June 2025

HOPE contribution to the European Commission Call for Evidence "The revision of the Cybersecurity Act"

Given the continuously evolving nature of cyber-threats affecting the hospital and healthcare sector, HOPE is generally in favour of targeted European coordination and measures that improve resilience, lend support national, regional and institutional stakeholders' cybersecurity actions, and enhance the protection of fundamental rights. The "European action plan on the cybersecurity of hospitals and healthcare providers" provides an example of how European and national measures can complement each other. Therefore, adapting the 2019 Cybersecurity Act (CSA) to reflect legislative developments that have altered the cybersecurity ecosystem over the last six years, and consistent with the changed mandate of the EU Agency for Cybersecurity (ENISA), appears to be sensible.

However, the Call for Evidence fails to describe in what way(s) the current Cybersecurity Act is inadequate for ENISA to fulfil its broad mandate of achieving a high common level of cybersecurity across the EU and what specific tasks were added to its portfolio by other EU legislative acts; this should be clarified. An expanded mandate should be accompanied by greater EU funding, both for actions to be carried out by ENISA itself and for EU-initiated measures undertaken at Member State level.

Regarding the CSA revision's focus on streamlining, prioritising and simplification of measures across different cyber legislations, HOPE thinks that the benefits of doing so depend on whether such harmonisation (e.g. in the areas of incident reporting and risk management) improves compliance with existing obligations, such as those stipulated by the NIS2 Directive. From the point of view of hospitals and healthcare, the protection of institutional assets, patient safety and privacy, takes precedence over boosting the competitiveness of technology providers. At the same time, the ability of businesses to effectively meet their obligations and secure their supply chains must not be restrained by overly complex processes or duplicate administrative requirements. Nonetheless, specific attention must be paid to the cybersecurity of critical sectors that harbour especially sensitive data; a revised CSA should not water down the efforts currently underway to strengthen healthcare resilience.

Establishing clear relationships between the CSA and the requirements and ambitions outlined in the Cyber Resilience Act (particularly relevant for technology providers), NIS2 Directive, Data Union Strategy / International Data Strategy and other legislative and non-legislative initiatives (e.g., the above-mentioned Action Plan) relevant to cybersecurity is important. A revised CSA should also consider current and anticipated technological developments including in the areas of cloud services and artificial intelligence.

****

HOPE, the European Hospital and Healthcare Federation, is a European non-profit organisation, created in 1966. HOPE represents national public and private hospitals associations and hospitals owners either federations of local and regional authorities or national health services. Today, HOPE is made up of 36 organisations coming from the 27 Member States of the European Union, as well as from the United Kingdom, Switzerland and Serbia as observer members. HOPE mission is to promote improvements in the health of citizens throughout Europe, high standard of hospital care and to foster efficiency with humanity in the organisation and operation of hospital and healthcare services.