CONFEDERATION OF INDUSTRY
OF THE CZECH REPUBLIC

Cyber Security of Cloud Services in the light of Digital Sovereignty Requirements

ROUNDTABLE STRUCTURE

On 31st of May 2022 the Confederation of Industry of the Czech Republic organized a roundtable on *"Cybersecurity of Cloud Services in the Light of Digital Sovereignty".* Among the main panelists were Dita Charanzová, Vice-President of the European Parliament, Petr Očko, Deputy Minister for Digitalization and Innovation at the Czech Ministry of Industry and Trade, Martin Klumpar, Head of Cloud Computing Regulation Unit at the National Cyber and Information Security Agency of the Czech Republic, Florian Pennings, Government Affairs Director for Cybersecurity at Microsoft and Michiel Steltman, Director at Online Trust Coalition, Netherlands. The debate was moderated by Jana Pattynová, partner at the technology law firm Pierstone.

ROUNDTABLE SUMMARY

It is increasingly recognized by experts from various national and international organizations that cybersecurity is not only a technical and legal matter. Foreign policy, cyber diplomacy and digital sovereignty are important elements of any cybersecurity framework. All these aspects can be found in policies and regulations that governments adopt in order to make their citizens and businesses safer and more resilient against cyberattacks.

Any regulatory interventions, however, have complex impacts. They may result in limitation of available technologies, reduction of customer choices, in delayed digital transformation, stifled innovation, distortion of competition and disproportionate administrative burden. We do not face simple choices such as whether we want a more robust cybersecurity, faster digital transformation, or more digital sovereignty. We face a difficult balancing exercise that would enable progress in all these strategic objectives.

In this context, discussion focused on current priorities of the European Union in the field of cybersecurity and digital sovereignty and on how they impact the proposed regulatory measures in cybersecurity and cloud services, both on the EU level and on the national level in the Czech Republic.

Summary of main agreed policy objectives and strategic priorities that must be reflected in the upcoming regulations:

1. TRANSATLANTIC COOPERATION AND COLLABORATION WITH LIKE-MINDED COUNTRIES

Due to the Russian aggression against Ukraine, cybersecurity and cooperation to protect data and respond effectively to the security challenges are now extremely high on the list of EU's strategic priorities. Europe needs to realize that working together with allies is necessary for avoiding both the digital isolation of Europe and imposing unjustified protectionist measures.

2. HARMONIZING STANDARDS ACROSS THE EU AND AVOIDING UNNECESSARY FRAGMENTATION OF THE EU MARKETS

Any deviation creates fragmentation. In order to achieve true digital single market, ensuring harmonized standards should remain a key objective of any newly proposed legislation.

3. BALANCE BETWEEN RESILIENCE AND CYBER SECURITY

It is not easy to determine where the line between assuring national and European security is. There is a need to ensure that the European approach is not based on the premise that a non-European solution is considered less secure. Ensuring resilience and cybersecurity of the supply chain of the advanced technologies like cloud, 5G or chips are issues that need to be discussed in open and transparent debate.

4. APPROACH TO REGULATION

Principle-based regulation can be considered better suited to implement these objectives than a rules-based approach. When preparing new legislative proposals, it should be borne in mind that not every scenario can be covered. Otherwise, the development of innovation may be limited.

5. THE LEGISLATIVE PROCESS MUST, FROM THE OUTSET, BE BASED ON TRANSPARENT DISCUSSION WITH ALL RELEVANT STAKEHOLDERS

It is important that the discussions on technical standards that take place within the expert groups are clearly separated from political discussions. Otherwise, all institutions, such as the European Parliament and the Council, and stakeholders should be part of the discussion.

CONTACT

For more information please contact Kateřina Kalužová at kkaluzova@spcr.cz.