FESE Position Paper on the NIS 2 Directive and the CER Directive

7th May 2021, Brussels

FESE welcomes the European Commission's recent proposal on the new EU Cybersecurity Strategy. We agree that the "Strategy will bolster Europe's collective resilience against cyber threats and help to ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools." Exchanges play an important role in supporting the stability of the financial system and as such are taking several measures to build up their cyber resilience.

We would like to take this opportunity to provide some additional considerations on the two proposed Directives, the revised Directive on Security of Network and Information Systems (NIS 2 Directive) and the Critical Entities Resilience (CER) Directive.

Harmonised regulatory regime

FESE favours the harmonisation of the already existing rules on cybersecurity at the EU level. We believe that the focus of the EU Cybersecurity Strategy for the financial sector should be to reconcile the divergences between the current frameworks at EU and Member State level, and to avoid further fragmentation. Actors in the financial sector, including highly regulated ones, should be able to use new technologies without a disproportionate burden. Standardised and proportionate requirements across the financial sector would improve overall resilience.

FESE believes that DORA is the most appropriate cybersecurity Regulation for the financial sector as it provides financial entities with the same consolidated set of requirements. The text of the draft NIS 2 Directive includes provisions on a *lex specialis* regime in recitals (12) and (13), and Art.2(6). The text stipulates that, where a sector-specific EU legal act requires similar obligations with an equivalent outcome, for those included in the NIS 2 Directive, then the sector-specific provisions should apply. Art.1(3) of the CER Directive depicts a similar regime. Nevertheless, Art.2(6) of the NIS 2 Directive proposal could be misconceived as it leaves room for interpretation with regards to the determination of equivalent requirements from other sectoral legislation.

At present, the interactions between the DORA Regulation and the three legislative files are insufficiently defined. Further clarification is needed to highlight the precedence of DORA over the NIS 2 and CER Directives. Financial entities should follow the DORA provisions whenever there are overlaps or inconsistencies with other legislative initiatives.

The Directives should not include additional reporting requirements on top of those foreseen by the DORA Regulation. However, if there is a specific matter that is not addressed by DORA but covered under the NIS 2/CER Directives (thereby making the proposed Directives still relevant for financial entities), the text should ensure the minimisation of regulatory obligations and clearly identify these in the articles of the relevant Directive. Nonetheless, FESE believes that a complete *lex specialis* regime should be explicitly included in the articles of both Directives, i.e. by including an express provision exempting 'financial entities' as defined in DORA from their scope of application with respect to overlapping entity-level obligations.

As the two initiatives are Directives, there is a residual risk of gold plating from Member States when transposing the text into national legislation. It should be well specified that the DORA Regulation is the primary legislative reference for the financial sector and the sole legislative reference in respect of entity-level organisational obligations. This would help to mitigate unintentional increases to their regulatory burden. Furthermore, in case there is a specific matter relevant for the financial sector covered in the Directives, the scope of such provisions should be harmonised across all Members States to the greatest extent possible to avoid divergences in implementation on a local/national basis.

Reporting to local authorities

FESE Members continue to experience different approaches in incident reporting requirements. We believe this is an unnecessary impediment to reaching the goal of keeping the sector resilient and would welcome initiatives aimed at streamlining and harmonising reporting duties.

A typical multijurisdictional company in the EU will likely have an incident response team operating cross-border in a coherent fashion. An incident impacting multiple locations must be reported to different entities, via different formats, with different deadlines. This process is time-consuming and takes attention away from the critical situation at hand.

FESE strongly supports a harmonised reporting process to local authorities which improves efficiency and aims at swiftly addressing critical incidents. Furthermore, when companies report incidents to one competent authority, this authority should share the content of such incidents with other relevant supervisors in an anonymised and aggregated way (with respect to market participants), thereby obviating the requirement to report separately the same incidents to multiple authorities.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80