June 2023

EUCS AND EU TRADE OBLIGATIONS - A CLEAR CONFLICT

The EU's draft cloud computing certification scheme (EUCS) is inconsistent with Europe's trade obligations and risks harming transatlantic relations, at a time when collaboration on technology policy is more important than ever.

The EU's efforts to shield its cloud computing market from foreign (primarily U.S.) competition through the use of a proposed certification scheme, designed to apply to government procurement (and possibly other services deemed "critical infrastructure" or otherwise supplied by private companies)[1], will significantly set back efforts to strengthen trust between two of the world's largest economies. While directed at well-known large U.S. companies, it will have a similarly restrictive effect on the myriad U.S. and European companies, large and small, supplying computing infrastructure and software services to government and critical infrastructure customers.

The U.S. market has no equivalent restrictions based on the nationality of a company in the cloud computing sector[2]. A recurring theme among proponents of excluding US cloud providers from the European market or forcing them to enter into joint ventures with local partners, is a desire to create a scheme that parallels the U.S. federal government's cloud security scheme, known as the Federal Risk Authorization Management Program, or FedRAMP[3]. FedRAMP is a mandatory certification for all cloud-based services that handle U.S. government information. Like EUCS, FedRAMP has multiple tiers of assurance (Low-Moderate-High) corresponding to increasingly rigorous sets of technical security controls and processes.

But unlike the proposed EUCS, which contains an EL4 tier that excludes non-EU cloud providers from certification, FedRAMP does not discriminate based on country of origin. Any European CSP can apply to be FedRAMP-certified, even at FedRAMP High, so long as they are capable of meeting agency-specific personnel criteria (e.g., US citizen working in a US-based office). EU companies have been certified, and successfully bid, on cloud computing contracts with the U.S. government at the FedRamp High level.

Because of the persistent surplus the EU enjoys in accessing the U.S. government procurement market[4], this scheme, if finalized, will likely invite calls for reciprocal measures in the United States, and inspire similarly restrictive policies in third markets, where EU companies have trade interests.

The following outlines 5 key reasons this scheme is inconsistent with EU trade obligations.

---

[1] See, for instance, the statement of Bruno Le Maire, French Minister of Economy (September 2022): "*[I]f our companies, which have extraordinarily sensitive data, choose not to take advantage of this [SecNumCloud] 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*", https://presse.economie.gouv.fr/download?id=99457&pn=116%20-Discours%20de%20Bruno%20Le%20Maire%20sur%20la%20strat%C3%A9gie%20nationale%20pour%20le%20Cloud.pdf

[2] Some defense contracts relating to national security require the use of a U.S.-based subsidiary, but full ownership by a foreign-based parent is typically permitted.

[3] See https://www.fedramp.gov

[4] See https://www.gao.gov/products/gao-19-414

1. The EU has broad commitments covering Cloud Computing under both the GPA and the GATS.

In both the Government Procurement Agreement (GPA)[5] and the General Agreement on Trade in Services (GATS)[6] the EU has broad commitments covering cloud computing, by undertaking national treatment and market access obligations with respect to "Computer and Related Services", identified under the Central Products Classification Code (CPC) Section 84. There is broad consensus that this category of services covers cloud computing, as evidenced by the EU-championed Understanding on the Scope and Coverage of CPC 84.[7] Based on these EU commitments, foreign cloud computing companies are entitled to access the EU market on terms no less favorable than those available to EU companies. If the current draft of EUCS is finalized unchanged, a significant number of procurements (deemed "high") by foreign suppliers will be excluded, creating a clear conflict with trade obligations.

In its GPA Schedule, the EU has undertaken obligations for computer services with respect to over 1,000 specific government entities, including the Commission itself and a broad range of entities in every Member State. While entity coverage varies country-by-country, most EU Member states cover almost every major governmental ministry and agency.

To the extent that EUCS requirements are extended to non-governmental users of cloud computing services, GATS obligations would apply to all such contracts. Accordingly, an EUCS requirement precluding U.S. firms from bidding on private sector contracts would also implicate the EU commitments under the GATS. While EUCS is described as a voluntary certification scheme, if sector-level regulators (e.g., a telecommunications, health, or financial regulatory body) incorporated this standard into its regulations, adherence would become mandatory, directly implicating GATS obligations.

2. GPA and GATS commitments both explicitly preclude discrimination on the basis of nationality.

As stated in Article IV. 2 (Non Discrimination) of the GPA:

> *With respect to any measure regarding covered procurement, a Party, including its procuring entities, shall not: (a) treat a locally established supplier less favourably than another locally established supplier on the basis of the degree of foreign affiliation or ownership[.]*[8]

Similarly, in the EU's GATS schedule, where the EU could have inscribed a foreign ownership or other nationality-based limitations with respect to computer service suppliers, its description of

---

[5] https://e-gpa.wto.org/en/Annex/Details?Agreement=GPA113&Party=EuropeanUnion&AnnexNo=5&ContentCulture=en
[6] https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=Q:/SCHD/GATS-SC/SC31.pdf&Open=True
[7] See https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=81272,77348,56640,10521,78671&CurrentCatalogueIdIndex=4&FullTextHash=371857150&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True
[8] See https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=Q:/SCHD/GATS-SC/SC31.pdf&Open=True

applicable limitations (*i.e.,* under both Market Access and National Treatment columns) states "none."[9]

For the GPA, the EU's obligations only extend to the other 15 parties to this agreement,[10] including the United States. Conversely, the EU is free to discriminate against suppliers originating from non-GPA member countries (including China).

With respect to the GATS, however, which disciplines measures affecting commercially-supplied services outside government procurement (*e.g.,* if the EU or a Member State sought to restrict the supply of computer services to an EU-based private telecommunications, finance, transport, or health care provider, for instance), the EU's obligations extend to suppliers from every WTO Member (*i.e.* 136 non-EU Members).

3. The explicit intent of EUCS is to reserve certain contracts for EU companies.

The draft EUCS (as of May 2023)[11] and its progenitor (France's SecNumCloud certification scheme, which is already in effect) creates a framework for discrimination against non-EU cloud computing suppliers, by reserving a vaguely-defined scope of contracts to majority EU-owned, controlled, and headquartered companies. For such contracts, a foreign supplier's only option is to enter into a minority joint venture or a technology licensing agreement, similar to what China requires (to access the Chinese cloud computing market generally).

EUCS is often described as a voluntary certification scheme, but once included as a tender requirement in specific procurements (as France has started to do for SecNumCloud, from at least 2022[12]) it becomes a mandatory obligation–and this is now general policy, at least in France[13]. Further, recent EU legislation[14] explicitly permits the European Commission and Member States to mandate this certification scheme to a wide range of public and private entities at any point in time.

The specific restrictions that EUCS applies to this range of "high risk" contracts (categorized as "CS-EL4") are unambiguous.

Per the current draft, control requirements for CS-EL4 contracts are:

> *The CSP's registered head office and global headquarters shall be established in a Member State of the EU.*

---

[9] See pp 31-33 of the EU GATS schedule, op. cit.

[10] Parties to the GPA apart from the EU and its Member States are: Armenia, Canada, United Kingdom, Hong Kong China, Iceland, Israel, Japan, the Republic of Korea, Liechtenstein, the Netherlands with respect to Aruba, Norway, Singapore, Switzerland, Taiwan (Chinese Taipei), and the United States.

[11] https://subscriber.politicopro.com/f/?id=00000188-06ec-deac-a39a-4fecbb520000

[12] See, for example, this August 2022 tender: https://ted.europa.eu/udl?uri=TED:NOTICE:423823-2022:TEXT:EN:HTML

[13] See Circulaire n° 6282-SG (5 July 2021: https://www.legifrance.gouv.fr/circulaire/id/45205) and Circulaire 6404-SG (31 May 2023: https://www.legifrance.gouv.fr/circulaire/id/45446?origin=list)

[14] See for instance, Article 24(1) and (2) of Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation, and Article 56(3) of Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification

> *Undertakings whose registered head office or headquarters are not established in a Member State of 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.*

The text further clarifies:

> *Control shall be constituted by rights, contracts or any other means which, either separately or in combination and having regard to the considerations of fact or law involved, confer the possibility of exercising decisive influence on an undertaking, in particular by:*
> *(a) ownership or the right to use all or part of the assets of an undertaking;*
> *(b) rights or contracts which confer decisive influence on the composition, voting or decisions of the organs of an undertaking.*[15]

4. The scope of high risk contracts is exceedingly broad and vague, significantly exacerbating its potential discriminatory effect.

The high-risk category CS-EL4 is a subset of general requirement (Annex J) intended to "Plan the provision of a resilient cloud service while minimizing the risk of dependence over third country legislation."[16] The specific risk identified relates to:

> *[Ri]sks related to non-EU laws with extra-territorial application that relate to the processing of customer data and cloud service derived data that does not have the prior consent of the owner of the data, or is missing the prior consent of the legal persons mentioned in the data, and including at least: commercially sensitive and confidential information, and trade secrets.*

Since a significant portion of data processed by any agency will likely include confidential and/or commercially sensitive information, it is unclear what contracts relating to foreign suppliers would not be subject to the requirements flowing from this risk factor.

A consent obligation with respect to data processed on behalf of a governmental agency would be impossible to implement, since an agency would have to retroactively obtain such consent from the data subject or data owner (e.g., individual or company whose data an agency might hold) before contracting with a foreign cloud computing supplier. This infeasible task (which would not apply with respect to EU companies) would almost certainly preclude U.S. cloud services from being awarded a contract.

A more specific definition of the risks CS-EL4 targets is provided in a description of risk categories, where it is noted that the high risk category intends to:

---

[15] See p. 305, Section J.2.4.2 at https://subscriber.politicopro.com/f/?id=00000188-06ec-deac-a39a-4fecbb5200PM00
[16] See p. 300.

> *"[M]inimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources", but it only targets the most sensitive cloud services, and more specifically those that process data, whether personal or not, of particular sensitivity, and the breach of which is likely to result in a breach of public order, public safety, human life or health, or the protection of intellectual property.*[17]

Although this description of risk is not in itself problematic (and tracks risk categories used by many countries, including the United States), a focus on cyberattacks, whether by state or non-state actors, would appear to have little relevance to the ownership of the cloud computing provider. This also makes the CS-EL4 focus on foreign legal regimes particularly difficult to comprehend, since cyberattacks generally are typically unlawful actions, performed either by criminals or state actors acting outside legal constraints. In short, it is not obvious how an ownership restriction would be a rational means to mitigating the identified risk.

The specific types of breaches that CS-EL4 seeks to mitigate, at least in relation to foreign ownership, are equally difficult to understand—data breaches "likely to result in a breach of public order, public safety, human life or health, or the protection of intellectual property."

While these effects mirror exceptions in the GPA and the GATS, and could, in a cases-by-case context be used to justify derogating from obligations, they have no obvious relation to cloud computing and are singularly unhelpful in providing a certification scheme guiding governments on what might constitute a legitimate basis for restricting procurements on the basis of nationality, particularly among the small club of GPA members.

The notion that members of the GPA (mainly OECD countries) would seek to leverage the contract of a supplier from their jurisdiction that is supplying an EU entity cloud services, and use that data processing function to threaten public order, public safety, human life or health; or to misappropriate intellectual property from that entity, is hard to fathom.

As noted above, if these restrictions were extended to the private sector generally (e.g., the telecommunications, health service, financial, or transport market), the measure would implicate the trade rights of the broader WTO membership. Needless to say, the risks related to countries, and their suppliers, from this broader grouping is heightened, but a blanket requirement affecting all foreign countries would be clearly disproportionate. To address a more reasonable risk profile, EUCS could better distinguish rule-of-law countries from those where coercive pressure on suppliers is a demonstrated practice.

[17] See p. 26.

5. The EUCS bases for exclusion would be tantamount to treating U.S. suppliers equivalently to suppliers from non-rule-of-law countries like Russia or China.

The EU is one of the few WTO members to have invoked the public order exception to justify trade-related restrictions. The context to what became a formal dispute is telling and makes clear the relatively absurdity to extend like concerns to U.S. firms. That case[18] related to the terms on which Russian natural gas suppliers were able to sell gas to European businesses, where the EU argued restrictions on Russian control of such supply were "necessary to maintain public order".[19]

Given recent Russian actions, this concern appears prescient and, indeed, justified—based fundamentally on the divergent geopolitical interests of the parties, and Russia's willingness to flout international law. In contrast, the U.S. and the EU have forged ahead with a strengthened transatlantic alliance to counter authoritarianism and global security threats in recent years. For U.S. suppliers of cloud computing services to be compared to state-owned Russian gas suppliers, in their ability to harm fundamental EU social and economic interests beggars the imagination.

Similarly, a position that foreign government influence over a cloud computing company would threaten EU citizens' health or safety, or pose a threat to the EU's protection of intellectual property, could only be credible with respect to a geopolitical adversary flouting the rule of law,[20] and certainly cannot be reconciled with membership in an alliance like NATO whose core tenet is mutual defense.

It is one thing to cite an exception (or, in the case of SecNumCloud, or EUCS, attempt to integrate it into the requirement.) But under both the GPA and the GATS, simply articulating a rationale is not sufficient to justify a restriction: a complaining party can challenge a restriction as being applied in an arbitrary manner, or as not being demonstrably necessary to achieve the cited goal. One can conceive of a broad range of reasonably available alternatives to a nationality-based restriction to achieve the EU's goal of minimizing the risk of foreign government interference through a cloud computing company. If EUCS in its current form is adopted, the EU would be at clear risk of implementing a measure that could not meet this basic threshold of showing that its proposed restrictions are not arbitrary and are, in fact, necessary.

[18] See DS476, available here: https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds476_e.htm

[19] Specifically, the EU argued disruptions to the supply of gas may "prevent the heating of households and public spaces" and as a result "disrupt the provision of essential social services, such as healthcare, childcare, education and other welfare activities as well as many other basic public services, such as transportation, police or the administration of justice" which, in turn, "may endanger the health, life, security and, more generally, the well-being of the European citizens, in particular in the event of prolonged disruptions during the winter months." Para 7.1197 of DS476, op. cit.

[20] While this is a real risk with respect to geopolitical adversaries that flout international law, they are not among GPA signatories. Russia and China are not GPA signatories.