COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

This translation is a working document. Only the French version is authentic.

OPINION N°2024-05 OF SEPTEMBER 4TH, 2024 ON POLITICAL AND ECONOMIC ISSUES OF THE EUROPEAN SAFETY CERTIFICATION SCHEME CLOUD SERVICES[1]

Members of the Commission supérieure du numérique et des postes (CSNP)[2] want to draw the attention of public authorities and members of Parliament on the political and economic consequences of the European Cybersecurity Certification Scheme for Cloud Services (EUCS) and make recommendations to strengthen the protection of sensitive personal or non-personal data of citizens, businesses and public administrations.

Indeed, while the Commission nationale de l'information et des libertés (CNIL)[3] has just expressed its opinion on the shortcomings and risks of the EUCS[1] and as the new European Commission is set up, it is crucial that these sovereignty issues are taken into consideration at the highest level.

It is also important to remember that digital security is based on three principles:

- integrity of information systems, data and associated processing;

- availability of information systems and data;

- confidentiality of data and associated processing.

Data confidentiality and associated process involve avoiding two major but distinct types of threat:

- unlawful and illegitimate access of a criminal nature, whether by criminal organizations or state agencies;
- access by intelligence agencies that act in a legal but secret framework, and of course illegitimate for the organizations that are victims of such actions.

Many opponents of any form of protection against legal access to data held by cloud services operators, deliberately maintain a confusion on confidentiality between the cyber security issues against illegitimate and illegal access to sensitive and strategic European data and the

[1] This translation is a working document. Only the French version is authentic.
[2] High Committee on digital and postal sectors
[3] National Commission of Information and Freedoms

provisions for protection of sensitive and strategic data against such legal access. This type of provision is implemented by intelligence agencies for any kind of activity, in particular to carry out economic intelligence activities for the benefit of their companies and to the prejudice of the companies of economic competitors.

I. Genesis of the European Cloud Services Certification Scheme (EUCS)

Given the rapid expansion of cloud services and their increasing adoption by companies and public administrations, the European Union has decided to establish a regulatory framework to ensure the security and compliance of these services on the European market. This initiative led to the creation of the European Cloud Services Certification Scheme (EUCS). The objective of this scheme is to strengthen users' confidence in cloud services by ensuring a high level of security, data protection and compliance with European laws.

The EUCS project is part of the broader strategy of the European Union to build a resilient and secure digital market. The adoption of Regulation 2019/881, known as the Cybersecurity Act, laid the foundation for a common framework for cybersecurity certification. The European Union Agency for Cybersecurity (ENISA) has been mandated to develop and manage different certification schemes, of which EUCS is a central part. The EUCS aims to provide a consistent legal framework within the Union, not only to protect sensitive data, whether personal or not, but also to strengthen Europe’s digital sovereignty in the face of global competition.

II. The CJEU ruling invalidating the Privacy Shield and its implications

On 16 July 2020, the Court of Justice of the European Union (CJEU) issued a landmark ruling that invalidated the Privacy Shield, an agreement on the transfer of personal data between the European Union and the United States. This ruling has highlighted the practices of US intelligence agencies, which access personal data of European citizens through US cloud service providers. These data, when hosted by US providers, are subject to legislation, including section 702 of the Foreign Intelligence Surveillance Act (FISA), which allows the US to collect data, in a massive way,, and without a judicial mandate, without offering the guarantees of proportionality required by European Union law. Recital 184 of that judgment stresses that those laws do not comply with the minimum guarantees required by the European Union, since the surveillance programmes which result from them are not limited to what is strictly necessary.

By invalidating the Privacy Shield, the CJEU has mainly focused on the protection of personal data. However, section 702 of the FISA is not limited to personal data but applies to non-personal data as well, and allows access to any type of sensitive or strategic data. This exacerbates concerns about the security of European economic information.

The Data Privacy Framework (DPF), adopted in July 2023 to replace the Privacy Shield, covers the adequacy of transfers to the United States only for personal data. On the other hand, the protection of sensitive or strategic non-personal data in relation to the activities of intelligence agencies still faces a legal vacuum within the European Union.

This incomplete framework highlights the need for a clear distinction between the legitimate needs of the United States to fight terrorism and international crime, and the risks that may be generated by abusive economic intelligence activities against European companies for economic benefits. Moreover, a major risk remains in the difference of interpretation between the European Union and the United States regarding the principles of proportionality and necessity. These principles are crucial for the implementaton of the guarantees provided by the DPF (Data Privacy Framework), but their application depends largely on the legal and cultural context of each jurisdiction. In Europe, the protection of personal data is a fundamental right strictly defined, and any limitation of this right must be necessary, proportionate and rigorously justified.

European authorities, including the CJEU, interpret these principles in a context where individual rights prevail, even when faced with security issues. In the US, these same principles are interpreted in a context where national security is a major issue. The U.S. legal framework, including section 702 of the Foreign Intelligence Surveillance Act (FISA), allows for extensive surveillance of foreign individuals (individuals or corporations) for national security reasons, which may include mass data collection.

Despite the reforms introduced by the Presidential Decree 14086, adopted by President Biden to enable the implementation of the DPF, and which aim to strengthen the protection of the European personal data, the concept of “necessity” in the United States may include actions that European authorities might consider excessive. This divergence of interpretation could become a source of tension in the future.

If the European authorities consider that the principles of proportionality and necessity are not applied according to GDPR standards, they could challenge the validity of the Data Privacy Framework. Such a disagreement could lead to further invalidation of the agreement, as it was the case with the Privacy Shield. This risk highlights the challenges inherent in the harmonization of data protection standards between two fundamentally different legal systems.

III. The Gaia-X certification framework

In November 2021, the Gaia-X association adopted a certification framework for cloud services, offering three levels of certification. The highest level of this framework requires the immunity from non-European legislation with extraterritorial scope. This consensus among the European members of Gaia-X reflects a clear will, both of the recipients of certified cloud services and of the providers of these services, to protect the most sensitive data from legal but potentially abusive interference by foreign legislation.

IV. The SecNumCloud certification and the law « Secure and regulate the digital space »

The SecNumCloud certification, developed by ANSSI in 2016, is a security framework designed to qualify cloud service providers. It is based on the ISO/IEC 27001 standard and meets European requirements, in particular with regard to data protection, while guaranteeing a high level of technical, operational and legal security. Version 3.2 of the standard, published in 2022, strengthens protection against non-European laws, in accordance with the judgment “Schrems

II" of the Court of Justice of the European Union. It is also consistent with the requirements of the High+ level of the previous version of the EUCS.

This reference framework aims to create a secure cloud environment, encourage the development of national and european actors for cloud services in particular to meet the needs of the state, and ensure lasting trust between qualified providers and their users, in particular for public administrations that manage sensitive data. The SecNumCloud certification, embodied by the ANSSI Security Visa, is a guarantee of reliability and compliance with the highest security standards, thus offering enhanced protection against cyber attacks and legal risks.

Legal uncertainty remains, but it is highly probable that the adoption of EUCS, whether or not it incorporates the High+ level, would make the SecNumCloud certification obsolete. If the European Commission shoulf adopt the EUCS without incorporating requirements for immunity to non-European legislation with extraterritorial scope, it would replace all other national cloud service certification standards in Europe and consequently, France would be unable to implement its so-called "cloud at the centre" strategy.

Furthermore, in such a case, the implementation of Articles 31 and 32, related to the protection of strategic and sensitive data on the cloud computing market, of the law aimed at securing and regulating the digital space, known as the SREN law of 21 May 2024 will be difficult as these articles refer to the SecNumCloud certification.

V. The High+ level of the EUCS

The first version of the EUCS has integrated the highest level of certification, also called High+, technical and legal criteria for cloud services' immunity to non-European legislation with extraterritorial scope. While many states have this type of legal provision, the High+ level targets primarily the states where are registered the world's leading cloud service operators. China has, with its law of 28 June 2017 on national intelligence, a legislative provision that obliges Chinese cloud operators such as Alibaba, Tencent or Huawei, to make available to the Chinese authorities the data they may detain in their infrastructures without referring to their customers. The mechanism is quite similar to that in the US as the section 702 of the FISA, highlighted by the CJEU, and which of course is the responsibility of the main US cloud service operators, including the three leading operators who take over more than 70% of the cloud services market in Europe.

This High+ level was designed according to principles similar to those of the French SecNumCloud reference, to provide proportionate protection for European companies processing data in the cloud and risking illegitimate appropriation via non-European legal channels with extraterritorial scope. This protection, although not mandatory, is considered essential for these companies.

There is a need for cloud services immune from extraterritorial non-European legislation in the European digital ecosystem, particularly for public and private bodies. Without this system, it

will be extremely difficult to get out of the increasing dependence on US operators, which could in the long run carry unbearable risks of an economic, geopolitical and legal nature.

VI. American critics

This European initiative has faced some strong reactions in the US. On May 25, 2023, several US professional associations, including the Computer & Communications Industry Association (CCIA) and the Business Software Alliance (BSA), sent a letter to the Biden administration, denouncing the EUCS High+ as a threat to the national security of the United States. In this letter, they write: "*EUCS is part of a broader concerted effort by Europe to enact a "digital sovereignty" agenda that seeks to disadvantage U.S. firms for the benefit of local alternatives, potentially threatening U.S. economic and national security interests*." According to them, the EUCS is part of a European "digital sovereignty" approach aimed to disadvantage American companies and to compromise the economic and security interests of the United States.

In September 2023, Mr Antony Blinken, US Secretary of State, sent a diplomatic note to Mrs Ursula von der Leyen, President of the European Commission, warning that these provisions could damage bilateral relations between the United States and the European Union, both economically and in terms of security: « *Including these provisions in the final scheme could also negatively impact the U.S.-EU bilateral economic and security relationship.* »

VII. European reactions

In response, the European Commission asked ENISA to review the EUCS scheme, which led, early 2024, to a new proposal without a High+ certification or any provision guaranteeing immunity from non-European legislation such as section 702 of the FISA.

In April 2024, the U.S. Congress renewed section 702 of the FISA for two years, also expanding its scope.

On 30 October 2023, at a ministerial summit between Germany, France and Italy, devoted to industrial cooperation in several sectors strategic for the European Union, all three countries reaffirmed their intention to strengthen the protection of sensitive data in Europe, particularly against extraterritorial legislation. This desire for protection has, however, been questioned, notably by Germany, in the context of discussions on the EUCS.

For many European companies, the EUCS High+ certification level is crucial to protect their sensitive or strategic non-personal data against legal but unwanted access by intelligence services in a non-binding manner. These companies do not want to exclude US cloud service providers from the European market, but they claim that a substantial part of their needs cannot be met by these operators. They stress the need to have cloud services in Europe that can meet their requirements for protecting sensitive and strategic data, implemented in a uniform manner throughout the European Union, with robustness guaranteed by a legally binding European certification scheme.

In the European Union, opponents at the EUCS High+ level are broadly divided into two categories:

- the Member States of the European Union, which are sensitive to threats of restriction of security guarantees by the United States;
- the economic sectors strongly dependent on the US market and sensitive to threats of restricted access to this market in case of adoption of the High+ level in the EUCS.

VIII. Compliance of the High+ level with the World Trade Organization (WTO) agreements

A recurring criticism of the High+ level of the EUCS is its compliance with the WTO agreements, on the grounds that it would cause the eviction of US operators from the European market. In an article published on September 1, 2023 on the website of the Center for Strategic and International Studies (CSIS), a, Meredith Broadbent is attacking the EUCS High+ level, notably by asserting that the High+ level is incompatible with the WTO agreements.

This argument is not valid because it is not the reference in itself that could be incompatible with the provisions of the WTO agreements, but the use which will eventually be made by the member states, in public procurement, to ensure open, fair and transparent conditions of competition, by reserving the use of the High+ level for the derogations explicitly provided for in the Treaty.

The European Union has not ruled that SecNumCloud is not in compliance with WTO agreements. On the other hand, the Prime Minister's first circular on the implementation of the "cloud at the centre" strategy, published on 5 July 2021, was criticised by Brussels for not complying with WTO agreements. It was updated in May 2023, in particular to take into account the comments of the European Commission.

IX. Position of the Commission Nationale de l'Informatique et des Libertés (CNIL)

In the context created by doubts about the robustness of the DPF with regard to the protection of the most sensitive personal data, the Commission Nationale de l'Informatique et des Libertés (CNIL), in an opinion published on 19 July 2024, criticised the shortcomings of the current EUCS certification project, in particular with regard to the protection of sensitive personal data against unauthorised access by foreign authorities.

The CNIL has pointed out that the absence of "immunity" criteria against non-European legislation weakens the competitiveness of the European cloud offer and compromises the ability of public and private actors to outsource their most critical projects in a secure manner.

The Commission called for the reintroduction of provisions inspired by the SecNumCloud framework into EUCS, allowing European cloud providers to demonstrate their ability to protect data from foreign interference.

X. The conclusions and recommendations of the CSNP

The Higher Commission for Digital and Postal Services:

- considers that the adoption of the EUCS certification scheme, including provisions guaranteeing immunity from non-European legislation, is a key issue for the technological autonomy of the European Union, the condition for the emergence of a European cloud services industry, and an urgent need to protect sensitive and strategic data, personal or not, of the public and private bodies that need to preserve their information heritage against foreign interference;

- requests the Government to present to the members of the Parliament the updated situation of the negotiations and its position;

- invites the Government to request the European Commission to confirm the voluntary use of the different levels of EUCS certification by beneficiaries of certified cloud services;

- suggests that the Government ask the different EU Member States, opposite at the High+ level, to explain why they intend to deprive companies and public administrations which express the need for it in Europe or in their own country;

– Requests the Government to take the necessary steps with the European Commission to stop any any decision to adopt the current version of the certification scheme and to intiate a solid and thorough study of the needs of the different stakeholders, European professional organisations representing potential future public and private beneficiaries of the EUCS;

– calls on the Government to conduct a thorough analysis of the medium-term geopolitical consequences of the EU's waiving of maintaining a High+ level in the EUCS;

– calls on the government to conduct an economic analysis of the consequences of European dependencies on the US cloud services industry and its impact on the competitiveness of the European economy;

– requests the Government to present an analysis of the risks that the adoption of the High+ level in the EUCS would place on the European Union under its commitments under the WTO agreements.