Joint document: alternative solutions regarding the issue of Independence to non-EU law in the context of EUCS

Context/background:
The European Commission intends to incorporate Independence to Non-EU law criteria in the EUCS, the so-called INL-criteria. These criteria would amongst others entail requirements on data localization, immunity to non-EU law and on personnel with regard to the control that may be exercised by legal or natural persons over the cloud service provider seeking to certify any of its services. According to the European Commission these additional immunity criteria would apply to assurance level high.
Member States have different views on adding these requirements in the EUCS. Some Member States are in favor of introducing INL-criteria since they assume it would allow use- companies to differentiate on the cloud market services that ensure a high level of protection from non-EU legislation with extraterritorial reach that threatens the confidentiality of European users' data hosted in the cloud.
Other Member States have strong concerns since they foresee huge and negative economic consequences for the cloud sector, their partners in the online chain and its customers. These Member States regret also the absence of an economic impact assessment on the requirements and would rather first seek a political mandate. Furthermore, they fear an unnecessary "race to the top" into the assurance level high.
Furthermore, it is not clear to what extent INL criteria are compatible with trade law. The signatories of this non-paper ask the European Commission to provide a respective assessment.
Because of the additional immunity requirements, there has been a delay in finalizing the draft of the cloud scheme. Germany, France, Spain and the signaturing Member States of the non-paper regarding *'Perspective on Cloud certification and data sovereignty under the Cybersecurity Act'* believe that progress on the cloud scheme must now be made in a timely manner.[1] Therefore, we are willing to discuss possible solutions brought up in the discussions regarding the issue on INL-criteria. This non-paper includes 5 possible alternative solutions to move forward and sets out benefits and disadvantages (pros and cons) of each alternative. Note: These solutions are of technical nature only and without prejudice to the assessment of the European Commission regarding the compatibility of INL criteria with trade law.

In addition, Member States could focus on a common understanding of scenarios where immunity requirements for cloud services should be applicable, e.g. all sectors or (in order to avoid a "race to the top") limited to limited sectors such as state security or health sector.

Solutions:

1 Sub/Sub+ and High
An option would be to add an extra sublevel in assurance level substantial in the scheme: substantial level 1, substantial level 2. Furthermore, assurance level high will contain the immunity requirements. Assurance level substantial 2 would contain the requirements of assurance level high of the original EUCS draft (before the immunity requirements have been proposed).
In short, the option means that another assurance level will be established.

Pros	*Cons*
• *Introducing immunity requirements for CSPs and their customers* • *Preserve the technical requirements of the original high -> restructuring: moving the criteria of the current high level to substantial level*	• *Scope is too broad/vague, especially if it becomes mandatory to get certified at assurance level high regarding 'critical infra' (NIS2)* • *A possible mandatory nature* • *Lack of flexibility: establishing or adjusting the requirements in the*

[1] 'Perspective on Cloud certification and data sovereignty under the Cybersecurity Act' by Denmark, Estonia, Finland, Greece, Ireland, Latvia, Lithuania, Poland, Slovakia, Sweden and The Netherlands

• *Enables comparison of certification schemes with regard to the level of assurance "high".* • *Provides extensive (not complete) protection against unfounded assurance at a high level according to EU certificate in case of cloud service providers under the influence of third countries in which government access to the data for undefined purposes must be ensured.*	*technical scheme itself is a very lengthy and complex process* • *Legal challenges by adjusting the CSA framework: introducing a new assurance level* • *Unclarity for the market.* • *Not covering all assurance levels* • *The number of cloud service providers at level "high" will remain limited, because the costs are significantly higher (public administration costs, resources and costs for the CSP with regard to compliance) than for level "substantial".* • *Only partly overcomes industry objections.* • *SMEs cannot demonstrate fulfillment of INL requirements, as they might not fulfil requirements of level "substantial plus", and due to costs and time that is necessary for appliance for Level "high".* • *2 substantial-level could be hard to distinguish.*

2 High+ (critical uses)

Another option would be to distinguish two high sub-levels by adding a new 4th assurance level, so-called high+. This 4th assurance level should entail the immunity requirements.

Assurance level high+ be suitable for those certain critical uses of cloud services that require enhanced protection. An option could be not to pre-empt the needs of users as to what may constitute a critical use, this means there will be no defined list of use cases – because it cannot be comprehensive. General guidelines to inform users, with no specific use cases identified, could be laid down.

Another option could be that assurance level high+ would only apply to some 'critical uses of cloud services', which will be clearly defined. That clarity needs to be further elaborated as a condition. The option means also that another additional assurance level will be established.

Pros	*Cons*
• *Introducing immunity requirements for CSPs and its customers regarding critical uses. Which could offer stronger protection to certain data* • *The scope of the immunity criteria is limited and strictly applicable at the highest level of certification.* • *Enables users, who do not need immune services, to identify high-level services that provide strong cyber protection guarantees.* • *Preserving assurance level high* • *If cloud usase is clearly defined/well-scope it brings clarity to the market.* • *Overcomes industry objections, as long as "high + immunity requirements" is not a regulatory requirement and the "+ package" is not too heavily marketed.*	• *Scope remains too broad/vague (especially) if it becomes mandatory to get certified at assurance level high regarding 'critical infra' (NIS2)* • *Mandatory nature* • *Lack of flexibility: establishing or adjusting the requirements in the scheme itself is a very lengthy and complex process* • *Legal challenges as it would not follow the CSA's provision on having three assurance levels* • *Not covering all assurance levels and might make assurance level "high" somewhat irrelevant* • *The assurance levels of the different certification schemes are not consistent with each other (especially in comparison with EUCC).*

	• *SMEs cannot demonstrate fulfillmet of INL requirements, as they might not fulfil requirements of level "high", and due to costs and time that is necessary for appliance for Level "high"* • *Unclarity for the market although less than in determining a substantial level 2, if cloud usage is not well-defined*

3 Extension Profiles

The draft of the cloud scheme contains the possibility to develop Extension Profiles. An Extension Profiles could entail additional requirements (to certification scheme) such as the immunity-to-EU law criteria. So this gives a cloud service provider the opportunity to opt for an Extension Profile existing of immunity criteria, irrespective of the chosen assurance level.
These Extension Profiles could be drafted for narrowly-defined ways of cloud usage, such as cloud usage in very sensitive sectors (for example Health or Military Industry). The Extension Profile concept would basically create an add-on (with immunity requirements) on top of assurance levels 'high', 'substantial' and 'basic'.

Pros	*Cons*
• *Covering all assurance levels* • *A case-by-case approach is possible: a cloud service provider or customer can freely opt for INL; possibility for actors under NIS2 or CRA to seek synergies* • *Customer oriented approach: customer can select a CSP which fulfills to the INL* • *Flexibility: adapting and introducing the Extension Profile* • *Fits in the current framework of the Cybersecurity Act* • *Cloud service providers from the EU can demonstrate the INL criteria via EP at level "substantial" too, thereby demonstrating possible compliance with legal requirements in the EUCS. This could give medium-sized cloud service providers in particular a competitive advantage over non-EU cloud service providers.* • *During certification, services that reach level "substantial" can demonstrate immunity to non-EU laws with the same criteria as in level "high".* • *Most EU providers are not yet able to achieve level "high", but they can set themselves apart from non-EU providers.* • *Regulations which do not necessarily require level "high" (e.g., personal data) but do have requirements for data location and monitoring could use EUCS "substantial" with immunity to non-EU law.*	• *Extension Profiles need to be developed and operationalized* • *Inconsistency with the overall logic behind the certification, as INL-criteria are intended to respond to EU companies' concerns regarding the protection of their particularly sensitive data – hence the ones that wouldn't be sufficiently protected with 'basic' and 'substantial' levels* • *Uncertainty.*

4 Five evaluation levels, two at level substantial, two at level high

The INL criteria will be implemented into EUCS by introducing sovereignty levels in both categories (substantial and high). That means the EUCS will consist of five evaluation levels with: basic | substantial (core); substantial (INL) | high (core); high (INL).

Pros	*Cons*
• *Nearly same as Option 3* • *Additionally easier in terms of transparency as extension profiles are more complex to communicate than clearly identified levels ("sovereign" always being INL requirements)* • *Easier to operationalize because the sovereignty requirements are a real part of EUCS*	• *Scope remains too broad/vague (especially) if it becomes mandatory to get certified at assurance level high regarding 'critical infra' (NIS2)* • *Mandatory nature* • *Lack of flexibility: establishing or adjusting the requirements in the scheme itself is a very lengthy and complex process* • *Legal challenges as it would not follow the CSA's provision on having three assurance levels* • *The assurance levels of the different certification schemes are not consistent with each other (especially in comparison with EUCC).* • *Unclarity for the market although less than in determining a substantial level 2, if cloud usage is not well-defined*

5 Evaluation mechanism based on Trustworthiness

Another option, which is outside the scope of the CSA, could be to introduce an European evaluation mechanism based on trustworthiness of the whole or part of supply chain of non-European cloud providers and suppliers. The evaluation or screening at EU level will be a prerequisite for suppliers to offer their businesses/services on the European market.

The evaluation (assessment) of non-European market parties could be based on a risk-based assessment. Such an assessment on politically motivated immunity requirements can be separately introduced next to all (future) certification schemes.

It could entail both security and legislative criteria, including criteria on extra-territorial legislation and data transfers and compliance to GDPR.

The building blocks of this approach could be based on elements of Germany's IT Security Law 2.0 and the strategic measures on risk profiles of the 5G toolbox.

Pros	*Cons*
• *Strong tool: governing market access to non-EU CSPs* • *Not affecting technical certification schemes* • *A targeted approach* • *Reusable on other future schemes* • *Max flexibility, ideally suited for customization requirements of political nature (immunity)* • *No adjustment to CSA framework*	• *Lengthy process, since it should be a separative EU initiative and might just postpone the discussion from one forum to another.* • *Challenge to define a clear scoping that is also futureproof* • *As it would cover all non-EU CSP's regardless of whether they provide services to critical services or not, compatibility with trade agreements need to be assessed* • *An approach that is not user-centric and may limit the choices that users may make about their service providers.* • *The setting up of a parallel assessment mechanism would undermine the readability of offers and would create*

	too much uncertainty for providers, in particular non-European ones. • *There will be certification at level "high" which might not fully comply with the Cybersecurity Act (security objectives under Article 51 in conjunction with assurance levels under Article 52 (7) and (8)).*

6 Integration through compliance requirement EUCS

The INL criteria will be governed by European legislation, for example Data Act, GDPR or CRA. The legislation will address the entities which should comply to these criteria. Strong requirements regarding compliance will therefore be introduced in the EUCS. Thus, the INL criteria will be ensured by the cloud service provider. However, the INL-criteria will not be part of the scheme itself. This solution can be applicable for all assurance levels. Guidance can be developed in order to describe what the CSP is entitled to do (investigate, analyze, address, comply, implement and prove) to be compliant.

Pros	*Cons*
• *Strong tool, political engagement* • *Not affecting technical certification schemes* • *Applicable for all assurance levels* • *Possibly a targeted approach: flexibility, customization immunity requirements and updating guidance* • *Reusable on other future schemes* • *No adjustment to CSA framework* • *No delay in the finalizing of the EUCS*	• *Modifying current/upcoming legislation to address the immunity aspects* • *One modification to the EUCS regarding explicit compliance with applicable law.* • *Lengthy process and might just postpone the discussion from one forum to another.* • *Amongst the potential EU law(s) feature also such laws (e.g. the data act) which are not about cyber security as such. Also potentially other legislative changes might be then needed; coherence among the proposals would need to somehow be guaranteed.*

Follow-up:

The following factors should be taken into account when elaborating on possible solutions:

- Strong involvement of both cloud service providers and customers and their perspective on immunity.
- Any possible solution should be accompanied by an economic impact assessment in advance which is not focusing on only costs/investments but also benefits and conditional for being able to adjust new developments and/or strengthen innovation capabilities in the EU.
- Taking into account the effect of INL-criteria on future schemes, such as the IoT-scheme.

Figure: various solutions