RegCORE Client Alert

Shoring up the defences – the EU's new cybersecurity competence centre (ECCC)

September 2021

EU Cybersecurity Competence Centre

Shoring up the defences – the EU's new cybersecurity competence centre (**ECCC**)

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas
@pwc.com

Contact RegCORE Team
de_regcore@pwc.com

Improving cybersecurity and resilience of financial services, certainly those performing critical economic functions, has been a long-standing priority of legislative policymakers but also supervisory authorities. Legislative but now with the ECCC also institutional action has been taken in a successive fashion[1].

Finance is changing and with an increasing shift by financial services firms to meet customers' demands for digitisation, online services, mobile applications as well as a sustained move amongst firms but their counterparts and clients towards remote and location-independent working means cyber-security is now ever more important than ever. With rapidly evolving threat actors that are constantly adapting their tactics, techniques and procedures (**TTP**s) to remain ahead of financial services firms' defences, the EU created the ECCC[2] by way of an EU Regulation (2021/887)[3].

[1] On 16 December 2020, the European Commission presented its new Cybersecurity Strategy and the revised Network Information Security Directive (**NISD2**) and the EU Critical Infrastructures Directive, which collectively aim to bolster the EU's collective resilience against cyber-threats and ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools across the EU's Single Market.
[2] Financial services firms may also want to take note of the annual guidance and recommendations published in the context of Europol's Internet Organised Crime Threat Assessment (**IOCTA**). IOCTA is Europol's flagship report providing a law enforcement focused assessment of evolving threats and key developments in the area of cybercrime. IOCTA should be available here from December 2021.
[3] Available here.

pwc

New kid on the block

From its new base in Bucharest[4], the ECCC is tasked to increase Europe's cybersecurity capacities and competitiveness, working together with a Network of National Coordination Centres (**NCC**s) to build a strong cybersecurity "competence community" of stakeholders with expertise in various areas[5]. As a "Competence Centre" the ECCC is not a formal authority or agency per se but nevertheless has wide-reaching powers, notably to, together with the NCCs, is tasked to pool investment in cybersecurity research, technology and industrial development and to better coordinate planning of funding from the EU's "Horizon Europe" (ca. EUR 2 billion) and "Digital Europe" funding programmes along with contributions from Member States matching EU Commission funding.

Furthermore, the ECCC plans to conduct research and innovation measures (with the support of Horizon Europe) as well as capacity-building measures (with the support of the Digital Europe Programme) on its own responsibility and will use its own expertise in advising other programmes (such as the European Defence Fund) in order to avoid duplication of efforts. The ECCC will work closely with NCCs to reach out to the cybersecurity community and gain its support. These activities will pay particular attention to the concerns of small and medium-sized enterprises (**SME**s) and start-ups.

The ECCC aims to ensure greater coordination of research, development and innovation and of strategies to introduce and integrate cybersecurity products, services and procedures at European and national level.

Equally, the ECCC will coordinate with the breadth of national and EU-level structures, notably the European Union Agency for Network and Information Security (**ENISA**), the EU's official cybersecurity agency based in Greece, which will continue to set standards under its revised mandate following the introduction of the EU's Cybersecurity Act (Regulation 2019/881).

When taken together, ECCC plus ENISA aim to increase the EU's "strategic autonomy" in the area of cybersecurity, support the EU's Digital Single Market efforts in areas ranging from e-commerce to smart mobility and the Internet of Things[6].

From getting started to getting up to speed

The ECCC, is expected to grow from an initial staff of 30 to 70 to 80 in the near future. It has an EU-27 wide governance structure. Its principal decision-making body is the Governing Board, in which all EU Member States take part but only those which participate financially have voting rights. The voting mechanism in the Governing Board is proposed as a double majority principle, requiring 75% of the financial contribution and 75% of the votes. The Governing Board will be assisted by an Industrial and Scientific Advisory Board (**ISAB**) to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders.

The ECCC's priorities on which projects it and NCCs will provide financing for is based on the advice the ECCC's Governing Board receives from the ISAB. The bulk of funding channels will follow established EU-

---

[4] Which was chosen following a competitive process over Brussels (Belgium), which went head-to-head with Bucharest in a 15-12 final vote. Munich (Germany), Leon (Spain), Vilnius (Lithuania), Warsaw (Poland) and Luxembourg were all in the running but lost out. Bucharest also convinced the panel due to Romania having been denied the possibility to host any EU agency/authority or hub since having joined the EU-27 in 2007. Bucharest is already home to a deeply active and rapidly growing IT sector with a number of cybersecurity firms in the city's digital ecosystem. A further factor that favored Bucharest was the fact that most recent figures showed that Romania ranks third in EU statistics on female employees in Information and Communication Technology (**ICT**) and 24 percent of ICT graduates in Romania are female The ECCC is expected to boost Bucharest and Romania generally as a center for cybersecurity companies. Once physical meetings return following COVID-19, the ECCC will also serve as a central meeting point for EU cyber policymakers and industry officials and thus boost Bucharest's economy over the medium to long-term.

[5] The NCCs will intensify exchange among EU Member States, enabling interested parties in government, industry and the research community in the European Union to identify partners for multilateral projects more quickly and easily, thereby increasing the EU's digital sovereignty. Within each EU Member State, a NCC will promote and intensify dialogue and exchange among interested national partners. In this way, the flow of information to the ECCC will be consolidated to provide optimal support to the national cybersecurity community and to ensure that national interests are represented effectively in the EU's funding programmes.

[6] This issue was highlighted in the draft legislation preceding the establishment of the ECCC and the Cyber NCCs in stating: "At the moment, the Union depends on non-European cybersecurity providers. However, it is in the Union's strategic interest to ensure that it retains and develops essential cybersecurity technological capacities to secure its Digital Single Market, and in particular to protect critical networks and information systems and to provide key cybersecurity services."

27 procurement processes and thus requests for proposals and calls for tenders that the ECCC will manage and disburse to recipients – i.e., academic and research institutions, private sector market participants and/or public authorities. The individual NCCs may also be able to financially support operations in their own "national ecosystems" by using cascading grants.

It is expected that the ECCC, once fully operational, may, together with the NCCs launch a range of large-scale cybersecurity projects and reform efforts. These range from improving cyber-threat intelligence, cyber-secured hardware and operating system standards and more harmonised security certifications[7]. They also extend to the ECCC facilitating relevant research and collaboration amongst industrial communities and public authority stakeholders in a pooled manner, thereby leveraging off joint efforts where Member States and national authorities have not been able to advance reforms individually.

About us

PwC Legal is assisting a number of financial services firms and market participants in forward planning for changes stemming from these proposals.

If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's RegCORE Team via de_regcore@pwc.com or our website.

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas@pwc.com

www.pwclegal.de

[7] Including interoperation with the work of the European Cybersecurity Certification Group and the Certification Framework, details available **here** and **here**.