Non-paper by DE, ES, FR and IT
on the EUCS requirements for immunity to non-EU laws

This non paper addresses the issue of the immunity to non-EU law in the EUCS scheme of the EU cybersecurity certification framework (Cybersecurity Act (UE) 2019/881).

The proposals below are preliminary and they do need to be further analysed with respect to technical and legal soundness and completeness.

1. State of play

FR proposed a non-paper regarding EUCS and EU sovereignty which was discussed in an ad hoc ECCG meeting on the 26th of March. At the last ECCG meeting held on June the 28th, France proposed a way to integrate requirements to address immunity to non-EU laws in the EUCS scheme for the assurance level "High".

An action point was taken to deliver a new version of those requirements to be reviewed by ECCG members before the 15th of September. This is the purpose of this non-paper.

2. Position

In the current version of EUCS, the transparency requirements are not sufficient to face the concern of the lack of immunity to non-EU laws.

This risk has to be handled within the EUCS scheme. For this purpose, we propose some limited auditable requirements which can be easily added to the EUCS draft scheme at the assurance level "High".

These requirements refine the 4 criteria initially proposed by FR to ensure that:

- Only the EU law applies;
- Trusted employees are dedicated to the maintenance of the cloud service ;
- Maintenance, operations of the cloud service and process, and data are located within the EU;
- Technology exchanges between the cloud services and technology providers are controlled.

The proposed requirements are technology-agnostic. They constitute the minimum set of requirements to ensure the immunity of cloud services to extra EU laws from both a legal and technical standpoint.

This proposal is a draft to be considered as a preparatory work; once discussed with ECCG members, it will help ENISA integrate them in the draft EUCS scheme.

3. Draft proposal

Criteria 1: Only the EU law applies	
Proposed requirements for EUCS	• **The cloud service provider shall ensure that its operational and commercial offer is performed by an EU organisation, detained by EU actors**

optional sub requirements (to be added to the scheme or to an appendix)	• *Possibility to add some requirements on the establishment – within in the EU - of the cloud service provider* • *Possibility to add requirements on the shareholding of the cloud service provider (at least X% of EU shareholders) (Cf. Note of the European Commission – NOTE FOR THE ATTENTION OF THE STRATEGIC CONFIGURATION OF THE HORIZON EUROPE PROGRAMME COMMITTEE – 19/05/2021)* • *Possibility to add requirements on the licensing of non EU technologies*
Criteria 2: Trusted employees are dedicated to the maintenance of the cloud service	

Proposed requirements for EUCS	• ***C2.1: The service provider must document and implement a procedure compliant with EU laws and regulations in effect in order to ensure trustworthiness of its personnel. These verifications apply to any person involved in the supply of services and must be in line with the sensitivity and the confidentiality of the client data as well as to the risks identified by the cloud service provider.***
	• ***C2.2: During its technical support, if some actions require an access to the client data for the diagnostic or the resolution of an incident, the cloud service provider shall document and implement that:***
	  • ***The access to data can be given only after the explicit approval or consent of the client***
	  • ***The access to data by employees shall be done according to the requirement C2.1***
	  • ***If the personal does not fulfill the requirement C2.1, it shall be supervised by a personnel compliant to C2.1***
	  • ***All actions requiring an access to data shall be managed as administration actions and shall be logged in the same way***
	  • ***The access to data is removed at the end of the action***

optional sub requirements (to be added to the scheme or to an appendix)	• *Possibility to integrate different categories of employees depending on their access rights (e.g for the most sensitive population, requirements on the background check or screening)*
Criteria 3: Maintenance, operations of the cloud service and process data are located in the EU	
Proposed requirements for EUCS	• ***C3.1: The service provider must document and forward to the client the location of the storage and of the processing of all the data (client and technical data).*** • ***C3.2: The service provider must store and process the client data within the European Union at any time.*** • ***C3.3: The service provider shall store and process technical data (identity of users and administrators of the infrastructure, logs of the infrastructure, …) within the European Union.***

	• ***C3.4: The administration and supervision operations of the service must be carried out from the European Union.***
Criteria 4: Technology exchanges between the cloud services and technology providers are controlled	

Proposed requirements for EUCS	• ***C4.1: The cloud service provider shall have a procedure to control all inputs (updates, …) and outputs (logs, …) of the technical infrastructure of the cloud service, accordingly to the sensitivity and the confidentiality of the client data, to:***
	  ◦ ***Have the ability to suppress some targeted data during the transfer before any data transfer out of CSP's data center***
	  ◦ ***Have the ability to scan inputs to only allow legitimate requests (in case of doubt, the ability to block the exchange)***
	  ◦ ***All those actions will be logged as administration actions***
	• ***C4.2: Verification performed on inputs and outputs of the technical infrastructure shall be done on dedicated devices by the cloud service provider.***

optional sub requirements (to be added to the scheme or to an appendix)	• *Possibility to give some examples in guidance indicating the use of demilitarized zone (DMZ)* • *Possibility to give some examples of forecast architecture with the Bleu example*

4. Proposed questions to discuss the proposed requirements

The ECCG members are invited to provide their national perspective on the following elements:

- For each criteria, do the requirements allow to achieve the main goal of the criteria? If not, what requirements are needed?
- For each criteria, are the requirements well described? If not, what amendments are needed? To what extent the optional sub requirements should be integrated in the scheme or in appendix?
- Do you have any other comment on the proposed requirements?