the broader picture of EU digital policy, which, in the past, has not contributed to improvements in the competitiveness of EU digital and less digital industries. EUCS immunity requirements risk to further widen the EU's growth and technology gap compared to other developed economies.

Consequently, EU Member States should advocate for ENISA and the European Commission to discard discriminatory and potentially far-reaching immunity requirements in the proposed cloud certification framework, EUCS.

ANNEX I: SECTOR AGGREGATION AND COVERAGE RATES APPLIED FOR CS-EL 4 REQUIREMENTS

TABLE 5: GTAP SECTOR CLASSIFICATION AND ALLOCATION

Name	GTAP sectors
Less IP-intensive manufacturing	26-31
IP-intensive manufacturing	32-45
Finance and insurance services	57; 58
Wholesale and retail trade services	50
Professional and technical activities, support services	59;60
Transportation and logistics services	52-55
ICT services	56
Healthcare services	64
Education services	63
Utilities	46-48
Government services	62
Other (less sensitive) sectors	1-25; 49; 51; 61; 65

Source: authors own aggregation based on detailed GTAP sectoral list.[96]

[96] See detailed GTAP sectoral list. Available at https://www.gtap.agecon.purdue.edu/databases/contribute/detailedsector.asp.

TABLE 6: EU SECTOR COVERAGE RATES OF CS-EL 4 IMMUNITY REQUIREMENTS

Sector	Scenario 1	Scenario 2	Scenario 3
Less IP-intensive manufacturing	80%	20%	10%
IP-intensive manufacturing	100%	17%[97]	10%
Finance and insurance	100%	80%	13%
Wholesale and retail trade incl. repair of motor vehicles	80%	20%	10%
Professional and technical activities, support services	50%	17%	10%
Transportation and storage	100%	83%	49%
ICT services	80%	67%	11%
Healthcare services	100%	100%	65%
Education	100%	100%	75%
Utilities	100%	100%	51%
Government services	100%	88%	44%
Other (less sensitive) sectors	50%	20%	10%

[97] As with other sectors, there is much uncertainty about how severely companies and organisations classified as "IP intensive" will be affected by restrictive EUCS immunity requirements. We have applied a relatively low value for scenario 2 (17% coverage rate) because there are many international cooperation in this area in particular, which make undesirably and, also, technically and legally difficult to impose restrictive EUCS requirements without having the effect of severely disrupting R&D and production chains.

TABLE 7: GTAP SECTOR CLASSIFICATION AND ALLOCATION

Sector	Scenario 1: EUCS EL 4 applies to all sectors in NIS2	Scenario 2: EUCS EL4 applies to all "Sectors of High Criticality" and some "other critical sectors" in NIS2	Scenario 3: EUCS EL4 applies to some organi-sations operating in "Sectors of High Criticality" and "other critical sectors" in NIS2	Sector assignment in model-ling
1) Sectors of High Criticality (ANNEX I NIS2)				
a) Energy	100%	100%	51%	Utilities
Electricity	100%	100%	60%	
Electricity undertaking	100%	100%	25%	
Distribution system operators	100%	100%	100%	
Transmission system operators	100%	100%	100%	
Producers	100%	100%	75%	
Nominated electricity market operators	100%	100%	100%	
Market participants	100%	100%	10%	
Operators of a recharging point	100%	100%	10%	
District heating and cooling	100%	100%	50%	
Operators of district heating or district cooling	100%	100%	50%	
Oil	100%	100%	50%	
Operators of oil transmission pipelines	100%	100%	25%	
Operators of oil production, refining and treatment facilities, storage and transmission	100%	100%	25%	
Central stockholding entities	100%	100%	100%	
Gas	100%	100%	68%	
Supply undertakings	100%	100%	75%	
Distribution system operators	100%	100%	100%	
Transmission system operators	100%	100%	100%	
Storage system operators	100%	100%	100%	
LNG system operators	100%	100%	50%	
Natural gas undertakings	100%	100%	25%	
Operators of natural gas refining and treatment facilities	100%	100%	25%	
Hydrogen	100%	100%	25%	
Operators of hydrogen production, storage and transmission	100%	100%	25%	

Sector	Scenario 1: EUCS EL 4 applies to all sectors in NIS2	Scenario 2: EUCS EL4 applies to all "Sectors of High Criticality" and some "other critical sectors" in NIS2	Scenario 3: EUCS EL4 applies to some organisations operating in "Sectors of High Criticality" and "other critical sectors" in NIS2	Sector assignment in modelling
b) Transport	100%	100%	46%	Transportation and logistics services
Air	100%	100%	53%	
Air carriers	100%	100%	10%	
Airport managing bodies, airports, ancillary airport service operators	100%	100%	75%	
Traffic management control operators	100%	100%	75%	
Rail	100%	100%	63%	
Infrastructure managers	100%	100%	75%	
Railway undertakings	100%	100%	50%	
Water	100%	100%	45%	
passenger and freight water transport companies	100%	100%	10%	
Managing bodies of ports, including their port facilities, entities operating works and equipment contained within ports	100%	100%	25%	
Operators of vessel traffic services	100%	100%	100%	
Road	100%	100%	25%	
Road authorities	100%	100%	75%	
Operators of Intelligent Transport Systems	100%	100%	10%	
c) Banking	100%	100%	15%	Finance and insurance services
Credit institutions	100%	100%	15%	
d) Financial market infrastructures	100%	100%	10%	Finance and insurance services
Operators of trading venues	100%	100%	10%	
Central counterparties	100%	100%	10%	
e) Health	100%	100%	65%	Healthcare services
Healthcare providers	100%	100%	100%	
EU reference laboratories	100%	100%	100%	

Sector	Scenario 1: EUCS EL 4 applies to all sectors in NIS2	Scenario 2: EUCS EL4 applies to all "Sectors of High Criticality" and some "other critical sectors" in NIS2	Scenario 3: EUCS EL4 applies to some organisations operating in "Sectors of High Criticality" and "other critical sectors" in NIS2	Sector assignment in modelling
Entities carrying out research and development activities of medicinal products	100%	100%	25%	
Entities manufacturing basic pharmaceutical products	100%	100%	25%	
Entities manufacturing medical devices considered to be critical during a public health emergency	100%	100%	75%	
Drinking water	100%	100%	25%	Utilities
Suppliers and distributors of water intended for human consumption	100%	100%	25%	
Waste, water	100%	100%	50%	Utilities
Undertakings collecting, disposing of or treating urban wastewater, domestic wastewater or industrial wastewater	100%	100%	50%	
h) Digital infrastructure	100%	100%	16%	ICT services
Internet Exchange Point providers	100%	100%	0%	
DNS service providers	100%	100%	10%	
TLD name registries	100%	100%	0%	
Cloud computing service providers	100%	100%	25%	
Data centre service providers	100%	100%	25%	
Content delivery network providers	100%	100%	5%	
Trust service providers	100%	100%	25%	
Providers of electronic communications networks	100%	100%	25%	
Providers of publicly available electronic communications services	100%	100%	25%	
i) ICT service management	100%	100%	18%	ICT services
Managed service providers	100%	100%	10%	
Managed security service providers	100%	100%	25%	
j) Public administration	100%	100%	75%	Government services
Public administration entities of central governments	100%	100%	100%	
Public administration entities at regional level	100%	100%	50%	

Sector	Scenario 1: EUCS EL 4 applies to all sectors in NIS2	Scenario 2: EUCS EL4 applies to all "Sectors of High Criticality" and some "other critical sectors" in NIS2	Scenario 3: EUCS EL4 applies to some organisations operating in "Sectors of High Criticality" and "other critical sectors" in NIS2	Sector assignment in modelling
k) Space	100%	100%	90%	Other sectors
Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties	100%	100%	90%	
b) Other critical sectors (ANNEX II NIS2)				
Postal and courier services	100%	50%	50%	Transportation and logistics services
Waste management	100%	50%	25%	Utilities
Manufacture, production and distribution of chemicals	100%	0%	0%	IP-intensive manufacturing
Production, processing and distribution of food	100%	0%	0%	Less IP-intensive manufacturing
Manufacturing of	100%	17%	0%	IP-intensive manufacturing
Medical devices and in vitro diagnostic medical devices	100%	25%	0%	
Computer, electronic and optical products	100%	25%	0%	
Electrical equipment	100%	25%	0%	
Machinery	100%	25%	0%	
Motor vehicles, trailers, and semi-trailers	100%	0%	0%	
Other transport equipment	100%	0%	0%	
Digital providers	100%	0%	0%	ICT services
Online marketplaces	100%	0%	0%	
Online search engines	100%	0%	0%	
Social network platforms	100%	0%	0%	
Research organisations	100%	50%	50%	Other sectors

TABLE 8: EU CLOUD SERVICES TRADE AND MARKET INDICATORS

Indicator	2022 value in billion	Currency	Source
European cloud market	44.0	USD	Synergy research
Total extra-EU imports of ICT services	98.3	EUR	Eurostat
Total extra-EU exports of ICT services	248.8	EUR	Eurostat
Total extra-EU imports of computer services	67.5	EUR	Eurostat (2021 value)
Total extra-EU exports of computer services	196.2	EUR	Eurostat (2021 value)
Total extra-EU imports of information services	6.5	EUR	Eurostat (2021 value)
Total extra-EU exports of information services	10.2	EUR	Eurostat (2021 value)
Total EU imports of ICT services from US	34.8	EUR	Eurostat
Total EU exports of ICT services to US	50.8	EUR	Eurostat
Total EU imports of computer services from US	24.5	EUR	Eurostat (2021 value)
Total EU exports of computer services to US	36.6	EUR	Eurostat (2021 value)
Total EU imports of information services from US	2.4	EUR	Eurostat (2021 value)
Total EU exports of information services to US	1.8	EUR	Eurostat (2021 value)
EU exports of ICT services to US	14.4	USD	US Bureau of Economic Analysis
EU imports of ICT services from US	16.4	USD	US Bureau of Economic Analysis
EU exports of computer services to US	11.9	USD	US Bureau of Economic Analysis
EU imports of computer services from US	10.8	USD	US Bureau of Economic Analysis
EU exports of cloud services to US	0.16	USD	US Bureau of Economic Analysis
EU imports of cloud services from US	2.2	USD	US Bureau of Economic Analysis
Data processing, hosting, and related supplied to foreign persons by US MNEs in Europe	12.6	USD	US Bureau of Economic Analysis (2020 value)
Market shares	**2022 value**		**Source**
Market share European service providers	13%		Synergy research
Market share non-European service providers	87%		Synergy research

TABLE 9: INDICATORS OF EU CLOUD AND CLOUD-ENABLED SERVICES IN TOTAL ICT SERVICES IMPORTS

Indicators of EU cloud and cloud-enabled services in total ICT services imports	Value	Source
Extra-EU imports of computer services in extra-EU imports of ICT services	68.7%	Eurostat
Extra-EU imports of information services in extra-EU imports of ICT services	6.6%	Eurostat
EU imports of cloud services from US in total ICT services imports from US	13.4%	US Bureau of Economic Analysis
EU imports of computer services from US in total ICT services imports from US	65.9%	US Bureau of Economic Analysis
[EU imports of computer services from US + Data processing, hosting, and related supplied to Foreign Persons by US MNEs in Europe] in European cloud market	53%	Synergy research US Bureau of Economic Analysis

ANNEX II: KEY ASSUMPTIONS AND LIMITATIONS OF THE CGE MODEL

In this study, CGE model simulations are conducted on the basis of the standard model by the Global Trade Analysis Project (GTAP) at the University of Purdue. CGE models are frequently used in economic impact assessments to estimate the magnitude of economic feedback effects, including structural changes in countries' international trade profiles for goods and services.

The model applied in this analysis is static-comparative and has been applied frequently in studies on the impacts of various trade policy measures such as tariffs and non-tariff trade barriers (NTBs). We apply a multi-regional and multi-sector model, characterised by perfect competition, constant returns to scale and a set of fixed Armington elasticities. The modelling is conducted on the basis of the default macro-closure, which applies a savings-driven model, i.e., the savings rate is exogenous, and the investment rate will adjust.

As concerns the economic base data on which we run the simulations, we apply the most up-to-date GTAP 11 database released in 2023. The database contains global trade data for 2004, 2007, 2011, 2014 and 2017 as reference years based on input output tables and recorded trade protection data. The database covers 141 countries and 19 aggregate regions of the world for each reference year. The sectoral coverage includes a total of 65 sectors. The GTAP 11 dataset on the global economy was extrapolated to reflect the "best estimate" of the global economy today.

Like any applied economic model, our model is based on several assumptions, which simplify complex behavioural economic relationships and the policy framework. The results of the estimations therefore only have indicative character as it is not possible to forecast the precise economic impacts of regulatory changes on macro-economic variables, mainly due to lack of empirical data, the influence of a many different policy and non-policy factors and causal relationships that change over time (Lucas critique).

In the following, we outline key assumptions and their implications for the modelling of the scenarios and the interpretation of the modelling results.

1) The applied model is comparative-static, i.e., the simulation results reflect two equilibria at different points in time. As concerns the timeframe for the economic impacts to evolve, the time horizon generally depends on the nature of the simulated policy shock. The timeframe is also sensitive to industry characteristics thus needs to be interpreted and discussed on a scenario-by-scenario basis (see discussion below).

2) The model assumes full factor mobility and full employment of factors of production, i.e., all factors of production including labour will adjust until they are fully absorbed by other sectors after the policy changes, has critical implications for the modelling and the assessment of the time horizon within which policy-induced economic impacts will unfold.

4) As concerns the "static" nature of the model, the model does not account for policy-induced changes in investment (both increases in investment and divestment). Neither does the static model endogenously capture economic growth, technological innovation, business model innovations and their implications on productivity. In the model, changes in productivity and, as a derivative, overall industrial output are only accounted for by the reallocation of production factors, e.g., capital and labour migrating to sectors in which they operate with lower or higher marginal productivity after the imposition of a policy shock. As a result, static models tend to under-predict the economic losses that follow the erection of new barriers to international trade as the link between innovation and productivity growth, on the one hand, and exports, imports, competition, and investment, on the other hand, is neglected. To correct this build-in bias, accounting for the well-documented positive impacts of trade and digitalisation on firm-level productivity, the simulations we conduct account for some of the effects of productivity changes in ICT / cloud services that are used by businesses and the public sector as input for production.

Discussion of timeframe of impacts of immunity requirements on cloud services providers and users of cloud services

As concerns the "comparative" dimension of the model, the time horizon for a new economic equilibrium to evolve critically depends, amongst other factors, on the policy scenarios, the industries directly and indirectly affected by regulatory changes, the degree of competition as well as the degree of substitutability of imports from abroad relative to domestic goods and services and vice versa.

As concerns cloud services, new regulatory requirements that increase businesses' costs while still allowing foreign cloud providers to operate in the EU will increase the costs of trade in the short-term and can be expected to remain a cost component for European companies over time. By contrast, a ban of foreign cloud services in the EU would result in significant short-term distortions of trade and domestic sectoral output. These short-term distortions can be expected to be largest in data-intensive sectors and sectors that to a large extent rely on cloud and related data services as input for production and the management of international operations, e.g., research-intensive companies and companies that operate in global markets.

Due to their uniqueness and the high degree of international competitiveness, many cloud and related data services that are currently used in the EU are characterised by a very low degree of substitutability. Accordingly, in the short- to medium-term these services imports are unlikely to be replaced by EU suppliers. Replacing the loss of imports of unique and internationally highly competitive cloud services would only be possible over a relatively long period of time. For example, if EU businesses lose access to relatively unique cloud services imports from non-EU countries, significant additional investment would be needed in the EU to establish new technological capacities (e.g., data centres), functionalities, and business entities that allow for the utilisation of significant network effects and economies of scale respectively.

For the simulation of the economic implications of immunity requirements, we therefore run three sets of simulations (as reflected by our scenarios) to compare our baseline with a "comparative" situation that accounts for the evolution of replacement effects and market development outside the EU.

ANNEX III: DETAILED BREAKDOWN OF ESTIMATION RESULTS FOR CHANGES IN REAL GDP

TABLE 10: TOTAL ANNUAL LOSSES IN REAL GDP, IN %, SHORT-TERM HORIZON (2Y)

Total forgone growth, in %	Scenario 1 Broad critical sector coverage Short-term	Scenario 2 Medium critical sector coverage Short-term	Scenario 3 Narrow critical sector coverage Short-term
EU27	-3.9%	-2.0%	-0.2%
Austria	-3.6%	-1.9%	-0.1%
Belgium	-5.4%	-2.7%	0.2%
Bulgaria	-3.0%	-1.7%	-0.5%
Croatia	-2.9%	-1.6%	-0.4%
Cyprus	-10.2%	-6.1%	0.1%
Czechia	-3.5%	-1.9%	-0.2%
Denmark	-4.9%	-2.4%	-0.2%
Estonia	-3.8%	-2.0%	-0.2%
Finland	-3.8%	-2.0%	-0.2%
France	-4.2%	-2.2%	0.0%
Germany	-3.8%	-1.9%	-0.2%
Greece	-2.8%	-1.6%	-0.5%
Hungary	-3.7%	-1.9%	-0.3%
Ireland	-4.7%	-2.7%	-0.2%
Italy	-3.5%	-1.7%	-0.2%
Latvia	-4.1%	-2.1%	-0.2%
Lithuania	-2.4%	-1.5%	-0.7%
Luxembourg	-9.3%	-4.5%	1.2%
Malta	-8.5%	-4.5%	0.6%
Netherlands	-5.8%	-3.0%	0.0%
Poland	-2.7%	-1.5%	-0.4%
Portugal	-3.3%	-1.8%	-0.3%
Romania	-2.5%	-1.4%	-0.5%
Slovakia	-3.1%	-1.5%	-0.3%
Slovenia	-4.0%	-1.9%	-0.1%
Spain	-3.2%	-1.6%	-0.3%
Sweden	-4.6%	-2.5%	-0.1%

TABLE 11: TOTAL ANNUAL LOSSES IN REAL GDP, IN EUR BILLION, SHORT-TERM HORIZON (2Y)

Total forgone growth, in EUR billion	Scenario 1 Broad critical sector coverage Short-term	Scenario 2 Medium critical sector coverage Short-term	Scenario 3 Narrow critical sector coverage Short-term
EU27	-610.00	-316.88	-28.52
Austria	-15.96	-8.36	-0.31
Belgium	-29.62	-14.62	1.21
Bulgaria	-2.50	-1.40	-0.39
Croatia	-1.94	-1.04	-0.26
Cyprus	-2.76	-1.64	0.02
Czechia	-9.78	-5.11	-0.41
Denmark	-18.50	-9.21	-0.80
Estonia	-1.36	-0.71	-0.09
Finland	-10.26	-5.43	-0.59
France	-111.11	-58.32	0.26
Germany	-148.48	-74.82	-6.20
Greece	-5.82	-3.27	-1.12
Hungary	-6.28	-3.15	-0.48
Ireland	-23.95	-13.57	-1.06
Italy	-66.25	-31.88	-3.82
Latvia	-1.58	-0.81	-0.08
Lithuania	-1.62	-1.00	-0.43
Luxembourg	-7.28	-3.55	0.91
Malta	-1.46	-0.78	0.10
Netherlands	-55.98	-28.56	-0.38
Poland	-17.41	-9.92	-2.43
Portugal	-7.99	-4.21	-0.62
Romania	-7.06	-3.92	-1.49
Slovakia	-3.36	-1.69	-0.29
Slovenia	-2.28	-1.07	-0.07
Spain	-42.07	-21.76	-3.98
Sweden	-26.04	-13.89	-0.73

TABLE 12: TOTAL ANNUAL LOSSES IN REAL GDP, IN %, MEDIUM-TERM HORIZON (5Y)

Forgone growth in %	Scenario 1 Broad critical sector coverage Medium-term	Scenario 2 Medium critical sector coverage Medium-term	Scenario 3 Narrow critical sector coverage Medium-term
EU27	-3.6%	-3.5%	-3.4%
Austria	-3.4%	-3.3%	-3.2%
Belgium	-4.0%	-3.8%	-3.7%
Bulgaria	-3.3%	-3.2%	-3.2%
Croatia	-3.3%	-3.3%	-3.2%
Cyprus	-6.5%	-5.3%	-4.1%
Czechia	-3.4%	-3.3%	-3.2%
Denmark	-4.1%	-3.9%	-3.7%
Estonia	-3.6%	-3.5%	-3.3%
Finland	-3.5%	-3.4%	-3.3%
France	-3.7%	-3.6%	-3.5%
Germany	-3.6%	-3.5%	-3.3%
Greece	-3.6%	-3.5%	-3.5%
Hungary	-3.5%	-3.4%	-3.3%
Ireland	-4.1%	-3.8%	-3.5%
Italy	-3.4%	-3.4%	-3.3%
Latvia	-3.8%	-3.7%	-3.6%
Lithuania	-3.5%	-3.4%	-3.3%
Luxembourg	-4.8%	-4.3%	-3.8%
Malta	-5.0%	-4.3%	-3.7%
Netherlands	-4.3%	-4.0%	-3.7%
Poland	-3.3%	-3.2%	-3.2%
Portugal	-3.5%	-3.4%	-3.3%
Romania	-3.3%	-3.2%	-3.2%
Slovakia	-3.2%	-3.1%	-3.1%
Slovenia	-3.7%	-3.6%	-3.5%
Spain	-3.6%	-3.5%	-3.4%
Sweden	-3.8%	-3.7%	-3.5%

TABLE 13: TOTAL ANNUAL LOSSES IN REAL GDP, IN EUR BILLION, MEDIUM-TERM HORIZON (5Y)

Total forgone growth, in EUR billion	Scenario 1 Broad critical sector coverage Medium-term	Scenario 2 Medium critical sector coverage Medium-term	Scenario 3 Narrow critical sector coverage Medium-term
EU27	-571.98	-554.55	-537.12
Austria	-15.02	-14.75	-14.48
Belgium	-21.76	-21.04	-20.33
Bulgaria	-2.81	-2.73	-2.66
Croatia	-2.23	-2.19	-2.15
Cyprus	-1.75	-1.42	-1.11
Czechia	-9.34	-9.09	-8.87
Denmark	-15.68	-14.84	-14.08
Estonia	-1.30	-1.25	-1.20
Finland	-9.51	-9.21	-8.95
France	-97.65	-95.01	-92.37
Germany	-138.40	-133.75	-129.10
Greece	-7.49	-7.36	-7.26
Hungary	-5.98	-5.79	-5.60
Ireland	-20.71	-19.24	-17.82
Italy	-65.10	-63.96	-63.00
Latvia	-1.47	-1.44	-1.40
Lithuania	-2.33	-2.28	-2.22
Luxembourg	-3.77	-3.34	-2.94
Malta	-0.86	-0.74	-0.64
Netherlands	-40.83	-37.96	-35.27
Poland	-21.48	-21.15	-20.76
Portugal	-8.25	-8.09	-7.92
Romania	-9.43	-9.21	-9.01
Slovakia	-3.49	-3.43	-3.39
Slovenia	-2.10	-2.04	-1.98
Spain	-47.11	-46.18	-45.39
Sweden	-21.60	-20.64	-19.69

DISCLAIMER

This ECIPE Occasional Paper is an independent report funded by the Computer and 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.