French non-paper on EUCS addressed to the CLS.

Member States and the European Commission are currently in the process of discussing, in the ECCG technical expert group, the content of the future EU cybersecurity scheme (EUCS), which will be adopted through an implementing act to the Cybersecurity Act ((EU)2019/881, hereafter "CSA").

Without prejudice to the end of these negotiations, the EUCS scheme is likely to be composed of three assurance levels, namely 'basic', 'substantial', and 'high' level. **According to the CSA, it will not be mandatory, but Member States will be able to require the use of the scheme for certain entities, including public administrations and user companies, at national level.**

After three years of discussions regarding the inclusion or the non-inclusion of criteria aiming at preventing unauthorized access to data hosted or processed by cloud services through non-EU laws with extraterritorial reach, when this access may create a conflict with EU law, (so-called « immunity criteria » - previously Annex I of the scheme) at the highest level of certification, the European Commission has recently proposed a new version of the scheme, which would still contain the three levels of certification (basic, substantial, and high), but with no « immunity criteria ».

French authorities are thankful for the Commission's attempt to present a new compromise proposal and for its explanations on the legal reasoning behind this new proposal, **according to which Member States could still legally, at national level, maintain or adopt national schemes covering the same services (*i.e.* cloud services) but limited to "immunity criteria" and require, in duly justified situations, these « immunity criteria » on top of the criteria described in the highest level of the EUCS scheme as proposed.**

However, in order for all Member States to be fully informed, and in order to clarify the legal reasoning behind such a proposal, as well as to ensure legal certainty for Member States, French authorities kindly ask the Council' Legal Service to provide Member States with written, legal clarifications on the possible interaction between EU and national law in the context of the CSA and of the EUCS scheme that is currently being discussed:

Considering that the legal principle of full harmonisation seems to be applicable to the CSA, and in particular in view of its article 57;

Considering that Article 2(1) of the CSA defines cybersecurity as "*the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats*";

Considering that Article 2(8) of the CSA defines a cyberthreat as "*any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons*";

Considering that Article 46.2 provides that "*The European cybersecurity certification framework shall provide for a mechanism to establish European cybersecurity certification schemes and to attest that the*

ICT products, ICT services and ICT processes that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle";

Considering that Article 51 provides that "*A European cybersecurity certification scheme shall be designed to achieve, as applicable, at least the following security objectives:*

(a) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;" […]

(c) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer";

Considering that the Commission recently informed Member States in March 2024 that its legal service considers that the CSA does not cover the risks related to unauthorized access to data by authorities of non-EU Member States through extraterritorial legislation, and that therefore, Member States could lawfully introduce or maintain such additional criteria in their national law, as long as it is in line with EU law,

French authorities kindly ask the Council's Legal Service (hereafter "CLS") to provide Member States with its written, legal analysis regarding the situation at stake, in order to better understand the possible interactions between the future implementing Act (EUCS) and national law, and in particular with regard to the following questions:

1) Does CLS confirm that the CSA rests on the principle of full harmonisation with regard to cybersecurity certification schemes?

2) Does CLS consider that the CSA could be interpreted as excluding the risks, and thereby associated specifications within cybersecurity certification schemes, associated to unauthorized access to data stored or processed in the Union via extraterritorial laws by non-EU authorities or governments, in particular in light of Articles 1, 2 and 57?

3) Assuming that Member States would agree with the Commission's new proposal as provided for in the latest version of the scheme (V1.0.413 of March 2024), what is CLS's analysis on the following situations:

   - **Could Member States maintain or adopt national, voluntary certification schemes** limited to national "immunity criteria" (as specified below), in order to allow private Cloud providers to guarantee - by a national certification cybersecurity authority having the power to check and control – their high level of protection offered by their services against access by non-EU authorities through the use of extraterritorial legislation (*i.e.* against risk of conflict of laws)?

"Immunity criteria" may include, for instance:

- The obligation to store and process data in the Union, and/or

- The absence of control/share capital/voting rights/veto rights of the Cloud Service provider (to be defined by national law) by non-EU entities (*i.e.* entities whose registered head office or headquarters are not established in a EU Member State)

  - **Outside of national security use cases and in compliance with EU law and international commitments, could Member States require – for very specific cases - public and/or private entities to comply with EUCS level high** + national "immunity criteria" (as specified above) regarding **certain categories of sensitive data and information systems**, and if so, in what circumstances and under which conditions? (*e.g.* public procurements…).

French authorities thank CLS for its precious contribution to the EUCS discussions, and would be grateful for any legal input on the above-situation and questions, as well as any other relevant, legal comment they may deem appropriate in order to provide Member States with a full understanding of the legal issues at stake.