European Association of CCP Clearing Houses

August 2022

EACH Letter – EACH members considerations and recommendations on EU Cybersecurity Certification Scheme for Cloud Services

1. Introduction

The European Association of CCP Clearing Houses (EACH) represents the interests of Central Counterparties (CCPs) in Europe since 1992. CCPs are financial market infrastructures that significantly contribute to safer, more efficient and transparent global financial markets. EACH currently has 18 members from 14 different European countries. EACH is registered in the European Union Transparency Register with number 36897011311-96.

The objective of this letter is to put forward EACH members' concerns and recommendations relating to some of the restrictions under consideration within the EU Cybersecurity Certification Scheme for Cloud Services (EUCS) on the ability to use cloud services providers (CSPs) **based on where the CSPs and their shareholders are located and where their data is being stored or processed**. While this is still a **voluntary scheme**, the **NIS2 could mandate certification of such service provisions for all entities falling within the scope of NIS2, including CCPs**.

2. EACH members' considerations

CCPs significantly contribute to the safety, efficiency and transparency of global financial markets. European CCPs are core to the financial stability of the EU, and because of this operational resilience is increasingly central to ensuring well-functioning EU financial markets. Over the recent years, financial markets are facing a rise in the number and sophistication of cyber attacks. As such, ensuring cybersecurity and operational resilience is at the heart of CCP operations.

EACH, therefore, welcomes the increased focus in the EU on harmonized emerging requirements on firms' cyber and operational resilience, including via the revised Network and Information Security Directive (NIS2), the Digital Operational Resilience Act (DORA) as well as the Resilience of Critical Entities Directive.

To efficiently manage operations and increase operational resilience, EACH members outsource their workflows to CSPs. CSPs can offer solutions with higher operational resilience by providing robust IT infrastructure, allowing geographical diversity of data centres, through enhanced disaster recovery and by mitigating legacy technology risks, such as single-points-of-failure. By outsourcing to CSPs, CCPs benefit from i**ncreased operational resilience,**

European Association of CCP Clearing Houses AISBL (EACH), Avenue des Arts 6, 1210 Brussels

improved efficiency and scalability, and higher flexibility and innovation capabilities. The use of CSPs allows for more efficient and timely workstreams and increases the flexibility to boost cloud capacities when necessary.

EACH supports the introduction of an EU Cybersecurity Certification Scheme for Cloud Services (EUCS) led by ENISA under the EU Cybersecurity Act, to create harmonised EU-wide standards and improve cybersecurity as well as enhanced oversight and auditing tools on cloud. However, as underlined in the introductory section, **the restrictions under considerations within the EUCS** on the ability to use CSPs based on where the CSPs and their shareholders are located and where their data is being stored or processed **would undermine EU CCPs' ability to manage their operational and cyber risk effectively** hence affecting our ability to provide clearing services underpinned by best-in-class operational resilience.

This would have ramifications for the EU financial sector, especially financial market infrastructures (FMIs) including CCPs and other sectors that rely on best-in-class technology for critical operations. Under current considerations, CCPs would be **forced to exit longstanding contracts** with existing non-EU based CSPs without a suitable alternative.

EUCS's focus on localisation provisions (EU headquarters and EU control/access) could not only affect the quality and security in the European cloud market but will also make it more difficult for European companies to **operate and compete globally**. It would make access to best-in-class technology challenging, thus **undermining EU CCPs operational and cyber resilience, but also the competitiveness of our operations in the EU**. This would put EU CCPs at a competitive disadvantage (fewer CSPs options) to their non-EU peers who would maintain access to non-EU providers, thus contradicting European Commission's ambition to increase the competitiveness of EU CCPs.

This could not only **deter innovation** and reduce the EU's attractiveness as a place to do business but also **weaken security by hindering the exchange of information**. Importantly, it will not add to increased levels of cybersecurity. Furthermore, every FMI and financial market participant could reduce overall dependence by following a so-called multi-cloud strategy in order to be more robust and flexible by using different service offering. We already observe new solution by the CSPs to integrate EU data concerns into their policies (isolated regions, "bring your own key" concepts).

Furthermore, such localisation rules could inspire **localisation rules from other jurisdictions**, which could severely impact EU service provision globally and should be avoided. Such counter measures from other jurisdictions would not only impact wider EU service providers but also **affect the competitiveness of EU CSPs** looking to offer or offering cloud services in strategically important non-EU markets.

Hence, if such requirements were to be adopted, it would impact not just the competitiveness of EU services but also the operational resilience of EU entities and the overall quality of

services provision. While we acknowledge the need to regulate and have a proper EU oversight of CSPs, we believe that there are more efficient ways of ensuring oversight and control over risks posed by CSPs that would protect cloud users in the EU and raise the operational resilience of the industry. We recommend developing industry solutions together with CSPs, such as isolated region concepts, "bring your own key" concepts and multi -cloud strategy.

3. EACH members' recommendations

EACH recommends the **following be considered in the finalising of EUCS**:

- **High level of resilience can be achieved through enhanced contractual arrangements with CSPs, increased supervision of critical CSPs, and rights of access, (financial industry pool-) audit and oversight , as introduced in DORA**. DORA aims to increase harmonisation of requirements to increase resilience in the EU and we believe that any **EU cybersecurity certification should also be aligned with this**. DORA has successfully avoided adding any requirements on data localisation in the latest negotiations and it would create more fragmentation in EU regulation should sovereignty measures be adopted in the draft EUCS.
- **Envisaged requirements in the EUCS draft for sectors using critical/level-high certified CSPs should be accompanied by a stakeholder engagement (taking into account technical/operational/legal solutions by CSP providers) and thorough impact assessment as well as consultations with the market participants before becoming a matter of discussion.**
- Furthermore, any concerns on customer data protection on cloud and supervision of non-EU cloud providers should be addressed in **international and cross-jurisdictional forums**, such as the EU-US Trade and Technology Council meetings. We need to have a constructive dialogue on creating efficient and workable solutions.

As such, we would recommend further **cooperation between the European Commission, Member States, ENISA, DORA NCAs, and the ESAs** to help achieve a proportionate and harmonised framework for operational resilience and cybersecurity on cloud e.g. by identifying critical cloud service providers with consultation from ENISA.
Finally, we also encourage **coordination at global level** to work together in tackling issues such as sector-wide concentration risk to combat systemic risk and financial stability concerns. Localisation requirements such as those envisaged within the draft EUCS could bruise historic cross-border relationships and dampen the motivation for effective collaboration on facing global issues.

-END-