Charles Russell Speechlys

Cyber Co-ordination 2024 - new MOU on co-operation between EBA ESMA EIOPA and ENISA

15 July 2024

The wave of legislation from the European Union in relation to cyber, operational resilience and ICT risk continues to demand unprecedented co-operation between European authorities.

Our previous paper from March 2024 highlighted the European Systemic Risk Board's (ESRB) review of macroprudential frameworks for cyber resilience (16 April 2024).

Four authorities, the European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA), European Securities and Markets Authority (ESMA) and European Union Agency for Cyber Security (ENISA) have issued a Memorandum of Understanding ESAs and ENISA sign a Memorandum of Understanding to strengthen cooperation and information exchange - European Union (europa.eu) to co-ordinate further their activities in this area. While the MOU is not binding, it sets out clear guides for strategic co-operation between authorities.

The MOU sets out a framework for co-operation and exchange of information between these European supervisory authorities, including in the areas covered by the NIS2 Directive, DORA and other areas of mutual interest. This is important, as regulated firms require consistency between their respective obligations in order to manage the increasing complex and hostile cyber environment.

The MOU is very short consisting of six articles. The key substance is the ten points in article 2 which emphasises that the parties will co-operate to implement "the tasks of common interest stemming from the NIS Directive and DORA". In particular this relates to:

- reporting of major ICT-related incidents;
- development of draft technical standards;
- mechanisms to share effective practices across sectors or the provision of technical advice and sharing of "hands on" experience on oversight activities.

ENISA will facilitate the participation of the various supervisory authorities in this context in order to collaborate on the implementation of efficient instant reporting processes for the EU financial sector. In this regard ENISA will support in the implementation of an IT tool for instant reporting based on ENISAs cyber incident reporting and analysis system (CIRAS) tool. As further undertaking of the parties to collaborate on the development of the Pan-European systemic cyber incident co-ordination framework (EU-SCICF). This resulted from the recommendation of the ESRB from 2021 and follow-on operational policy review from April 2024.

Of course, these obligations will require co-ordination and development of capability consistently across the authorities and exchange of information and views in relation to cyber risk, emerging technologies of mutual consent and common strategic interests. This does not explicitly include AI, but the risks from AI are implicitly covered within cyber.

The parties will establish a single contact point organisation for monitoring the MOU, including a work plan which will be reported on at least once a year to specify the initiatives and actions and appropriate allocation of tasks between the parties.

Whilst the MOU is high level at present, the parties can agree to establish joint or bi-lateral service level agreements on instant reporting, cyber security audits trainings or other topics within their fields of competence. As such it will be necessary for firms to continue to monitor each of the ESAs' own releases in order to establish the co-ordination.

In terms of reporting frameworks, the indication of the reporting tool is a useful insight, and firms should keep their contractual contracts, contractual obligations and reporting procedures up to date to cover the co-ordinated approach and ensure its supply chain is fully appraised of the consolidated reporting obligations and multi regulator coordination.