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

Date: 2021-10-11

In the ECCG meeting on 22th September 2021 the Member States were invited to share in writing feedback on the criteria mentioned in the non-paper.

The Netherlands acknowledge the importance of the topic 'Digital sovereignty' and thanks our French colleagues and the European Commission for enabling this interesting and relevant discussion. The Netherlands supports efforts to address European Data Sovereignty and Digital Sovereignty. We agree that the discussion on data sovereignty and digital sovereignty is an important, political and urgent European policy topic.

- The Netherlands is firmly convinced that this topic must be addressed on a European political level before requirements of a political nature in the certification schemes are discussed by the ECCG.
- The criteria and requirements as such may easily result in disbanding non-European enterprises, personnel and services. A proper political discussion on guiding starting points is needed.
- We foresee inconstancies and contradictions with related EU-regulation like NIS, Data Act, Artificial Intelligence and GDPR. Alignment is needed.
- We believe that the European Commission is sufficiently equipped to organises the discussion on a more political level and is able to incorporate the relevant perspectives of the GDPR, data-autonomy, data sharing, Artificial Intelligence, NIS etc.
- The EUCS must not be delayed by the discussion on 'Digital Sovereignty' otherwise the CSA-implementation will lose its momentum.

In the annex we share more detailed comments on the criteria and requirements.

The opinion of the Netherlands and annex may be shared with the ECCG members, the Commission and ENISA.

Annex: Detailed comments on the criteria and requirements

In the this annex we address several important, more technical issues with the current version.

> In general the criteria and requirements in the current form are not effectively auditable by CABs and thus not ready yet to incorporate in a certification scheme.
>
> A substantial amount of work is needed to get the requirements on the right auditable level and some of the existing requirements in EUCS need probably adjustments as well.
>
> This work will hamper the progress on the EUCS and cause serious, and for us, an unacceptable delay.

Contents

General

Source document: "Non-paper by DE, ES, FR and IT on the EUCS requirements for immunity to non-EU laws" provided for the agenda of the ECCG at 22th September 2021.

Remark: Due to the lack of the policies /scoping and further conditions only addressed the main issues that arise.

In general: from "EUCS requirements for immunity to non-EU laws" towards elements of data sovereignty. Which is not addressed at political / economical level.

A detailed analysis and documentation on the impact of these criteria / requirements is not performed yet, but necessary to identify the impact for the current draft version of the EU CS. Generic risk is that adding a separate set of criteria that do not follow the same structure as the EU CS will slow down the further development of the EU CS scheme and making the criteria/security requirements confirmed as a standard by CEN/CENELEC, significantly. Which in itself imposes a slower implementation at CSP's and response to increasing cyber risks.

We suggest to take knowledge of the Zero Trust approach when identifying security criteria and requirements to implement data sovereignty.

The proposed criteria to add to the EUCS scheme according to the non-paper:

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

Only the EU law applies (1)

Ref	Proposed requirements for EUCS	Initial remarks
1.1	The cloud service provider shall ensure that its operational and commercial offer is performed by an EU organization, detained by EU actors.	In general what is the goal of this criteria? Of course CSP's need to adhere to EU laws. Is it the goal to prevent the export of knowledge, access to EU data (originated / produced), processing of EU data elsewhere, realize applicability for EU rules and procedures, define the boundaries for AI solutions in the future ……
		A lot of SME SAAS providers and new initiatives make use of Microsoft Azure / Google Cloud and AWS. This criteria requires additional controls and measures to fulfill by these CSP's. If compliance is not realized at start by these CSP's, this might have economically large direct impact for startups and limitation in developing new startups.
		What is the definition of 'EU Organization'' since many EU service providers are acquired by non-EU organizations. In the optional requirements some examples are shared. Most important is to define the maximum level of impact of the non-EU involvement. Need to be consistent with other regulation.
		A lot of subservice organizations are involved in providing the ultimate services as part of the Cloud orchestration. Subservices are not always offered by EU organizations.
		In the sub-requirement an option of licensing EU technologies is mentioned. Licensing is a domain on its own. This needs a lot of development for specific (and auditable) requirements and therefore the context and goal setting. This requires policy statements at EC level.
		Limitations of using high quality / interesting new services in the cloud service (as international players will do) from abroad, thus limiting the innovation at European level.
		Starting at short term it is expected that the EUCS scheme will be referred to by European legislation with a mandatory status. As also proposed by the CSA where at start schemes are voluntary but is mentioned that other regulation can make the schemes mandatory.
		Why limited to Assurance level 'High' where here we have the risk that EU knowledge at substantial / basic level can also be obtained / acquired by non-EU organizations.
		'High' Assurance level will become a relevant competence for a CSP in the market. Equal level playing field for SME CSP's.

Trusted employees are dedicated to the maintenance of the cloud service (2)

Ref.	Proposed requirements for EUCS	Initial remarks
C2.1	The service provider must document and implement a	The scope is 'Its' personnel.

Ref.	Proposed requirements for EUCS	Initial remarks
	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.	Subservice organizations are involved as being a part of the orchestration of the service or involved with internal processes (e.g. network scanning / SOC services etc). Personnel perform their activities as being employee of the subservice organization. CSP usually does not know who is / will be involved.
		Necessity to define trustworthiness.
		The sensitivity and the confidentiality of the client data is a responsibility of the client and not of the CSP.
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	This is a challenge in a virtualized environment where client data reside on different servers and are also dynamically transferred and shared on more locations.
		What is the scope of the data to be logged as routers, switches etc. also cache information and create information.
		Extra challenges in identifying who is in charge at the client side + integer documenting + decision about storage of that information. And have a reference with the GDPR requirements. And Data Governance Act.
		Waiting for a response from the client before accessing the environment limits the cyber resilience of the service.
		Logging data becomes sensitive either. - Specific requirements of encryption. - Authorizations of configuring log settings. - Access to logs. - Use of service accounts. - …
		Context for rules regarding monitoring using the log data etc.??

Ref.	Proposed requirements for EUCS	Initial remarks
		Log data in themselves is data with personal identifiable data. And have a reference with the GDPR requirements.
		Discussion: removing the access of data. This might be crucial data to replay the access and identify impacts and therefore an argument to define a period of storage And have a reference with the GDPR requirements.

Maintenance, operations of the cloud service and process, and data are located within the EU (3);

Ref.	Proposed requirements for EUCS	Initial remarks
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).	This is a challenge in a virtualized environment where client data reside on different servers and are also dynamically transferred and shared on more locations.
		How can the client determine the geographical location based upon technical information from the CSP? Challenge for the conformity assessment.
C3.2	The service provider must store and process the client data within the European Union at any time.	Difficulties to determine where the data is / has been.
		To define client data. Network traffic data is also personal identifiable data and carries client data.
		Non-EU Companies in the EU of owner of EU companies have to adhere to their country rules as well. Patriot Act in the USA / China regulations may have an opening to ask for data. See GDPR problems with Schremm II and Safe Harbor / Privacy shield issues.
		Sometimes for processing data non-EU resided personnel / organizations are involved. Accessing from abroad mean processing outside the EU.
		I drive with my (in EU bought) Volvo Car outside the EU. The motor management system is updated through cloud services that read data from the car upfront. Data storage and processing outside the EU.
		Network equipment (routers, switches, firewalls etc.) also caches client data. Scope discussion including the cyber risk effect
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.	Challenged in a virtualized environment + if users of that data provide their services from outside the EU.

Ref.	Proposed requirements for EUCS	Initial remarks
C3.4	The administration and supervision operations of the service must be carried out from the European Union.	- Copy in Non-EU… - Decision level in non-EU.. - Non-EU employees involved …

Technology exchanges between the cloud services and technology providers are controlled (4)

Ref.	Proposed requirements for EUCS	Initial remarks
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	Challenges in a virtualized environment.
		Extra requirements for having a register / integer CMDB as well.
		Extra requirements creates a cyber risk as well (taking notice of updates).
		In what respect is then the client involved?
		Expected is a reference to requirements for risk management process and how to involve that in the procedures. A better approach is to add Architecture requirements based upon risk analysis / classification. Which are not adequately addressed in the EUCS scheme yet.
		Sub requirement of a DMZ might be a relevant aspect and contribution to the current scheme. Preferably addressed in the current structure of the EUCS. But is already mentioned in CS-03.2. But might be further extended and more explicit and preferable better addressed as part of Operations security.
C4.2	Verification performed on inputs and outputs of the technical infrastructure shall be done on dedicated devices by the cloud service provider.	Definitions are relevant and necessary (verification / dedicated / devices).
		What is the goal setting of the verification?

Ref.	Proposed requirements for EUCS	Initial remarks
		Who are involved and how is this monitored and supervised?
		Input and outputs contain PII, therefore there are requirements from the GDPR applicable.
		The importance is not only to perform this on dedicated devices but more to perform this in control of the CSP and secured devices against access etc. from unauthorized systems etc.