# "SOVEREIGNTY REQUIREMENTS" IN FRANCE—AND POTENTIALLY EU—CYBERSECURITY REGULATIONS: THE LATEST BARRIER TO DATA FLOWS, DIGITAL TRADE, AND DIGITAL COOPERATION AMONG LIKEMINDED PARTNERS

POSTED ON DECEMBER 10, 2021

NIGEL CORY (HTTPS://WWW.CROSSBORDERDATAFORUM.ORG/AUTHOR/NCOREY/)

France's national cybersecurity agency (known as ANSSI (https://www.ssi.gouv.fr/en/)) is revising its cybersecurity certification and labeling program (known as SecNumCloud) to disadvantage—and effectively preclude—foreign cloud firms from providing services to government agencies as well as 600-plus firms that operate "vital" and "essential" services. If put into place without changes, it would essentially make it impossible for foreign cloud firms, or firms using services from foreign cloud firms, to be considered "trusted." The regulation includes severe, China-like restrictions that force foreign firms to store data locally and only use local support and technical staff, which makes it impossible for them to leverage system-wide security and functional services. It also imposes strict limits on foreign ownership and representation on a company's board of directors. Similar to China, it would effectively only allow local firms to attempt for certification, and thus force foreign firms to set up a local joint venture to try to be certified as "trusted." This post analyzes the problematic provisions in the proposed update to SecNumCloud.

ANSSI first launched SecNumCloud in 2016 as a label to show public agencies and firms in critical sectors which cloud services are "trusted." It is based off ISO 27001, a globally recognized information security standard, and thus, its goal is genuinely good cybersecurity practices, like physical access controls, strong authentication protocols, encryption, and the use of hardware security modules.

However, baked into the latest update to SecNumCloud (French/ (https://www.ssi.gouv.fr/uploads/2021/10/anssi-referentiel_exigences-secnumcloud-v3.2.a.pdf)unofficial English translation (https://www2.itif.org/2021-secnumcloud-3.2.a-english-version.pdf)) is explicit protectionism against non-French cloud services providers. The window for submitting comments on the proposed revision just closed and it could go into effect as early as January 2022. These new explicitly protectionist provisions are in addition to its current use as a de facto discriminatory barrier as France has not certified firms from other EU member states and from outside the EU. Thus, it appear to breach the European Union's (EU) trade commitments. Since 2016, only four companies, all French, have been certified (3DS Outscale (https://en.outscale.com/certificates/secnumcloud-anssi-security-visa-granted-to-3ds-outscale/) (a subsidiary of Dassault Systems), OVHcloud (https://www.ovhcloud.com/en/enterprise/certification-conformity/secnumcloud/), Oodrive (https://www.oodrive.com/blog/security/cybersecurity-600-sensitive-infrastructure-operators-facing-specific-obligations/), and Worldline Cloud services

(https://fr.worldline.com/fr/home/newsroom/press-releases-general/2021/pr-2021_11_18_01.html)). Its discriminatory use is problematic given the policy's broad impact. It is mandatory for public agencies to use SecNumCloud certified services. ANSSI is also pushing for its use by hundreds of health, energy, finance, transport, and other firms that are deemed Operators of Vital Importance (OVIs) and Operators of Essential Services (OESs).

French policymakers justify SecNumCloud's protectionist restrictions on the fear of U.S. CLOUD Act's potential extraterritorial reach (https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/) (although this issue is not explicitly mentioned anywhere in the proposal). As otherwise, SecNumCloud's protectionist restrictions have no legal basis in European privacy or cybersecurity law, in that, the EU's General Data Protection Regulation has its various requirements, but this proposal's explicit data localization, local staff requirements, and ownership and board caps aren't reflected elsewhere. The protectionist measures do not contribute to the privacy or security of the data, and in fact, undermine cybersecurity best practices.

In moving ahead with these restrictions, France shows it is willing to disregard cooperation and constructive alternatives to address concerns over government access to data, including the use of technical measures and ongoing bilateral and G7 discussions and negotiations over law enforcement (https://academic.oup.com/idpl/article/11/2/81/6133744?login=true) and government access to data (https://www.g7uk.org/uk-g7-presidency-statement-digital-and-tech/). Given this, it's hard not to see it as simply another attempt to use regulatory protectionism to target U.S. cloud firms and. Targeting U.S. firms is the clearest part of France (https://www.ft.com/content/9edea4f5-5f34-4e17-89cd-f9b9ba698103) and Germany's (https://www.ft.com/content/956ccaa6-0537-11ea-9afa-d9e2401fa7ca) vision of European tech and digital sovereignty. Most worryingly, France is advocating for these SecNumCloud "sovereignty requirements" in a Europe-wide cloud cybersecurity framework. It raises a new point of conflict just as the United States and Europe try to repair the transatlantic digital relationship via the Trade and Technology Council (https://itif.org/publications/2021/12/02/how-eu-us-trade-and-technology-council-can-navigate-conflict-and-find) (TTC) and negotiate a successor to Privacy Shield. In the broader debate about global data governance and Japan's "data free flow with trust" initiative, the French proposal effectively means no data flows, nor trust.

**Foreign Ownership and Management Restrictions: France Takes a Page Out of China's Cyber Sovereignty Playbook**

The SecNumCloud's most clearly discriminatory provision is its requirement (article 19.6) that cloud service providers be "immune to non-EU laws," established via corporate ownership structure limitations. Specifically, the law specifies that individual shareholders outside the European Union (EU) can't possess more than 25 percent of the company, and collectively 39 percent of the value and voting rights of the company. They also can't have veto rights, nor can they nominate a majority of members of boards. Together, all of these requirements essentially preclude majority foreign owned and run cloud firms from SecNumCloud certification.

These foreign ownership and management restrictions are similar to those used by China to strictly control its domestic cloud services (https://itif.org/publications/2021/04/15/testimony-us-china-economic-and-security-review-commission-regarding-chinas) market via discriminatory licensing requirements and by forcing foreign firms to partner with a local firm as part of a joint venture. In some ways, France has been even more restrictive given it hasn't designated any foreign firm as "trusted," whereas at least China has allowed a small number of foreign firms (like AWS, Microsoft, and SAP) to set up a local joint venture. Either way, the effect will likely be the same in effectively excluding foreign providers from a large part of the domestic cloud services market without making a positive impact on the actual security or privacy of data.

**Forced Local Data Storage and Local Staff Requirements**

France's proposal creates local physical requirements that undermine the distributed nature of the Internet and modern cloud services. It includes several data localization provisions: cloud providers must store and process all customer data within the EU; the administration and supervision of the service must be carried out from within the EU; and the service provider must store and process technical data (identities of beneficiaries and administrators of technical infrastructure, data handled by the Software Defined Network, technical infrastructure logs, directory, certificates, access configuration, etc.) within the EU. This would prevent French and EU-based companies from leveraging security expertise of U.S. and other foreign cloud service providers.

French policymakers who genuinely think that the geography of data storage (mainly, local data storage) solves privacy and cybersecurity concerns misunderstand the issue. To the extent nations have laws and regulations governing the treatment of data, a company operating in the country is subject to those laws regardless of where the data is stored and regardless of the nationality of ownership of the company. Having complete and direct ownership and control of the information technology (IT) systems "stack," from the building floor and walls to the software on the servers, may make people feel that their data is as secure as possible. But this represents a false sense of security. Most cybersecurity vulnerabilities are exploited remotely, so the physical location of data has little to no impact on cyber threats (as demonstrated by the hack of the U.S. Office of Budget and Management). Furthermore, inadvertent disclosures of data are the result of security failures, often exploited by the activities of foreign hackers.

Data localization actually undermines good cybersecurity. It prevents the sharing of data to identify IT systems vulnerabilities and to help firms detect and respond to cyber attackers. It precludes cloud service providers from using cybersecurity best practices, such as through "sharding," where data is spread over multiple data centers. Firms also need to share data to reconcile if cyberattacks (such as those from China, Russia, or elsewhere) are new or known. Sharing system vulnerability information also allows cybersecurity providers to identify vulnerabilities.

The proposal also changes common business practices whereby firms—whether they are manufacturers, banks, or in other service sectors—have a local subsidiary (and thus legal nexus) for market and regulatory compliance purposes, but can use foreign facilities and staff to support local operations. The proposal creates a difficult, if not impossible, requirement for cloud providers to set up duplicative technical staffing operations in the EU as it allows only local personnel to conduct key tasks. The proposal forces firms to only allow people located in the EU to conduct the technical support necessary to diagnose and resolve problems that users face in accessing their data and in conducting remote (general) maintenance. In both cases, firms must "check that the person to whom access must be authorized is located within the European Union."

These requirements fundamentally undermine the distributed nature of cloud services and the "follow the sun" model of customer and technical support, where global firms staff three shifts in Asia, the Americas, and Europe to provide continuous support. It would require significant, and unnecessary, duplication of staffing and operations in the EU. It would extend well beyond key engineers to the many support staff involved in identifying, fixing, testing, and deploying service upgrades to address cybersecurity issues. For cloud service providers, having all relevant regulatory compliance and service support expertise in each and every market isn't viable. Obviously, many firms set up country and regional support teams, such as to ensure compliance with the EU's General Data Protection Regulation or U.S. financial regulators, but they all report to, and benefit from, seamless engagement with central support teams based in their home country. For example, if an EU customer identifies an issue with a firm's service, the firm may well need an engineer or customer service representative based in the United States, India, or elsewhere to resolve it.

It is unreasonable to expect tech firms to not only set up local data center infrastructure but also duplicative full-service engineering and customer support operations in each market, so the right person to fix an issue is based locally (and data doesn't need to be transferred as part of a fix). Ultimately, French customers would face the choice of having service only during limited hours, or paying a hefty premium for service to be provided through night shifts and overtime.

**Administrative Overload: Paperwork For the Cloud**

The proposal creates an onerous general monitoring and reporting requirement for cloud firms. As part of its risk assessment requirements, the proposal requires firms to take into account "the risks of breach of the confidentiality of commissioning entity data by third parties involved in the provision of the service (suppliers, subcontractors, etc.)." Service providers "must list, in a specific document, the residual risks associated with the existence of extraterritorial laws aimed at collecting data or metadata from commissioning partners without their prior consent" and must "make available to the commissioning entity, at the latter's request, the elements for assessing the risks linked to the submission of the data of the commissioning entity to the law of a non-member state of the European Union."

This is similar to the European Data Protection Board's (EDPB) post-Schrems II reporting and monitoring requirements that required firms to review the laws and practices of each country data is transferred to in determining whether these raise a risk to data. The EDPB eventually decided (https://iapp.org/news/a/edpbs-data-transfer-recommendations-adopt-a-risk-based-approach-with-teeth/) to allow firms to use a primarily risk-based approach to assessments, allowing certain data transfers to proceed, even where the text of the laws of the importing country do not strictly satisfy EU requirements, so long as certain conditions are met (such as the use of encryption).

This is problematic for several reasons. Operationally, it'd be difficult for cloud firms as they do not have unfettered access to the data the customers store in their cloud, such that they don't know what type of data it is and what the specific risks may be. For any associated data that is stored overseas, it'd be hard for them to know exactly which countries it transits or is stored in and the associated risks. It would cover national security laws that are often broad and vague and thus hard to monitor and report upon (this would presumably include France's own intelligence operations). Similar to issues with the EDPB's guidance, it requires firms to have a detailed and nuanced understanding of both the law and practice of local surveillance and government access laws, which is not straightforward given the lack of transparency (as many operate in secrecy).

But the impact and reporting requirement would be much broader than just surveillance. Data and metadata collection is a common, legal requirement in France and other EU member states, as well as countries elsewhere around the world, as part of competition, anti-money laundering and fraud, and criminal investigations. It would represent a massive effort for firms to keep an updated list of all such requirements around the world. Never mind that it would also require ANSSI to have its own comprehensive list to use as a reference list to cross-check, and that ANSSI's database itself may become a target of interest to hackers scoping out possible entry points.

**Trade Law Be Damned: SecNumCloud Breaches Core EU Trade Commitments**

The EU's international trade commitments include the principles of non-discrimination and national treatment in terms of the nationality of persons, products, services, or technologies. These are foundational trade law principles that are part of the EU-United Kingdom Trade and Cooperation Agreement, the WTO Government Procurement Agreement, and pretty much every other major trade agreement.

For example, the SecNumCloud update appears to be a clear violation of the WTO Government Procurement Agreement's (https://www.wto.org/english/docs_e/legal_e/rev-gpr-94_01_e.pdf) national treatment provision (Article III):

2. With respect to all laws, regulations, procedures and practices regarding government procurement covered by this Agreement, each Party shall ensure:

(a) that its entities shall not treat a locally-established supplier less favourably than another locally-established supplier on the basis of degree of foreign affiliation or ownership;

(b) that its entities shall not discriminate against locally-established suppliers on the basis of the country of production of the good or service being supplied, provided that the country of production is a Party to the Agreement in accordance with the provisions of Article IV.

A central question is whether France (and the EU) would try and defend these sovereignty requirements via trade law exceptions for national security, privacy, and other public policy interests. There are trade law guardrails to prevent countries from misusing these exceptions to enact disguised barriers to trade, but there is considerable uncertainty as there are very few (https://www.csis.org/analysis/wtos-first-ruling-national-security-what-does-it-mean-united-states) national security-related disputes to provide legal precedents to apply to this potential case.

**Conclusion**

There has been no clear reaction from the Biden administration to this new barrier to transatlantic digital trade and cooperation. The Biden administration and other EU trading partners should push back strenuously given that the policy is clearly discriminatory and holds Europe-wide market access implications. France is advocating that the European Union Agency for Cybersecurity (ENISA) include "sovereignty requirements" identical to SecNumCloud in its work to develop an EU Cloud Security Scheme (EUCS), which aims to standardize the proliferation of cloud security schemes and procurement standards across Europe. EUCS could be adopted by the EU parliament in 2022. Such EU-wide regulations would make it mandatory for many firms and government agencies to only use EUCS certified services to which only very few service providers would be able to qualify. This would thus be hugely problematic for foreign providers if it mirrored SecNumCloud. As president of the Council of the EU in the first half of 2022, France will be able to push (https://www.politico.eu/article/macron-seeks-electoral-boost-from-french-sway-over-eu-trade/) its preferred approach on EU trade and digital policy.

Not that it should be surprising given France's track record of targeting U.S. tech firms, but it obviously goes against the recently rekindled spirit of cooperation at the EU-U.S. TTC and undermines ongoing efforts to address concerns about law enforcement and government access to data. It's ironic in that French outrage over its perceived mistreatment by Australia, the United Kingdom, and the United States nearly derailed the recent TTC meeting (given Australia's decision to switch from French to British/American firms to build its submarines). If only the United States reacted with one-tenth of the outrage that the French government exhibited in reaction to this, France might realize that it can't have it both ways and should treat U.S. tech firms how it wants its own firms to be treated.

**Nigel Cory** (https://itif.org/person/nigel-cory) is an Associate Director covering trade policy at the **Information Technology and Innovation Foundation** (https://itif.org/).



# AUTHOR

NIGEL CORY (HTTPS://WWW.CROSSBORDERDATAFORUM.ORG/AUTHOR/NCOREY/)

VIEW ALL POSTS (HTTPS://WWW.CROSSBORDERDATAFORUM.ORG/AUTHOR/NCOREY/) (MAILTO:NCORY@ITIF.ORG)