



THE CYBERSECURITY COMPETENCE CENTRE STARTS TO TAKE SHAPE REGULATION ADOPTED BY THE COUNCIL OF THE EU

1. Introduction

In the recent years, cybersecurity has become one of the crucial areas that the European Union (“EU”) decided to invest in to get fit for the digital era. In order to acquire leadership and autonomy in this field, the EU takes steps to develop competencies, capacities and capabilities.

One step in this regard is represented by the draft regulation establishing a new EU body - the European Cybersecurity Industrial, Technology and Research Competence Centre (the “**Competence Centre**”), which has been adopted on April 20, 2021 by the Council of the EU.

2. Role of the Competence Centre

As it now stands, the draft regulation provides that the Competence Centre’s main mission is to help increase the security of critical network and information systems. In order to fulfil the same, it will perform a dual role:

- (i) it will undertake strategic and implementation tasks in cybersecurity industry, technology, and research;

- (ii) it will manage cybersecurity-related funding from several Union programmes, particularly from Horizon Europe¹ and the Digital Europe Programme².

From an organisational perspective, the Competence Centre will consist of (i) an executive director, (ii) a governing board, and (iii) a strategic advisory group. In its activity, it can also call upon the expertise of natural persons as ad-hoc experts.

The draft regulation also establishes the organisation of:

- the Network of National Coordination Centres (the “**Network**”) which will consist of state-owned entities with research and technological expertise in cybersecurity; and
- the Cybersecurity Competence Community (the “**Community**”) which will gather stakeholders that have cybersecurity expertise in various domains.

Both entities’ role will be to support the Competence Centre’s activity.

The Competence Centre will be headquartered in Bucharest, Romania and will work closely with the Network and the Community and, where appropriate, with the European Union Agency for Cybersecurity (“**ENISA**”), on the following main tasks:

- (i) facilitate access of the small and medium enterprises, start-ups, associations to knowledge; such access will help the same solve the cybersecurity challenges they face, such as the implementation of the security by design approach;
- (ii) facilitate collaboration and the sharing of expertise among all relevant stakeholders, in particular members of the Community, on a regular basis;
- (iii) support the adoption and integration of state-of-the-art cybersecurity products, services and processes by public authorities at their request, by demand-side industries and by other users.

Through this approach, the Competence Centre will put an end to the fragmentation of the research and development efforts throughout EU and will shape a strategic orientation for the future of cybersecurity.

3. Next steps

The draft regulation will be sent to the European Parliament, who has to provide its input on the Council’s position within three months and to either:

- (i) approve it – case in which the draft regulation will be adopted;

¹ More information are available here: https://ec.europa.eu/info/horizon-europe_en.

² More information are available here: <https://digital-strategy.ec.europa.eu/en/activities/digital-programme>.

- (ii) reject it – case in which the draft regulation will not enter into force and the whole procedure shall end;
- (iii) propose amendments and return the proposal to the Council for a second reading.

If amendments are proposed, the Council will have to examine the same and either approve them all or convene the conciliation committee.

According to the draft regulation, the European Commission is entrusted with setting up and running the Competence Centre until the same can operate independently. Thus, pending the final vote in the European Parliament, the European Commission already started discussions with the Romanian authorities on the practical aspects related to the incorporation of the Competence Centre.

The EU’s initiative to build a centre for cybersecurity is more than welcome given the fragmentation of expertise and know how across more than 660 cybersecurity expertise centres that now exist throughout EU. The Centre is thus expected to help Member States take a proactive, longer term and strategic perspective to cybersecurity industrial policy. This should fuel the EU’s competitiveness in this field in a time when safeguarding data and creating more diverse supply chains environments are in the spotlight.



Alina Popescu
Founding Partner

alina.popescu@mprpartners.uk



Cristina Crețu
**Senior Privacy
& Technology Consultant**

cristina.cretu@mprpartners.com



Laura Dinu
Associate

laura.dinu@mprpartners.com

WE TRANSLATE LEGAL
TO BUSINESS