Central Eastern European digital industry's appeal for responsible development of the European Cybersecurity Certification Scheme for Cloud Services (EUCS)

The significance of cybersecurity becomes clearer than ever before. An increase in the number of incidents and attacks is nearly universal. Central Eastern European countries are struggling with a major uptick of incidents and attacks these events recently as well. In 2021 Lithuanian police registered more than 50% increased rate of cyber-offences compared to 2020. Earlier this year Lithuania's officials admitted an "unprecedented cyber attack" following introduction of block on the transit of sanctioned goods to Kaliningrad. A 50% increase in the number of attacks on networks in the private sector in 2021 compared to the previous year was also recorded in the Czech Republic according to Check Point. The same research agency reported that number of cyberattacks on Polish companies grew by 35% in the period of January-June 2022.

As Europe transforms, adoption and development of cloud computing technology and solutions remain a crucial factor in pursuing the goals of the European digital strategy. Cloud services and technologies provide access to novel services for citizens and tools for growth of businesses. Many countries of Central Eastern Europe are still considered "digital challengers" as their economies continue to have enormous opportunities to benefit from the technology's capabilities and potential for growth. Thus regulations affecting these areas bear a major impact on the ability of our region's economies to develop, continue on the path of digital transformation and remain resilient.

We, the digital industry of Central Eastern Europe, gathered around the initiative of CEE Digital Coalition, continuing our efforts to build a competitive and innovative digital economy and prosperous, safe modern civil society in our region, wish to call upon our national leaders and European Representatives to address the concerns revolving around the ongoing development and process related to the European Cybersecurity Certification Scheme for Cloud Services (EUCS), and to raise awareness of the impact the final EU Implementing Act that defines the EUCS may bear on our region and thus entire Europe's security and ability to innovate and develop the digital single market

The European Union Agency for Cybersecurity (ENISA) is working on the European Cybersecurity Certification Scheme for Cloud Services (EUCS). The EUCS will be translated into an EU Implementing Act that must clearly define the requirements for entities to achieve this EU-wide certification. International certification schemes and standards play an important role in the evolution

of the digital services' market by providing clearly defined frameworks supposed to guarantee safety of end users and fair competition. However, provisions of the EUCS' draft scheme already appear to pose a real risk to building a fair, open and resilient market as well as to the emergence of innovative, globally competitive solutions using and based on cloud computing solutions in Europe.

The EUCS will follow the EU Cybersecurity Act by introducing three levels of assurance: "basic", "substantial" and "high". A growing number of EU Member States and industry entities have serious concerns about so-called "sovereignty requirements" imposed on entities wishing to receive the "high" assurance level of certification as defined in the draft EUCS. ENISA, drafting the EUCS at the request of the European Commission, is responsible for defining the strict "sovereignty requirements"[1] necessary to acquire "high" assurance level certification. ENISA and the European Commission are very much aware of the growing criticism from both governments and industry regarding these non-technical requirements. These include a requirement for providers of cloud services to be globally headquartered in Europe and not be controlled or owned by any non-EU entity. Moreover, the scope of "high" assurance level requirements is currently described vaguely and without sufficient precision of which concrete workloads would be covered by the assurance level "high" or which sectors of economy would be in scope (financial services and banking, energy, healthcare etc.). This may lead to an unharmonized interpretation and legal uncertainty across the European Union as well as creating significant obstacles to the Internal Market principles. Both of these phenomena are undesirable in the digital single market.

These provisions may make it difficult or impossible for cloud services providers legally operating in Europe to apply for the EUCS "high" assurance level. Without this certification, these market players would be deprived of their ability to provide online services, advanced technology, and cloud security solutions to their business customers and consumers in the EU. It is clear that this would result in stunted emergence of innovative solutions and services in European Union, harm to growth of the digital economy and in limiting of the potential of companies to compete on global markets

The bottom line goal of all regulatory initiatives affecting digital technology - including the cloud - should be to remain resistant to lapse of time and to limit the risk of regulations not responding to the reality of the digital market and technological progress. The EUCS Implementing Act will have a fundamental impact on the cloud market by limiting the choices for European customers, both at SME levels and entities providing critical infrastructure services. Therefore, we feel obliged to appeal to European and our region's national officials to:

Assure transparency of project's progress and conduct public consultations amongst all parties affected and cloud cybersecurity experts. The EUCS security requirements and controls will affect all businesses providing, developing and using cloud computing solutions (e.g. automotive manufacturers, banks, healthcare providers). Due to a wide range of entities interested in the Scheme, a transparent process of creating EUCS is a must. It should include proper consultations with those affected. Regular publishing of updated projects and informing about significant developments as well as estimated timeline of work on EUCS is advised. ENISA launched a public consultation on a first draft of the EUCS in the end of 2020, however the EUCS has significantly been changed by adding non technical requirements, This requires a new consultation, since it significantly changed the impact of the EUCS.

[1] Also known as "Independence from non-EU laws", as defined in the leaked draft candidate scheme Annex J

Present a precisely defined impact assessment for EUCS and provide guidelines on adhering to Certification Scheme. Impact assessment and guidelines will grant support for European companies providing, developing and using cloud solutions, which will need to comply with the requirements set out in the EUCS Implementing Act in order to remain active in Europe. This is particularly important in the case of entities, which will aim to meet the "high" assurance level. Assessment and guidelines based on thorough risk analysis should address costs and predicted benefits of the Scheme and clearly define data categories, processes and use cases affected by EUCS.

Consider replacing the requirement to be headquartered in Europe and not be controlled by any non-EU entities with a simple requirement of having a legally operating EU branch. From the Digital Sovereignty standpoint, provisions asking for a legally operating EU branch of non-EU headquartered entities allows for sufficient auditing and enforcement. Most importantly it would not override World Trade Organization regulations and avoid implementing policies that may be considered protectionist by our western non-EU governmental partners. Such a requirement would not only be sufficient to assure compliance with EUCS but also much easier to verify. EUCS must not be a Scheme based solely on a political vision, but should rather answer to the reality of the Digital Single Market, be aligned with the cybersecurity needs and allow for use of best, most secure and efficient technology available, regardless of its country of origin.

Guarantee access to auditing and enforcement of EUCS requirements. Should they be introduced, meeting sovereignty requirements may prove to be difficult to control in scope of auditing procedures. As the structures, ownership statuses and business models constantly evolve (i.e. in case of start-ups, i scale-ups, by mergers etc.), officials and bodies responsible for auditing compliance with security requirements will struggle to determine whether all the shareholders of any given company are based in the EU. This may also lead to issues related to state aid and competition law, where one European enterprise might be in a more favourable position than others. Complex enterprise structures can also make the task of clearly stating whether the global headquarters of a company are in fact located in Europe.

Make compliance with EUCS voluntary, while following a regulatory path and timeline allowing for adaptation to evolving regulatory framework. Attempting to speed up the imposing of cybersecurity certification requirements by introducing articles of such effect in other EU regulations (i.e. the NIS 2 directive, AI Act, eIDAS), designed within the framework of the Cybersecurity Act of 2019 by Even if impact and risk assessment and public consultations are carried out, following the Certification Scheme should remain optional for the sake of growth of digital single market, which draws its potential and innovativeness from freedom and diversity. Without the promised consultation and evaluation described in the EU Cybersecurity Act (2019) to do an assessment by December 2023, the Commission is moving ahead faster by implementing articles in NIS2, AI, E-IDAS that require EU cybersecurity certification.

Consider the impact on existing business partnerships and potential investments. As residents of the Three Seas Initiative and representatives of its countries' digital industry, we are well aware of the value of close, healthy transatlantic relations and the immense boost business cooperation with US partners grants to CEE's economy and subsequently, our security. We are concerned that limitations projected to be imposed on providers headquartered across the Atlantic Ocean are of major economic impact for our region and might not be based in pursuit of cybersecurity in its technical scope, but

rather an effect of political incentives that differ from our regional political incentives and interests. Strictly technical aspects of cybersecurity and its certification schemes should not be tainted by politically driven issues of "digital sovereignty".

Hear the voice of all Member States. We must also voice our doubts, whether simply copying certification schemes existing in some European countries is the proper way of creating EU-wide requirements. Using the great foundation of already existing tools is recommended but insight of all Member States, including CEE's countries must be considered while EUCS is developed.

We appeal to our national leaders, European officials and CEE's representatives in the EU to steer the development of EUCS towards the above requests. **We call upon all parties involved in the development of EUCS and those striving for our region's digital progress to consider the impact of Certification Scheme on the fairness of competition in the digital single market and opportunities granted by cloud computing which are at stake, if we move forward with the concerning proposals. We wish to offer our full support in providing expertise, know-how and to declare our deep will to engage in constructive discussion. We remain at the disposal of officials developing the European Cybersecurity Certification Scheme for Cloud Services and are looking forward to the introduction of a Scheme providing security and fostering growth of the digital market.**

Respectfully,

- On behalf of Confederation of Industry of the Czech Republic, Ondřej Ferdus, Director of Digital Economy and Technology Unit
- On behalf of Association of Producers and Dealers of ICT equipment, APDETIC, Valentin Negoita, President
- On behalf of Employers' association of the Software and Services industry, ANIS, Gabriela Mechea, Executive Director
- On behalf of Slovak Alliance for Innovation Economy, SAPIE, Michal Kardoš. Executive Director
- On behalf of DigiTech Sector Association INFOBALT, Mindaugas Ubartas, CEO
- On behalf of Digital Poland Association, Michał Kanownik, President